DRN-4600052

The complaint

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

What happened

Ms F says that she was searching for a job opportunity and had signed up to some agencies. She received a message that appeared to have come from a representative of a recruitment agency advising her of a job opportunity. Ms F was referred to a representative of a well known company I'll refer to as G who explained the role. It involved completing sets of tasks to help hotels improve their rating and attract more tourists. Ms F was told that she would receive £70 to £120 a day and commission. She didn't know at the time, but the job opportunity wasn't genuine, and she was communicating with scammers.

Ms F was introduced to a platform and was advised she needed to maintain a positive balance to be able to complete the tasks and earn money. These funds would be returned when the set of tasks were completed (along with the commission earned). To add money to her account at G, Ms F was given instructions to buy cryptocurrency using a peer-to-peer exchange platform. She then sent it to cryptocurrency wallet addresses provided by the fraudsters, and that cryptocurrency then appeared on her account at G.

Ms F was repeatedly given 'commercial orders'. These were said to be randomly generated tasks which cost more and brought nine times more commission than ordinary tasks. Ms F was then asked to make further payments before she could complete the set of tasks and withdraw her funds. These payments related to insurance to cover the costs of commercial orders, a validation fee, a fee to unfreeze her account and tax.

Ms F realised she was the victim of a scam when she was unable to withdraw her money. She now knows that G was a fake company, and the platform was also fake.

Over the period 21 August to 4 September 2023 Ms F completed 59 transfers which totalled over £90,000. A number of card transactions to a cryptocurrency provider were also declined. The investigator set out the relevant transactions in his view, so I won't list them here as well. But the investigator didn't include the fees charged by Revolut when the transactions were made, which also form part of Ms F's loss.

Ms F notified Revolut of the scam through a professional representative on 16 September 2023.

Revolut didn't agree to reimburse Ms F's loss. It said the transactions were authorised and it had sufficient fraud prevention measures in place. Revolut also said it had tried to recover Ms F's funds but hadn't been successful.

Ms F was unhappy with Revolut's response and brought a complaint to this service through her professional representative.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. He said that although there were points when Revolut should have gone further and provided tailored written warnings or some form of human intervention, it wouldn't have made a difference.

This was because he said Ms F was being coached by the scammer. Ms F also gave incorrect answers to some of Revolut's questions.

Ms F didn't agree with the investigator's findings. In summary, she said:

- The transactions she made were clearly out of character. There were multiple new high risk peer to peer payees, multiple transactions in a single day in quick succession and Ms F lost over £90,000 overall. Revolut also knew Ms F was buying cryptocurrency. These features matched known fraud trends.
- The automated and pop-up warnings Ms F received were ineffective and contained irrelevant information. Ms F clearly said she was sending funds to buy cryptocurrency but instead of receiving cryptocurrency related warnings she was given safe account warnings. Revolut should have asked Ms F open questions about the transactions.
- In response to the investigator's comments that Ms F was coached, she said that she openly said she was buying cryptocurrency using the peer-to-peer method which should have prompted strong intervention from Revolut. This demonstrates Ms F was forthcoming and there is no reason to believe that better intervention wouldn't have made a difference.
- Task based job scams were very common at the time. Revolut should have been aware of this and gone further. If it had, there were numerous other red flags that would have come to light such as the fact Ms F was contacted via a messaging service, had no contract or documents, was buying cryptocurrency and a legitimate brand was impersonated.

As the complaint could not be resolved informally it was passed to me to decide. I reached the same outcome as the investigator but as I included additional reasoning I issued a provisional decision on 29 January 2025. In the 'What I have provisionally decided – and why' section of my provisional decision I said:

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; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Having done so, I have reached a different provisional conclusion to the investigator about what is fair and reasonable in all the circumstances of this complaint and about what Revolut should do to put things right and will explain why.

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.

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 August 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); 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.*

Should Revolut have recognised that Ms F was at risk of financial harm from fraud?

It isn't in dispute that Ms F has fallen victim to a cruel scam here, nor that she authorised the payments she made by transfers to third parties. The cryptocurrency she bought was then passed on to wallet details provided by the scammer.

