DRN-5049544

## The complaint

Ms A complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by a 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.

Ms A was approached on WhatsApp by someone I'll refer to as "the scammer" who claimed to represent "Company E". The scammer told Ms A about an opportunity to work from home with flexible hours. They said the job would require her to make deposits in cryptocurrency to purchase tasks which she would compete in return for a commission of 1.5% of the value of the task. They explained the merchants that pay for the service benefit from the scheme as the simulated 'purchases' improve the algorithms of each product which in turn improves the chances the merchant will be able to sell the item.

The scammer explained Ms A would need to add deposits to the platform to simulate 'buying' the item, and that each task would use up some of the deposit, but the commission would be added to her account. At the end of a 'set' of 20-30 tasks, she would have the opportunity to withdraw her commission as well as the original deposits.

Ms A was actively looking for a job, so she checked E's website and looked on online for reviews. She was also satisfied the scammer had answered all her questions and when she agreed to take on the job she was added to a WhatsApp chat group with others doing the same job.

The scammer instructed her to open an account on the platform and to open an account with Revolut, which she did on 23 April 2023. They also asked her to first purchase cryptocurrency and then load it onto an online wallet. Between 26 April 2023 and 28 April 2023, Ms A made four faster payments from her Revolut account totalling £21,270 (having transferred funds from her account with Bank H). She received some returns after tasks 2, 4 and 7, but when she was unable to make any further payments, she tried to make a withdrawal and was told she'd have to complete the set to recover her money. She realised she'd been scammed when she was continually required to put money into the portal.

Ms A complained to Revolut when she realised she'd been scammed, but it said it didn't have enough information to investigate the claim. She wasn't satisfied and so she complained to this service with the assistance of a representative who said that as the account was newly opened, Revolut should have been suspicious that she was sending large sums of money to a cryptocurrency merchant. They said that if it had intervened, it would have realised there were red flags present including the fact she was contacted via an unsolicited WhatsApp message, she was required to make deposits in cryptocurrency to unlock tasks, she was added to a group of others doing the same job, and the payments were getting larger and more frequent.

Revolut said the payments were sent over a period of three days. It argued that Ms A had authorised the transactions and the fraudulent activity didn't take place on its platform as it was used as an intermediary to receive funds from the Ms A's main bank account. The funds were then transferred to a legitimate cryptocurrency platform where she subsequently lost control them.

It also said Ms A was given warnings which were appropriate and proportionate. It explained she made the first transfer on 26 April 2023 when an internal alert was triggered and she was warned about the risk of falling victim to a scam. Two similar alerts were triggered for the subsequent transactions, but she proceeded with the payments. It said she was warned about the risks she could face if she proceeded with the transfers and that it may not be able to recover the funds if it later turned out that the beneficiary was fraudulent. The warning, which was displayed prominently at the top of the page, stated: "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 explained Ms A acknowledged the warning and it conducted a further review as she was paying a new beneficiary. She was then shown a set of dynamic educational story messages to warn her about the risks associated with the payment. She was also asked about the purpose of the payment and given tailored warnings relating to the nature of the payment.

It also said the returns were unrealistic and Ms A failed to complete reasonable due diligence or evaluate the risk or verify the legitimacy of the transfers. And it acted promptly to recover any potential losses.

Our investigator didn't think the complaint should be upheld. She commented the account was newly opened, there was no transaction history to compare the payments with, and Revolut did present warning messages and education about scams. She noted Ms A still wanted to go ahead with the payments and she didn't think Revolut could have done anything else to prevent that. Finally, she explained that when Ms A reported the scam, Revolut requested additional information, but she didn't provide it, so a recovery attempt wasn't possible.

Ms A asked for the complaint to be reviewed by an Ombudsman. Her representative argued Revolut ought to have contacted Ms A and questioned her about the payments. They argued the payments were out of character and well above what this service would generally say required questioning. Overall, she sent £21,270 to a high-risk cryptocurrency merchant with £16,270 sent in quick succession in a single day. They also argued that the second payment of £4,000 brought the total daily spend to £6,600 which is well above what this service would normally say needed questioning.

They maintained that if Revolut had asked Ms A about the purpose of the payments she would have explained that she intended to use cryptocurrency to purchase tasks and it would have uncovered the scam and prevented her loss.

I issued a provisional decision explaining that I thought Revolut ought to have intervened when Ms A made the third payment and that its failure to do so represented a missed opportunity to have prevented her loss. I said I was minded to direct Revolut to refund the money Ms A had lost from that payment onwards and that the settlement should be reduced by 50% for contributory negligence.

Ms A's representative has indicated that she is happy to accept my provisional findings, but Revolut made further arguments. It said Bank H is Ms A's main bank and should have intervened in respect of the payments from that account. It also argued that Ms A gave the

account opening purpose as ‘transfers’, when its clear the account was opened to facilitate payments to the scam, and it has questioned what she said to the family members from whom she borrowed money to fund the scam payments.

Finally, it argued that Ms A was making payments to a legitimate cryptocurrency merchant so it would have been difficult to persuade her that she was the victim of a scam because she was receiving cryptocurrency into another account under her control.

**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 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.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer’s instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer’s payment decisions.

- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In *Philipp*, the contract permitted Barclays not to follow its consumer’s instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut’s contract with Ms A modified the starting position described in *Philipp,* by expressly requiring Revolut to refuse or delay a payment “*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*”.

So Revolut was required by the implied terms of its contract with Ms A and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in April 2023 fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

In reaching the view 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 am mindful that in practice all banks and EMI's like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[2]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[3].
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the

[1] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

[2] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

[3] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code[4], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

Overall, 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 April 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 – (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 A was at risk of financial harm from fraud?*

It isn't in dispute that Ms A has fallen victim to a cruel scam here, nor that she authorised the payments she made.

