DRN-4898943

The complaint

Mr S complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by an investment 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 S received a text message from someone who claimed to work for a recruitment company, who I'll refer to as "the scammer". The scammer told him about an opportunity to earn money by creating hotel reviews. He was encouraged to join a 'Google ads review scheme' which would enable him to earn commission on each hotel review and told it would be a commitment of one to two hours a day.

Mr S understood he would be required to complete one to three 'sets' of ads every day and that he would need to 'seed fund' the work using cryptocurrency, which would be returned when he withdrew the commission upon completion of a 'set' of ads.

He researched the recruiter's name and the company website and was initially asked to make small payments, which he felt comfortable with, and which allowed him to become familiar with the process. He was also encouraged to join a group of people who were doing the same job, which reassured him the job was legitimate.

The scammer told him to first purchase cryptocurrency through a cryptocurrency exchange company which I'll refer to as "L" and then load it onto an online wallet. He transferred money from an account held with Bank H to Revolut, and on 25 August 2023 he made three faster payments for £1,271.98, £3,210.01, and £2,489.84 to L.

Mr S contacted Revolut later the same day when the payments he was asked to make began to grow in value and the scammer's tone changed, at which point he realised he'd been scammed. But Revolut refused to refund any of the money he'd lost, stating it had sought recovery of the funds, but no funds remained.

It said its systems had detected that Mr S was paying a new beneficiary and the following message was displayed in his Revolut app: "*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".* Mr S acknowledged the warning and was free to continue with the transfer. He was also shown educational screens regarding the type of potential scam.

Mr S wasn't satisfied and so he complained to this service questioning why he couldn't be reimbursed under the Contingent Reimbursement Model ("CRM") Code. He said he accepted he was shown warnings in the app, but he didn't think they were sufficient.

Revolut said the account was opened on 19 May 2018, and Mr S had selected foreign exchange, spending abroad, overseas transfers, budgeting, rewards and transfers as the

account purposes. He was given one generic and three specific warnings when he set up the new payee, including a warning that he might not be able to recover the funds if the beneficiary was fraudulent. After he acknowledged the warning, the transaction was held, and Mr S received a set of dynamic educational story messages to warn him about the risks associated with the payment.

He was also asked about the purpose of the payment, and he responded “cryptocurrency” which resulted in him receiving a further warning that there was a high probability that the payment was a scam. He was also provided with tailored warnings, after which he decided to proceed with the payment.

Revolut said Mr S was initially suspicious because he asked the scammer how they got his number, and when asked for his personal details, he provided them reluctantly, asking for them not to be shared.

It also argued that the funds were transferred to Mr S’ cryptocurrency account and from there a fraudulent external wallet and the CRM code didn’t apply.

Our investigator felt the complaint should be upheld. He thought Revolut ought to have been concerned about the second payment because it was a high value payment to a cryptocurrency merchant. He accepted Mr S was presented with tailored warnings based on the payment purpose he’d selected, but he thought Revolut should have asked him questions about the payment and tried to identify the specific scam risk. It should also have provided a warning which covered off the key features of the scam risk, such as making payments to gain employment, being paid for ‘clicks’, ‘likes’ or promoting products and not being able to withdraw funds.

Had it done so, as there was no evidence Mr S had been coached to lie, he was satisfied he’d have explained the purpose of the payments and the scam would have been exposed. He also felt it was likely he’d have listened to the warnings because they would have resonated with his situation and his loss would have been prevented. So, he thought it should refund the money Mr S lost from the second payment onwards.

However, he thought Mr S should have been concerned that he’d been approached via text message, he wasn’t given any employment documents, and he was having to use his own money when the whole purpose of a job is to earn money. So, he thought the settlement should be reduced by 50% for contributory negligence.

Finally, our investigator explained there had been no chance of a successful recovery because Mr S had paid an account in his own name and the funds had been moved on from there. And he didn’t think he was entitled to any compensation because the main cause of the upset was the scammers who persuaded him to part with his money.

Both parties have asked for the complaint to be reviewed by an Ombudsman. Mr S has argued that Revolut should have to adhere to the CRM Code, and it should have done more to recognize and stop suspicious payments.

Revolut has argued that Mr S was given warnings on three occasions and that the interventions were proportionate considering the value of the payments and the fact he was paying an account in his own name.