I am mindful that when Ms F made the payment requests Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Ms F might be the victim of a scam. Ms F's account had been opened for some time but had been dormant from August 2019 onwards.

I don't consider Revolut would have had any reason to intervene when Ms F made the first payment to a third party. The value of the transaction was low (£1,480). Taking into account that Revolut needs to strike a balance between protecting against fraud and not unduly hindering legitimate transactions, as well as the value of this payment, I don't think Revolut ought to have been so concerned about this payment that it ought to have provided warnings to Ms F at this point.

Revolut blocked transactions attempted by Ms F after this first transaction had been made and directed her to its chat. I have discussed this in more detail below so for now I will just say that when she was asked to provide more details about the goods and services she was buying (as this was the payment purpose Ms F chose), she said she was buying cryptocurrency using the peer to peer method.

By August 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. And by August 2023, when these payments took place, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allow customers to use their accounts to purchase cryptocurrency with few restrictions.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that the vast majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Ms F made in August 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency.

In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And, as I've set out, the introduction of the FCA's Consumer Duty, on 31 July 2023, further supports this view. The Consumer Duty requires Revolut to avoid causing foreseeable harm to its customers by, among other things, having adequate systems in place to detect and prevent scams.

What did Revolut do to warn Ms F?

Revolut says it warned Ms F prior to each transfer to a new payee that she might be falling victim to a scam by providing the following message:

"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."

Ms F's first payment to a new payee for £1,480 was processed. Further payments to the same payee were declined. Ms F was directed to Revolut's in app chat and told a transaction for £3,396.31 to the same payee as her original payment had been held by Revolut's security system. Ms F was asked to provide a selfie but didn't do so. Shortly after, Ms F tried to make the payment again. She was asked to provide a payment reason and chose 'Payment for Goods and Services'. She was directed to Revolut's in app chat, where she was told that there was a high chance her money might be at risk and that her payment had been declined and she would have to wait for 24 hours to proceed.

Ms F told the Revolut agent she wasn't happy with the delay. The agent suggested she tried making a smaller payment, which she did. This payment (£1,686.31 on 21 August 2023) was also blocked, and Ms F received a message in Revolut's chat saying it was being held. The message included safe account scam information. The agent went on to ask Ms F for more information about the goods she was buying. Ms F responded by saying she was buying cryptocurrency using the peer-to-peer method. But she was provided with a warning tailored to buying goods and services, which included information about market value, social media adverts and completing research.

The information Ms F gave to Revolut about buying cryptocurrency was totally ignored and a warning that had no relevance to the payment Ms F was making was provided. So I'm not satisfied that Revolut did enough to protect Ms F.

This wasn't the only time Revolut failed to respond appropriately to information provided by Ms F. On 26 August 2023 a further payment to a different payee was held and Ms F was again directed to the chat. Ms F was asked to provide more information about the goods and services she was buying and told Revolut she was purchasing cryptocurrency using the peer-to-peer method. Again, Ms F was provided with a warning related to buying goods and services.

Revolut has explained to this service that it asked Ms F to provide a reason for the payment she was making on 19 occasions. On three occasions Ms F chose cryptocurrency and for all remaining transactions she chose paying for goods and services. Revolut said it provided educational screens about victims losing millions of pounds to scams each year and fraudsters being professionals, and some advice based on the payment reason chosen. When Ms F chose goods and services, she was provided with screens which discussed the price, payment method and research completed. When she chose cryptocurrency, the screens provided to Ms F covered access to her account, screen sharing, and the fact research was required if she was making an investment.

Revolut says Ms F was provided with other warnings related to buying goods and services. But given Ms F told Revolut she was buying cryptocurrency very early on, and that later payments to a cryptocurrency exchange were declined, I don't think Revolut did enough to protect Ms F at the time the payments were made.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's primary duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by August 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam.

I consider a firm should by August 2023, on identifying a heightened scam risk, have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew that Ms F was making payments for cryptocurrency. Revolut should have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation, job, and investment scams.

Taking that into account, I am satisfied that, by August 2023, fairly and reasonably, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Ms F made payment two (£1,698.31 plus fee on 21 August 2023), Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Ms F was at risk from.

