DRN-5238485

The complaint

Miss F is unhappy Revolut Ltd ("Revolut") won't refund the money she lost as the result of a scam.

What happened

In August 2023, Miss F was looking for work when she received a message about an opportunity to earn money whilst working from home. The role was to promote various different products. Over the following few days Miss F was told how to use the website and that her job would actually involve completing assigned 'tasks' to earn commission. Miss F opened an account with the employer. This displayed her tasks, 'earnings' that day and her overall 'balance'. Miss F was given two sets of 40 tasks to complete per day, where she would click a button on the app which would automatically boost the data for the product. Each task would cost a certain amount of USDT cryptocurrency. Once she completed a set, she would receive her commission from the profits made on any sales for the products, and this would be allocated to her wallet on the job platform.

Miss F would sometimes be granted 'combination tasks', which required a group of tasks to be completed before any withdrawal could take place. Each combination task had a value, given in USDT. Each time a combination task was assigned, the value of the task in USDT would be deducted from Miss F's balance on the job platform. That would leave Miss F with a negative balance that, it was claimed, would need to be made positive (by depositing USDT into her job account) before any withdrawals could be made (both of earned commission and the money that she'd paid to the platform). All of the money she paid to the platform was supposedly refundable as long as the tasks were completed.

In order to add money to her job account on the platform, Miss F needed to convert her money into USDT. Once the cryptocurrency had credited her accounts with Cryptocurrency B and B2, she sent it to cryptocurrency wallet addresses provided by the fraudsters and that cryptocurrency then appeared on her account on the fake job platform.

But, before Miss F could remove her negative balance and withdraw her money, she'd be given another combination task of a greater value – meaning she'd have to complete those tasks (and therefore make another payment) before accessing her money. When Miss F questioned this, she was told that she couldn't cancel the tasks, they had to be completed and if she didn't resolve the negative balance on her account, she'd lose all of her money – both the commission she'd earnt and the money she'd paid.

The assignment of these combination tasks was apparently random and fortunate (given that Miss F would be paid more for completing combination, rather than regular, tasks). In fact, it is these tasks which are integral to the success of the scam. The scam tends to go on for as long as the fraudsters are able to persuade the victim to keep making payments.

After not receiving her funds, she realised this was a scam and raised it with Revolut.
As a result of the scam, Miss F made the following transactions by card:

Transaction #	Date	Payee	Amount
1	18 August 2023	Cryptocurrency B	£260
2	18 August 2023	Cryptocurrency B	£300
3	19 August 2023	Cryptocurrency B	£1,600
4	19 August 2023	Cryptocurrency B2	£2,800
5	20 August 2023	Cryptocurrency B	£2,123
6	20 August 2023	Cryptocurrency B	£500

Revolut declined Miss F's claim as she carried out the transactions herself. It also highlighted the following points when submitting its file:

- The fraudulent activity did not take place primarily on the Revolut platform and Miss F lost control of the funds further along in the chain.
- Miss F's lack of appropriate due diligence before making the payments, such as searching online. She was asked to pay money in order to work which is completely illogical.
- The scam was not a 'heat of the moment' single payment or 'out of character' transaction scenario, but a scam where six payments were sent over a period of three days.

Our investigator upheld the complaint in part. He felt by the fourth transaction Revolut ought to have done more than it did, and this would have likely prevented the scam. So he recommended Revolut refund Miss F. However, he also thought this refund should be reduced by 50% as there was more Miss F could have done to prevent her losses.

Miss F accepted the view; Revolut did not respond.

I issued my provisional decision on 8 November 2024. Revolut did not respond. Miss F did not accept my provisional decision. In summary Miss F's representatives said:

Regarding the payment options outlined within the provisional decision if the client can't recall the option she chose, surely Revolut can provide which option she chose. It does not necessarily mean she would have lied to revolute if they intervened effectively by asking probing questions.

It outlined that better probing and questioning would have bought the scam to light.

Regarding the circumstances of the payment to her main High Street bank this has no relevance to Revolut's lack of effective intervention and Revolut's obligations should not be withdrawn simply because a different bank previously had intervened.

I responded to Miss F's representative as follows:

- The payment options listed were a list sent to Miss F from her cryptocurrency provider (B). Miss F shared the screen shot of this list within the messages with the scammer to ask what to choose – so Revolut would not be aware of this or what she selected.

- Given the pattern and sums involved - as outlined in my provisional decision – my view is that a proportionate intervention would have been "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 Miss F was at risk from". To be clear – for the pattern and sums involved, I do not think Revolut needed to intervene further (for example directing Miss F to its in-app chat function for further questioning).

- Please also note I am not making any opinion on Miss F's High Street bank or its intervention) in this case. I am simply assessing whether I think better intervention by Revolut would have made a difference (causation) to Miss F's decision making. Assessment of that is based on the balance of probabilities. As outlined in my provisional decision: "That is on what I consider is more likely to have (or would have) happened in light of the available evidence and the wider circumstances."

Neither Miss F nor her representative were able to get a copy of the call recording from her High Street bank.

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.

I appreciate neither Miss F nor her representative were able to obtain the call recording from her High Street bank. Having reviewed my provisional decision, I have concluded that I don't need to rely on this evidence when reaching my final decision. Having reconsidered all the evidence and arguments, my final decision remains the same as my provisional decision – broadly for the same reasons. For completeness I have attached this below – removing any reference to the third-party call recording from Miss F's other bank.

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.

