DRN-4997440

The complaint

Miss T complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an employment 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 2003, Miss T received a WhatsApp message from someone who claimed to work for a company which I'll refer to as "A". The person told Miss T about an opportunity to work from home and as she'd been actively looking for work, she didn't think there was anything suspicious about the call.

She was subsequently contacted by someone who I'll refer to as "the scammer" who explained the role would require her to leave 5-star reviews on hotels. She would have to complete 38 tasks a day (or 66 to receive a bonus) and she would receive commission depending on the amount of work she did. The scammer explained that Miss T would have an account manager, but she would have access to the platform and be able to make withdrawals herself.

Miss T looked at the company website, which seemed professional and featured a certificate of registration, an FAQ page, and the logos of affiliated companies. She created an account which required her to provide ID, and she was added to a group chat on WhatsApp with other employees who were completing the same tasks.

The scammer explained she'd have to purchase tasks using cryptocurrency and asked her to first purchase cryptocurrency through a cryptocurrency exchange company, and then load it onto an online wallet. Miss T topped up her Revolut account with funds from Bank L and on 18 September 2023 and 19 September 2023, she made four debit card payments totalling £5853.74 to a cryptocurrency exchange which I'll refer to as "M". During this period, she also tried to make four payments which were cancelled by the recipient and returned to the account.

As Miss T completed the tasks, she could see the balance on her account and commission increasing. She made a small withdrawal on the second day, but was later told her account had a negative balance and she'd have to clear the balance before she could make a further withdrawal. She was eventually alerted to the scam by her partner and when she refused to make any further payments, she was locked out of the account.

She complained to Revolut arguing it had failed to take the necessary steps to protect her from financial loss. She also asked it to dispute the transactions via the chargeback process. But Revolut refused to refund any of the money she'd lost, stating the transactions had been authenticated by 3DS.

Miss T wasn't satisfied and so she complained to this service with the assistance of a representative. She argued that if Revolut had told her how to protect herself and explained the potential consequences of making the payments, she wouldn't have gone ahead with the payments.

Her representative said Miss T didn't receive any pop-up notifications or scam warnings, and that Revolut should have intervened because she was making multiple payments to a new, international payee. This represented a sudden increase in spending, it was a sudden change to the operation of the account, and the payments were high-value when compared to the previous spending on the account. They said it should have intervened and asked probing questions and had it done so her loss would have been prevented.

Revolut further explained it had no chargeback right as there was no fraudulent activity on the account and the transactions were authorised by 3DS. It also said that once the funds were deposited to the cryptocurrency exchanges, the service was considered to have been provided. It said there were no interventions or warnings and as Miss T was transferring funds through card payments to her own cryptocurrency accounts, the transactions were self-to-self and weren't within the accepted definition of an APP scam.

It further argued that Miss T had sufficient time to research the opportunity, yet she rushed to deal with the company on the promise of unrealistic returns. She received the job offer via WhatsApp, she had no employment documents, and had to pay for tasks using cryptocurrency, which ought to have raised concerns. Further, there was no interview process or required experience, and she was being asked to submit fake reviews on hotels.

Our investigator felt the complaint should be upheld. She didn't think payments 1 to 3 were suspicious because they were low value. But she thought Revolut should have done more when Miss T made the fourth payment because it was the eight-payment Miss T had attempted to make within two days to a high- risk cryptocurrency merchant. She thought Revolut should have contacted Miss T, asked her about the purpose of the payment, and provided a tailored scam warning before allowing it to be made.

Had it done so, she thought the scam would have been uncovered because there was no evidence Miss T been coached to lie and so she'd have shared that she was making payments in cryptocurrency for tasks in return for which she expected to be paid a commission. She further explained that she thought Revolut would have detected the scam and that Miss T would have listened to advice because she was already concerned that she didn't have the funds to make further payments.

Our investigator thought liability should be shared between both parties because Miss T didn't check A was a genuine company and had she done so, she'd have seen it had no online presence. She also noted that before Miss T had made the second payment, she said she had concerns "that all of this is a scam", commenting that she should have stopped to make checks, especially as the commission was unrealistic.

Revolut has asked for the complaint to be reviewed by an Ombudsman arguing that there is no rational explanation as to why it should be held responsible for Miss T's loss in circumstances where it was merely an intermediate link, and there were other authorised banks and financial institutions in the payment chain that had comparatively greater data on Miss T.

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've thought about whether Revolut could have done more to recover Miss T's payments when she 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 (Miss T).

Miss T's own testimony supports that she used cryptocurrency exchanges to facilitate the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Miss T'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.

I'm satisfied Miss T '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 Miss T 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 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 Miss T 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*".