I'd have expected Revolut to have asked a series of simple questions in order to establish the risk the payment presented. These questions needed to go beyond simply asking what the payment was for and why cryptocurrency was being purchased. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Ms F gave.

<u>If Revolut had provided a warning of the type described, would that have prevented the losses Ms F suffered from the second payment (£1,698.31 on 21 August 2023)?</u>

I've thought carefully about what is most likely to have happened if Revolut had intervened in the way I have set out above.

Ms F funded her Revolut account by making transfers from other accounts. This service has contacted those other financial institutions to find out if any of them intervened when Ms F credited her Revolut account.

I have listened to a call Ms F had with a bank on 21 August 2023. The bank concerned asked questions to satisfy itself Ms F wasn't at risk of falling victim to a scam. Ms F explained that she was doing cryptocurrency trading when the market was good. This led the agent to ask additional questions and to provide warnings. Ms F was advised there were a lot of scams related to cryptocurrency and to be extremely cautious before investing. The agent discussed guaranteed returns, returns that seem too good to be true and pressure to act quickly. The agent went on to advise Ms F to be wary of adverts online or on social media and to be cautious if she was contacted out of the blue, including via social media.

The agent asked Ms F if she had discussed what she was doing with family or friends and whether she had checked the FCA register to make sure she was dealing with an authorised firm and there was no warning in place. Ms F said that she had. The agent then advised that cryptocurrency was high risk, volatile and not regulated and asked Ms F to do her due diligence.

Although Ms F was open about buying cryptocurrency, she misled her bank about why she was buying it and the research she had completed. She was also provided with warnings that were relevant to her, like out of the blue contact, and to do her own research.

In a conversation with another bank on the same day, when Ms F was transferring funds to her Revolut account, Ms F said she was using her Revolut account for a holiday in Spain.

The adviser from her bank asked her if anyone had contacted her via social media offering a way to earn money or invest and get good returns. Ms F said she hadn't. The adviser had concerns and Ms F was asked to go into branch. In a call with the fraud team two days later the adviser checked that Ms F hadn't been contacted and told to lie to her bank or been asked to move the money for any reason. Ms F told the bank it was her decision to move money and it was her own account.

Ms F's bank gave advice about sending funds to a platform which shows she is making money every day and of additional charges for things like tax. Whilst this advice related to an investment, parts of it were relevant to the situation she was in.

It's also clear to me that Ms F followed the scammer's instructions in her interactions with Revolut. Ms F sent the scammer screenshots and took the steps the scammer advised. She was told to tell Revolut she was buying cryptocurrencies via the peer-to-peer method. Ms F responded by saying, "they advised that if an institution is guiding on what to say on this chat support, they are trying to scam you…". The rest of this advice from Revolut was that if an institution was guiding Ms F on what to say in chat support, they were trying to scam her, and she should notify Revolut immediately. Ms F didn't take this step.

Having carefully considered the evidence I'm not persuaded Ms F would have been honest with Revolut and explained that she was making payments in respect of a job opportunity. Ms F misled both banks who intervened and followed the scammer's instructions. On balance, I consider it more likely than not that Ms F would have told Revolut she was investing and that nobody was helping her. The warning Revolut should then have provided would have been tailored to cryptocurrency investment scams and wouldn't have resonated with Ms F or prevented her from making further payments.

Could Revolut have done anything to recover Ms F's money?

The payments Ms F made were to individuals selling cryptocurrency who were very likely unconnected to the fraudsters. As those individuals were unlikely to be involved in the fraud, even if it were practical or possible to recover funds from them, it would be unlikely to be fair for that to happen (given that they'd legitimately sold cryptocurrency). So, I don't think Revolut should have done anything more to try and recover Ms F's money.

Revolut didn't respond to my provisional decision. Ms F let me know she disagreed but didn't tell me why.

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.

As neither party has raised any new points or provided any further evidence for me to consider, my final decision is the same as my provisional decision, which is set out above.

In summary, although I'm satisfied Revolut should have done more to protect Ms F, I'm not persuaded that further or better intervention would have prevented her losses. I say this based on the intervention of other banks and the messages Ms F exchanged with the scammer.

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 F to accept or reject my decision before 13 March 2025.

Jay Hadfield
Ombudsman