Where the evidence is incomplete, inconclusive or contradictory (as some of it is here), I reach my decision on the balance of probabilities – in other words, on what I consider is more likely to have (or would have) happened in light of the available evidence and the wider circumstances.

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.

However, taking into account relevant law, regulatory 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 Miss F was at risk of financial harm from fraud?

It isn't in dispute that Miss F has fallen victim to a cruel scam here, nor that she authorised the payments she made by card to her cryptocurrency wallets (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst we now know the circumstances which led Miss F to make the payments using her Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Miss F might be the victim of a scam.

All the payments here were made to cryptocurrency providers. I'm aware that cryptocurrency exchanges like B (and B2) generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Miss F's name.

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[1]. And by August 2023, when these payments took place, further restrictions were in place[2]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wished to purchase cryptocurrency for legitimate purposes would be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant 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 in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Miss 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, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements (including the Consumer Duty), Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the payments in this case were going to an account held in Miss F's own name should have led Revolut to believe there wasn't a risk of fraud.

---

[1] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.
[2] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

So, I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Miss F might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the payments were going to a cryptocurrency provider (both merchants are well-known cryptocurrency providers and Revolut acknowledged that), but the first three payments were low in value (although I appreciate it is a lot of money to Miss F), and in keeping with previous transaction Miss F had made from the account, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

But, not only was payment 4 clearly going to a cryptocurrency provider, it was significantly larger than any other payment that had debited Miss F's account in the previous six months. It had been preceded by a payment of £1,600 just forty minutes earlier and was the fourth transaction to a cryptocurrency exchange in two days. The purchase of cryptocurrency was out of character for Miss F. On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, and also considering the value of this payment (and the pattern that preceded it), I think Revolut ought to have been sufficiently concerned about this payment that it would be fair and reasonable to expect it to have provided warnings to Miss F at this point.

Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Miss F was at heightened risk of financial harm from fraud.

In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by August 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud.

Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What kind of warning should Revolut have provided?

Revolut didn't provide any warnings in this case. So 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 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 for both APP and card payments. I understand in relation to Faster Payments it already had systems in place that enabled it to provide warnings in a manner that is very similar to the process I've described.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by August 2023, on identifying a heightened scam risk, a firm such as Revolut should 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 the payments were being made to cryptocurrency providers and its systems ought to have factored that information into the warning it gave. Revolut should also 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, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Miss F made the fourth transaction, 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 Miss F was at risk from.

However, I do acknowledge that any such warning relies on the customer answering the questions honestly and openly.

If Revolut had provided a warning of the type described, would that have prevented the losses Miss F suffered from £2,800 payment?

Even if I did conclude that Revolut should have done more here, it isn't enough that Revolut failed to act unfairly or unreasonably. Its acts or omissions must be the immediate and effective cause of losses that were reasonably foreseeable at the time of the breach.

I can't know for certain what would have happened if Revolut had attempted to narrow down the potential risk of Miss F payment to cryptocurrency further. In such situations, I reach my conclusions on what I find more likely than not to have happened in the circumstances. In other words, I make my decision based on the balance of probabilities – considering the evidence and wider circumstances of the case.

Looking at the messages Miss F had with the scammer – the evidence suggests earlier on in the scam (around 15 August 2023) that her cryptocurrency provider sent her a scam alert. It seems her cryptocurrency provider sent this when she sent funds from her wallet to the job platform. It alerted her to a possible scam. She was also asked by the cryptocurrency provider about the purpose of the withdrawal from her wallet. There appears to have been a number of options (this is a screenshot of a screenshot and is not fully displayed within the chat messages) including:

- high returns from mining/financial investment projects
- paying additional fees/taxes/commissions from other platforms
- transferring assess to a safe address under the guidance of police/customer services/tax professional/experts
- personal transfer for non-profit purposes
- participation in blockchain giveaway
- received some income from a cryptocurrency company
- profits from an arbitrage trading platform

Miss F shared this screen shot with the scammer and asked advice about what to choose. As the scammer didn't reply immediately, Miss F told us she called the fake job customer services, and they told her what to choose – but this isn't evidenced within the messages I've seen. Miss F can't now recall what option she chose but didn't think it was any of those listed above. However, she recalled that it "definitely was not to do with business ..something to do with family and friends". I can't see there was an option similar to the latter. I have thought about this carefully in the context of whether a better warning would have made a difference here.

Based on the fact Miss F was heavily relying on the advice of the scammer and being coached through the answers she needed to give at the time the transactions were made - I think it likely the scammers would have provided plausible answers to any further intervention. On balance I am not persuaded she would have explained she was making the payment as part of a job (or business related). And so, I don't think Revolut could reasonably be expected to identify that Miss F was specifically falling victim to a job scam.

Overall, whilst I'm very sorry to hear about this cruel scam and the impact it has had on Miss F, having carefully thought about this, I'm not convinced that any further intervention would have made a difference to Miss F's decision-making. I therefore can't fairly ask Revolut to reimburse her.

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

The payments were made by card to a cryptocurrency provider. Miss F sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that cryptocurrency B provided cryptocurrency to Miss F, which she subsequently sent to the fraudsters.

I realise my decision will be a significant disappointment to Miss F especially as it differs to the investigator's assessment. I sympathise with her circumstances, and I am sorry she has fallen victim to a scam. But having considered all the evidence and arguments, for the reasons above, my decision is Revolut cannot fairly be held liable for her losses.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss F to accept or reject my decision before 31 January 2025.

Kathryn Milne
Ombudsman