In this respect, section 20 of the terms and conditions said:

> *"**20. When we will refuse or delay a payment***
>
> *We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:*
>
> - *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 Miss T and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

I am satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in September 2023 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.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment. And I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp*.

I have taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I am also mindful that in practice, whilst

its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R:

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in September 2023 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.

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;[1]
- 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.

For example, it is my understanding that in September 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

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).
- 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

[1] 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_/

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 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[2], 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).

- Since 31 July 2023, under the FCA's Consumer Duty[3], regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"[4].*

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[5] 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.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain

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

[3] Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

[4] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

[5] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

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 September 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.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in September 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Miss T was at risk of financial harm from fraud?

Revolut didn't intervene in any of the payments and Miss T wasn't given any warnings or scam advice. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Miss T normally ran her account and I note the account was opened in December 2022, so there was an account history to compare the payments with. All the payments were to legitimate cryptocurrency exchanges, and the first three successful payments were for relatively small amounts. So, even though Miss T hadn't previously made payments to M, I don't think Revolut needed to intervene.
But by the time the fourth payment was processed, this was the eighth time Miss T had tried to pay a high-risk cryptocurrency merchant and the payment was for £3,690, which should have raised concerns. So, think Revolut missed an opportunity to intervene.

What kind of warning should Revolut have provided?
Scams involving cryptocurrency have become increasingly diverse, and given the prevalence of 'employment scams' we'd expect it to have both questions and warnings tailored towards the key risks of those scams. I would expect Revolut to have provided a 'better automated warning', asking Miss T a series of questions to try and establish the actual scam risk. There's no evidence Miss T had been coached to lie and so I'm satisfied

she'd have answered the questions honestly, which would have enabled Revolut to have provided a written warning tailored to employment scams.

If Revolut had provided a warning of the type described, would that have prevented the losses Miss T suffered from the fourth payment?

If Miss T had been given a warning which was tailored to employment scams, I think this would have stopped the scam. Payment four occurred on the second day of the scam and so Miss T wouldn't have been so far into the process that she felt she had no choice other than to proceed to recover her funds, and a properly tailored warning would have matched with the circumstances of the scam. Significantly, there's no evidence she was being guided by the scammer in terms of her communications with Revolut or that she'd ignored any warnings from Bank L. And as she was already concerned that she didn't have enough money, I've no reason to think she wouldn't have listened to a warning from Revolut, particularly as she ultimately stopped making payments as soon as she'd was alerted to the scam by her partner.

Is it fair and reasonable for Revolut to be held responsible for Miss T's loss?

I've set out in some detail above, I think that Revolut should have recognised that Miss T might have been at risk of financial harm from fraud when she made the fourth payment, and in those circumstances, it should have declined the payment and provided a better automated warning. If it had taken those steps, I am satisfied it would have prevented the losses Miss T 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 Miss T's own account does not alter that fact and I think Revolut can fairly be held responsible for Miss T'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 Miss T 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 Miss T could instead, or in addition, have sought to complain against those firms. But Miss T 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 Miss T'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 Miss T's loss from the fourth payment (subject to a deduction for Miss T's own contribution which I will consider below).

Should Miss T bear any responsibility for their losses?

I accept Miss T was actively seeking work and this is why the call from A didn't seem suspicious. I also accept A's website was sophisticated and the scammer seemed knowledgeable and articulate, which further persuaded Miss T the opportunity was genuine. She was also presented with online screens that appeared to show her commission and she had access to her account, giving her a sense of control over her funds.

However, Miss T considered whether the opportunity was a scam at the outset and so she should have acted on this before agreeing to send funds to the scam. The commission she believed she was being paid was high for a job which didn't require qualifications or an interview and in respect of which she didn't receive any employment documents, and in those circumstances its unreasonable that she didn't do anything to check what she was told by the scammer. Further, she ought to have questioned why she was being asked to use cryptocurrency to pay for tasks which she was expecting to be paid for.

By the time Miss T made the payments, there was a lot of information online about job scams which Miss T would have seen if she'd done some simple research. There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence, and, in the circumstances, I don't think Miss T did enough to protect herself. Consequently, I agree with our investigator that the settlement should be reduced by 50% for contributory negligence.

Compensation

I've thought carefully about everything that has happened, and with all the circumstances of this complaint in mind, I don't think Revolut needs to pay any compensation given that I don't think tit acted unreasonably when it was made aware of the scam.

Recovery

Miss T has described that she paid an account in his own name and from there the funds were moved to an online wallet in the scammer's control, so I'm satisfied there was no prospect of a successful recovery.

My final decision

My final decision is that Revolut Ltd should:

- refund the fourth payment.
- 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 Miss T with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 5 December 2024.

Carolyn Bonnell
Ombudsman