DRN-4515007

Complaint

Ms R is unhappy that Revolut Ltd didn't reimburse her after she fell victim to a scam.

Background

In June 2023, Ms R fell victim to a scam. She was contacted on a messaging app by someone who claimed to be a recruitment consultant. They asked if she was looking for work and told her they could offer her a job opportunity that was flexible and remote. She would be asked to carry out tasks on a software platform maintained by the client. These tasks involved submitting product ratings. The premise was that her activity on the client's platform would indirectly simulate demand for those products which would give them better visibility in digital marketing efforts. Unfortunately, this wasn't a legitimate job opportunity. Ms R had been contacted by a fraudster.

She was told that she would be paid based on the number of tasks that she completed on the platform. However, to participate she needed to deposit funds into her account. She did this in the anticipation that she'd be able to earn that money back with her commission payments from the employer.

She used her Revolut account to make the payments in the table below. Payees A, B and C were private individuals. Payee D was a third-party cryptocurrency firm.

	Date	Payee	Value
1	14-Jun-23	Payee A	£8.64
2	15-Jun-23	Payee B	£43.25
3	15-Jun-23	Payee C	£43.47
4	15-Jun-23	Payee A	£86.65
5	16-Jun-23	Payee D	£173.22
6	16-Jun-23	Payee D	£257.13
7	17-Jun-23	Payee D	£1,281.75
8	17-Jun-23	Payee D	£341.80
9	17-Jun-23	Payee D	£811.78
10	17-Jun-23	Payee D	£811.78
11	17-Jun-23	Payee D	£845.96
12	17-Jun-23	Payee D	£803.23
13	17-Jun-23	Payee D	£1,709.00
14	17-Jun-23	Payee D	£3,417.99
15	17-Jun-23	Payee D	£1,794.44
16	17-Jun-23	Payee D	£4,101.58
17	17-Jun-23	Payee D	£1,811.53
18	19-Jun-23	Payee D	£4,013.12
19	19-Jun-23	Payee D	£3,244.06
20	19-Jun-23	Payee D	£1,707.70

21	22-Jun-23	Payee D	£8,000.28
22	22-Jun-23	Payee D	£3,880.85
23	22-Jun-23	Payee D	£1,893.26

Once she realised that she'd fallen victim to a scam, Ms R notified Revolut. It appears to have contacted her via her professional representative to request further information relating to the complaint. Revolut says that, as no reply was received, it wasn't able to carry out an investigation and issue a response. At that point, it says that it couldn't be sure that a scam had occurred.

In any event, Ms R's representatives eventually referred the complaint to this service. It was looked at by an Investigator who gathered the relevant evidence. The Investigator was persuaded that Ms R had fallen victim to a scam and recommended that Revolut refund her losses in part. She thought that Revolut ought to have spotted the risk that Ms R was falling victim to a scam at the time she asked it to make payment 13 in the table above. Revolut shouldn't, in the Investigator's view, have processed that payment without first making enquiries with Ms R to ensure that she wasn't at risk of financial harm due to fraud. Nonetheless, the Investigator concluded that it was fair and reasonable for her to bear some responsibility for her own losses by way of contributory negligence.

Revolut disagreed with the Investigator's opinion. It said:

- The Investigator had wrongly assumed Revolut owed a duty to Ms R to prevent fraud.
- Ms R made payments to an e-wallet held with a cryptocurrency platform. That e-wallet was in her own name. As she was paying her own account, this doesn't meet the definition of an authorised push payment (APP) fraud as set out in the DISP rules.
- The cryptocurrency firm appears to have had a robust process for verifying customers before allowing them to purchase cryptocurrency.
- Ms R didn't do adequate due diligence before going ahead with these payments.

As Revolut disagreed with the Investigator's view, the complaint has been passed to me to consider and come to a final decision.

Findings

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 customer'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 R 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 R 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 June 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or undertaken 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.

---

[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_/

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 *"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 [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 June 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

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

- 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 R was at risk of financial harm from fraud?

I accept that Revolut was in a more difficult position in respect of detecting fraud risk than, for example, a high street bank. It needed to be on the lookout for account activity that was unusual or out of character to the extent that it indicated a fraud risk. Ms R already had a Revolut account, but it doesn't appear to have been used much. As a result, Revolut didn't have any meaningful data to serve as a basis of comparison.

Nonetheless, I still think it was clear that there was a significant risk of fraud here. The Investigator identified payment 13 as the point at which any concerns on Revolut's part should've resulted in action. I'd agree with that conclusion. By processing that payment, Ms R had transferred over £7,000 to a new payee in less than 48 hours. There were other concerning factors too. The payments were rapidly increasing in value – payment 13 was ten times bigger than payment 5, for example. Furthermore, if this had been legitimate activity, it's not clear why Ms R would transfer funds to the payee by making frequent smaller payments, rather than making fewer large payments. Such a pattern is in keeping with this type of scam. By the time she'd transferred such a large amount of money in a manner consistent with that pattern, Revolut ought to have been concerned.

