DRN-4817167

The complaint

Mr H complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by a job scam, or to help him recover the money once he'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.

Mr H was approached on WhatsApp by a someone I'll refer to as the scammer who claimed to work for a recruitment company, which I'll refer to as "K". The scammer told Mr H about an opportunity to work from home by reviewing products to improve their ratings on the platform.

Mr H had been looking for work and so the fact he'd been approached didn't raise concerns. He searched for K on google and didn't see any negative reviews. He looked at K's website and was satisfied it seemed genuine, and he was also added to a WhatsApp group with others doing the same job. The scammer explained he could earn commission after a set of 20-30 tasks which could be between 1% and 4% per task, depending on the level of the task.

The scammer explained Mr H would be required to purchase tasks using cryptocurrency purchases from P2P sellers (to simulate buying the item) which would then be deposited to the platform. Between 22 May 2023 and 3 July 2023, he made eight faster payments from his Revolut account to five beneficiaries totalling £7,865.59. He borrowed money from friends and family and the funds were credited to Revolut from his account with Bank B.

Mr H realised he'd been scammed when he asked to make a withdrawal and was told he hadn't completed the set within the timeframe and would need to pay £5,000 to top up the account or he'd lose his funds. He complained to Revolut, but it refused to refund any of the money he'd lost, so he complained to this service with the assistance of a representative.

The representative said the pattern of payments was typical for this type of scam and should have been seen as high risk. And if Revolut had intervened, he'd have said he was approached on social media, he was sending cryptocurrency to pay for tasks, and he had no employment contract. They said he couldn't remember why he chose 'transfer to safe account" when asked for the payment purpose, but the selection should have raised concerns that he was being scammed.

Revolut said the account was opened on 22 May 2023 and Mr H declared the purpose of the account was 'overseas transfers and crypto, scheduling payments, spending abroad, vaults, invest in gold and silver, budgeting, stocks, cashback, accounts overview, stays, foreign exchange, smart delay, and rewards. It said the transactions fell within the account purpose declaration and each time he paid a new beneficiary he was warned about the risks he could face if he decided to proceed with the transfer and that he may not be able to recover the funds if the beneficiary was fraudulent.

It said the first warning was triggered when Mr H transferred £826 on 2 July 2023. He chose 'transfer to a safe account' and had to go through educational story messages before continuing with the payment. The next four payments triggered similar warnings.

Revolut said Mr H was committed to proceed with the transactions regardless of the warnings and the opportunity to stop and reflect before determining whether to proceed. It said its interventions were proportionate to the risk and if Mr H was more truthful, it could have taken a different course of action. It also said there was an element of contributory negligence because Mr H received a WhatsApp message, which wouldn't have been sent by a genuine recruitment agency, and a Google search of K shows concerning results.

Our investigator felt the complaint should be upheld. She accepted the account was newly opened and so there wasn't a spending history to compare the payments with, and she didn't think the first two payments were concerning because they were relatively low value and weren't sent in quick succession. But she thought Revolut ought to have been concerned when Mr H selected 'transfer to a safe account' when asked to give a payment purpose.

Our investigator explained that each time he selected this payment purpose, Mr H was given warnings relevant to safe account scams, which she didn't think was sufficient. She thought Revolut ought to have contacted Mr H and made further enquiries before allowing it and the subsequent payments to be made.

Our investigator noted that Mr H had received a cryptocurrency scam warning from B on 3 July 2023 and that he sent a copy of the warning to the scammer who said, *'this is just a warning and an important note. Some of the merchants in B are also scammers in buying or selling coins'.* She accepted this showed the scammer was guiding Mr H, but she didn't think it was evidence of him having been told to lie, so she thought a better intervention would have detected the scam. She further explained that the communications between Mr H and the scammer showed he'd tried to contact Revolut when he encountered an issue on the cryptocurrency platform, but he was later enticed back by the scammer. She felt that if Revolut had done more when he made the third payment, he'd have reacted positively because he was already on alert following issues with the first payment.

So, she was satisfied Revolut could have stopped the scam and that it should therefore refund the money he'd lost from the third payment onwards. However, she thought the settlement should be reduced by 50% for contributory negligence because even though Mr H had been looking for work, he was contacted on WhatsApp, which ought to have raised concerns. She also felt the commission was too good to be true - if he worked five days, he could earn around £640 - for such a simple task which required no experience. And she noted he'd borrowed money to fund the payments and had ignored a relevant warning from B. So, she didn't think he'd taken reasonable care before he made the payments.

Revolut has asked for the complaint to be reviewed by an Ombudsman. It maintains Mr H wasn't truthful when he selected the payment purpose, and he went ahead with the payments despite a scam warning from B, so a further intervention wouldn't have made a difference.