It has argued that a small proportion of payments to cryptocurrency merchants are reported as fraudulent and don’t justify treating all payments to cryptocurrency platforms as suspicious. And to apply the reimbursement rules to self-to-self transactions is an error of law because they are distinguishable from transactions subject to the regulatory regime

concerning APP fraud because customers have transferred funds to their own account with a third party and it is merely an intermediate link.

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.

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.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr S says he's fallen victim to, in all but a limited number of circumstances. But Revolut isn't a signatory to the code.

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 S 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 S 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 August 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:

- 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 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.

---

[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_/

- The October 2017, BSI Code[3], 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[4], 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"*[5].
- 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 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

[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"
[4] 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.
[5] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

- 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 S was at risk of financial harm from fraud?

When Mr S set up the new payee, he was shown a generic warning which asked whether he knew and trusted the payee and warned he might not be able to get the money back if the payment turned out to be fraudulent. He was also shown more specific warnings including education story messages, a warning that the payment was probably a scam and a tailored warning. I've considered whether these warnings were proportionate to the risk, and, considering payments to cryptocurrency merchants should attract greater scrutiny, I don't think they were.

The first payment was slightly higher than previous payments on the account, but it wasn't so high that Revolut needed to intervene and so I'm satisfied it did act proportionately in respect of that payment. But the second payment was for an amount which ought to have raised concerns because (Mr S hadn't made any high value payments from the account in the months prior to the scam), it brought the cumulative spend for the day to £4,481.97 and Mr S was paying a cryptocurrency exchange having never previously paid a cryptocurrency merchant.

What kind of warning should Revolut have provided?

I agree with our investigator that Revolut ought to have asked Mr S why he was making the payments, whether there was a third party involved, and if so, how he'd met them, whether he'd been promised unrealistic returns, whether he'd made any withdrawals, whether he'd done any due diligence and whether he'd been advised to make an onwards payment from the cryptocurrency exchange.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr S suffered?

There's no evidence Mr S had been coached to lie and so I'm satisfied he'd have described the circumstances of the job, including how he'd been contacted, the fact he hadn't received any employment documents and the fact he'd been told to make payments in cryptocurrency to seed fund tasks he expected to earn commission on. With this information, I'm satisfied Revolut would have easily detected the scam and gone on to provide tailored warnings about the particular scam type, including advice on additional due diligence and specific information such as common red flags which would by indictive of a job scam.

Had it done so, I'm satisfied Mr S would have listened to and acted on the advice he was given. This is because there's no evidence he ignored any advice from his other bank and as I've explained, I don't think the warnings he'd had from Revolut were sufficient to draw the scam risk to his attention. Further, I think it's significant that Mr S realised he'd been scammed very shortly after he made the payments, and that he acted so decisively on his suspicions when he was asked to make larger payments and the scammer's tone changed. So, I think it's unlikely that he'd have made any further payments to the scam.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr S purchased cryptocurrency which credited an e-wallet held in his own name, rather

than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

I think that Revolut still should have recognised that Mr S might have been at risk of financial harm from fraud when he made the second payment, and in those circumstances, it 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 Mr S 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 S's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr S'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 S 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 S could instead, or in addition, have sought to complain against those firms. But Mr S 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 S'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 S's loss from the second payment (subject to a deduction for Mr S's own contribution which I will consider below).

Should Mr S bear any responsibility for his own 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.

There were several red flags present which I think ought reasonably to have caused Mr S to think more carefully about what he was being asked to do by the scammer. He was contacted out of the blue by someone who claimed to be offering him a job opportunity, and yet he was required to make payments in cryptocurrency to before he could withdraw any commission. Further, he wasn't given any employment documents and was told he could increase his commission simply by adding more seed funding.

Revolut has argued that Mr S had expressed concerns when he was initially contacted and that he was reluctant to give his personal details to the scammer, and, in the circumstances, I agree that it was unreasonable for him not to have acted on those concerns and taken more care to check the opportunity was legitimate. Consequently, and weighing up the fault on both side, 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 they acted unreasonably when they were made aware of the scam. And, he wasn't entitled to compensation for legal fees, as our service is free to access.

Recovery

Mr S has described that he 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 money Mr S lost from the second 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 Ltd deducts tax in relation to the interest element of this award it should provide Mr S with the appropriate tax deduction certificate.

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

Carolyn Bonnell
Ombudsman