I've considered that most of the payments were transfers to a cryptocurrency platform. Those funds were placed into an e-wallet in Ms R's name. The first four payments were made to private individuals and so are an exception. I've taken that into consideration when deciding whether Revolut needed to take any action here. From the evidence I've seen, it's not clear to me that Revolut could've known much about the destination of the payments. The IBAN is associated with a PSP that does more than just process payments for a cryptocurrency firm. Furthermore, although it appears it knew the name of the ultimate recipient of the funds, it's not a particularly well-known cryptocurrency exchange.

In other words, although knowing that a payment was destined for a cryptocurrency platform is a relevant factor when weighing up the fraud risk associated with an individual payment, I can't see that Revolut would've been aware of the risk with these particular payments. It also means that Revolut wouldn't have known that the destination of those payments was an e-wallet in Ms R's name. The payment instructions were to pay an account belonging to a limited company that operated the cryptocurrency platform. Revolut couldn't, therefore, have factored in that the funds weren't leaving Ms R's control when assessing fraud risk.

Taking all of this into account, I'm satisfied that Revolut ought fairly and reasonably to have recognised that Ms R could be at an increased risk of fraud when making these payments. It should have had appropriate systems for making checks and delivering warnings before

processing them. And, as I have explained, Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

As far as I can see, Revolut didn't take any steps to warn Ms R about this payment. Having thought carefully about the risk Payment 13 presented, I think a proportionate response would have been for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Ms R's account. I think it should have done this by, for example, directing Ms R to its in-app chat to discuss the payment further.

If Revolut had attempted to establish the circumstances surrounding payment 13, would that have prevented the losses Ms R suffered?

If Ms R had told Revolut that she was making the payments to enable her to work online, it would've swiftly recognised that she was in the process of falling victim to a scam. It could, therefore, have provided her with a clear and unambiguous warning about job scams. Ms R would've had nothing to gain from going ahead with the payments, so it's likely she would've stopped following the fraudster's instructions and her subsequent losses would've been prevented.

The question I have to consider, therefore, is whether she would've revealed why she was making these payments. She's told me that she wasn't asked to provide a cover story should the payments be questioned. There's also nothing that contradicts this in the messages I've seen between her and the fraudster. Ultimately, as Revolut didn't question payment 13, it can provide no compelling evidence that she would've misled it about its purpose or the surrounding circumstances.

Once it had established why Ms R was making these payments, Revolut should've provided her with a clear warning that explained the prevalence of job scams, how they operate and that (except perhaps in very rare circumstances) no legitimate employer would ask an employee to pay for the ability to work, let alone do so using cryptocurrency. I think, on the balance of probabilities, that's likely to have caused Ms R to stop. I can see no reason for her to have continued to make the payment if she was presented with a warning of this nature.

I'm satisfied that, had Revolut established the circumstances surrounding Payment 13, as I think it ought to have done, and provided a clear warning, Ms R's loss from and including Payment 13 would have been prevented.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Revolut wasn't the point of Ms R's loss. She was paying her own account and needed to take further steps to transfer those funds into the control of the fraudster.

Revolut has pointed out that that means this doesn't constitute an APP scam as defined in the DISP rules. I'm not persuaded that's relevant to the outcome. The DISP rules contain a definition of an APP scam for the purpose of delineating this service's jurisdiction over a specific type of complaint. I don't think it has any bearing on whether Revolut acted fairly and reasonably in its dealings with Ms R.

As I've set out above, I think that Revolut still should have recognised that Ms R might have been at risk of financial harm from fraud when she made payment 13, 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 she

suffered. The fact that the money used to fund the scam wasn't lost at the point it was transferred to Ms R's own account does not alter that fact and I think Revolut can fairly be held responsible for her 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 R 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 R could instead, or in addition, have sought to complain against those firms. But she has not chosen to do that, and I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Ms R's compensation in circumstances where: she has only complained about one respondent from which she is entitled to recover her 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 have been) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Ms R's loss from payment 13 (subject to a deduction for Ms R's own contribution which I will consider below).

Should Ms R bear any responsibility for her 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. I recognise that Ms R's belief that this was a legitimate job opportunity was sincerely held, but I'm not persuaded that it was a reasonable one. It was presented to her following unsolicited contact on a messaging platform. There was no formalisation of the arrangement between her and the employer – for example, there was no written contract and indeed no clear setting out of the terms of her employment.

In addition to that, the arrangement was an inversion of the normal employer-employee relationship. In most circumstances, people expect to be paid by their employer, rather than the other way around. As far as I can see, there wasn't really any attempt to explain this unusual arrangement and Ms R doesn't appear to have asked about it. I think she ought to have proceeded only with great caution. Overall, I think it's fair and reasonable for Revolut to make a 50% deduction from the redress payable to her.

Final decision

For the reasons I've set out above, I uphold this complaint. If Ms R accepts my final decision, Revolut needs to refund 50% of her losses from payment 13 onwards. It also needs to add 8% simple interest per annum to those payments calculated to run from the date the payment debited her account until the date any settlement is paid to her.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 10 January 2025.

James Kimmitt
Ombudsman