Whilst I have set out in detail in this decision the circumstances which led Ms A to make the payments using her Revolut account and the process by which that money ultimately fell into

[4] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

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 Ms A might be the victim of a scam.

I'm aware that cryptocurrency merchants generally stipulate that the card used to purchase cryptocurrency 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 the payments would be credited to a cryptocurrency wallet held in Ms A's name.

By April 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. 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 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 a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud. 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 Ms A made in April 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.

To be clear, I'm not suggesting as Revolut argues that, as a general principle (under the Consumer Duty or otherwise), Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in April 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

*What did Revolut do to warn Ms A?*

Revolut has explained an internal alert was triggered when Ms A made the first payment. She was warned was about the risk of falling victim to a scam and that it might not be able to recover the funds if the beneficiary was fraudulent. She was also shown a set of dynamic educational story messages to warn her about the risks associated with the payments and

given tailored warnings related to the nature of the payment.

I've considered whether this intervention was proportionate, and I'm satisfied that it was. Even though the first payment was to an account in Ms A's name, this was a new payee and it would have been apparent that she was buying cryptocurrency, so I think its decision to intervene was fair. But as the payment wasn't particularly high value, I'm satisfied a written warning was proportionate and that the scam warnings were relevant to the circumstances. So I don't think it needed to do anything else.

Ms A's representative has pointed out that by the time she made the second payment on 26 April 2023, the cumulative spend for the day was £6,600. But Revolut has explained similar warnings were given for the subsequent transactions, and I'm satisfied a written warning remained proportionate to the risk.

*What kind of warning should Revolut have provided?*

By the time Ms A made the third payment on 26 April 2023, this was the third consecutive payment, and it brought the cumulative spend in one day from a newly opened account to £16,270. Even though Ms A had received warnings in respect of the two earlier payments and this payment wasn't to a cryptocurrency merchant, it was a high value payment to a new payee and followed two payments to cryptocurrency merchants. I think Revolut ought to have been concerned about the pattern and cumulative value of the transactions and contacted Ms A either by phone or live-chat to ask her some questions payment before allowing it to debit the account.

I haven't seen any evidence that Ms A been coached to lie and so I think she'd have said she was making payments in cryptocurrency for a job opportunity in respect of which she'd been contacted on WhatsApp. I'm satisfied that with this information Revolut would have identified that the payments were being made in relation to fraud and advised her that there were red flags present indicating that she was being scammed. It should then have provided a tailored cryptocurrency warning including education relevant to job scams.

*If Revolut had provided a warning of the type described, would that have prevented the losses Ms A suffered from the third payment?*

There's no evidence that Ms A ignored any advice from her other bank, and I don't think the warnings she received from Revolut were sufficient to draw the scam risk to her attention.

If Revolut had provided robust warnings and education about the specific scam type, I'm satisfied Ms A would have listened to the advice she was given. This wasn't a high-risk investment and it's clear from her communications with the scammer that she'd genuinely believed this was a genuine employment opportunity. Consequently, I think she'd have listened to and acted on some robust advice from Revolut that she was probably being scammed.

It may be that there wasn't any information online about the scam company and I accept she was paying a legitimate cryptocurrency merchant, but some basic internet research would have confirmed that the circumstances fit with a common scam type and that there were red flags present indicating that she was a victim of fraud.

Consequently, I'm satisfied that Revolut missed an opportunity to intervene in circumstances which might have prevented her loss.

*Is it fair and reasonable for Revolut to be held responsible for Ms A's loss?*

In reaching my decision about what is fair and reasonable, I have taken into account that Ms A purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

But as I've set out above, I think that Revolut still should have recognised that Ms A might have been at risk of financial harm from fraud when she made the third payment, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Ms A suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Ms A's own account does not alter that fact and I think Revolut can fairly be held responsible for Ms A's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Ms A has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Ms A could instead, or in addition, have sought to complain against those firms. But Ms A has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Ms A's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Ms A's loss from the third payment (subject to a deduction for Ms A's own contribution which I will consider below).

*Should Ms A bear any responsibility for their losses?*

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

Having considered the circumstances of this scam, I think it was unreasonable for Ms A not to have questioned why she was being asked to make payments in cryptocurrency for a job she was expecting to be paid for or not to have questioned why she wasn't given any employment documents, for example a contract.

I accept she'd been looking for work and that she was reassured by the fact she'd been added to a chat with others doing the same job, but there's no evidence she did any due diligence beyond looking for reviews online and as there would have been plenty of

information available online about this type of scam I'm satisfied that some simple research might have indicated to her that she was at risk.

As I've explained above, it seems Ms A was satisfied this was a genuine opportunity to make extra money and she didn't become suspicious until she was prevented from withdrawing her commission. But in the circumstances, I think its unreasonable that she didn't question sooner what she was being asked to do and seek some confirmation that the job was genuine, so I think the settlement should be reduced by 50% for contributory negligence.

*Compensation*

The main cause of the upset was the scammer who persuaded Ms A to part with her funds and as I haven't found any errors or delays to Revolut's investigation, I don't think she was entitled to any compensation.

*Recovery*

I don't think there was a realistic prospect of a successful recovery because the funds were transferred to a legitimate cryptocurrency platform where they were subsequently lost.

**My final decision**

My final decision is that Revolut Ltd should:

- refund Ms A the money she lost from the third payment onwards, less any withdrawals she made during that period.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Ms A with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms A to accept or reject my decision before 25 October 2024.

Carolyn Bonnell
**Ombudsman**