It has also cited the Supreme Court's judgment in Philipp v Barclays Bank UK plc where the Court held that in the context of authorised push payment fraud, where the validity of the instruction is not in doubt, "no inquiries are needed to clarify or verify what the bank must do. The bank's duty is to execute the instruction and any refusal or failure to do so will prima facie be a breach of duty by the bank."

It maintains it has adequate systems and controls in place to detect unusual or suspicious transactions, but given the payments went to a legitimate cryptocurrency platform in Mr H's name, it didn't have enough details to detect the transactions were suspicious. It has also stated that it is an Electronic Money Institute ("EMI") and it's not uncommon for customers to engage in transactions involving digital assets, especially as he declared 'crypto' and 'transfers' as the purposes of the account. So, the payments weren't out of character with the typical way in which an EMI account is used.

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 Mr H 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 Mr H 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 July 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 July 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 Mr H was at risk of financial harm from fraud?

Mr H was presented with a new payee warning each time he paid a new beneficiary, and he was required to give a payment purpose for payments three to six. Each time, he said he was transferring funds to a safe account and was then given warnings relevant to the selection which stated that Revolut or other banks wouldn't tell customers to transfer funds to a new safe account.

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

I've considered whether this was a proportionate response considering the payment purpose Mr H selected, and I don't think it was. Even though the transfers weren't identifiably for cryptocurrency, any suggestion from a consumer that they are sending funds to a safe account should reasonably indicated that they are at risk of fraud, and I don't think the warning he was presented with were proportionate to the risk presented.

I accept Mr H selected the wrong payment purpose and this stopped Revolut from identifying that he was sending funds to a job scam, but I agree with our investigator that it ought to have contacted him via its live-chat facility and asked him why he was moving money to a safe account. Had it done so, I there's no evidence he was coached to lie (the scammer wouldn't have told him to say he was sending money to a safe account and so its most likely he just selected the first option he saw, and I agree that sending the warning to the scammer on 3 July 2023 isn't the same as being coached to lie) and as he believed the job was genuine, I'm satisfied he'd have said he was buying cryptocurrency to pay for tasks in return for which he expected to be paid commission.

With this information, Revolut should have identified that Mr H was falling victim to a scam and provided a tailored warning and information about how to confirm the opportunity was a scam, which would be relatively straightforward as there is lots of information about job scams online. As our investigator has described, there's evidence that Mr H had doubts early on and, while I accept he was presented with a warning on 3 July 2024, this warning wasn't tailored to job scams and the scammer's explanation was plausible, so I'm satisfied he'd have listened to some robust and relevant advice from Revolut, and, ultimately, decided not to make any further payments.

Is it fair and reasonable for Revolut to be held responsible for Mr H's loss?

As I've set out above, I think that Revolut should have recognised that Mr H might have been at risk of financial harm from fraud when they made the third payment, and in those circumstances, it should have made further enquiries before processing it. If it had done that, I am satisfied it would have prevented the losses Mr H 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 Mr H's own account does not alter that fact and I think Revolut can fairly be held responsible for his 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 Mr H 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 Mr H could instead, or in addition, have sought to complain against those firms. But Mr H 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 Mr H'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 Mr H's loss from the third payment (subject to a deduction for Mr H's own contribution which I will consider below).

Should Mr H bear any responsibility for his loss?

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.

Mr H had been looking for work and so I don't think it's unreasonable that he didn't raise questions when the scammer initially contacted him. However, I think he should reasonably have questioned why he was being asked to make payments in cryptocurrency for tasks he expected to be paid for and whether the commission was realistic, considering the role required no experience or training and he wasn't given any employment documents.

Having considered the circumstances of this scam, I'm satisfied it was sophisticated, I don't think it was unreasonable for Mr H to have thought it was genuine and the warning he was shown on B's platform wasn't relevant to job scams. But there's plenty of information available online which could have alerted him to the scam, and the evidence shows he had concerns at the outset, so if he'd acted on those concerns, his loss could have been prevented. So, I think the settlement should be reduced by 50% for contributory negligence.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr H paid an account in his own name and moved the funds onwards from there.

Compensation

The main cause for the upset was the scammer who persuaded Mr H to part with his funds. I haven't found any errors or delays to Revolut's investigation, so I don't think he is entitled to any compensation.

My final decision

My final decision is that Revolut Ltd should:

- refund the money Mr H lost from the fourth payment onwards.
- 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 deducts tax in relation to the interest element of this award it should provide Mr H with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 8 January 2025.

Carolyn Bonnell
Ombudsman