DRN-5542918

The complaint

Miss F complains that Revolut Ltd won't refund money she lost to a scam.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything again here. In brief, Miss F fell victim to a fake job scam after she was approached about a job opportunity on social media. She was told she would be paid for completing a number of tasks, but she would have to pay in funds to the task platform first. In total, Miss F made 50 payments to the scam, these were a mixture of payments direct to cryptocurrency providers, payments to her own accounts elsewhere (from where the funds were again used to buy cryptocurrency) and payments to third parties. She made payments totalling over £40,000. I've set the payments out below.

Payment	Date	Payee	Payment type	Amount
1	13/07/2023	Miss F's bank account	Transfer	£310
2	14/07/2023	Cryptocurrency exchange	Transfer	£240
3	14/07/2023	Cryptocurrency exchange	Transfer	£180
4	15/07/2023	Cryptocurrency exchange	Transfer	£500
5	15/07/2023	Cryptocurrency exchange	Transfer	£1,000
6	16/07/2023	Cryptocurrency exchange	Transfer	£500
7	16/07/2023	Cryptocurrency exchange	Transfer	£1,500
8	17/07/2023	Cryptocurrency exchange	Transfer	£180
9	17/07/2023	Cryptocurrency exchange	Transfer	£800
10	19/07/2023	Miss F's bank account	Transfer	£290
11	20/07/2023	Cryptocurrency exchange	Transfer	£2,000
12	20/07/2023	Cryptocurrency exchange	Transfer	£1,500
13	22/07/2023	Cryptocurrency exchange	Transfer	£2,000
14	22/07/2023	Cryptocurrency exchange	Transfer	£2,000
15	22/07/2023	Cryptocurrency exchange	Transfer	£1,000
16	22/07/2023	Cryptocurrency exchange	Transfer	£1,160
17	24/07/2023	Cryptocurrency exchange	Transfer	£2,000
18	24/07/2023	Cryptocurrency exchange	Transfer	£1,980
19	24/07/2023	Cryptocurrency exchange	Transfer	£1390
20	25/07/2023	Miss F's bank account	Transfer	£35
21	26/07/2023	Cryptocurrency exchange	Transfer	£100
22	30/07/2023	Cryptocurrency exchange	Transfer	£830
23	02/08/2023	Cryptocurrency exchange	Card payment	£830
24	08/08/2023	Cryptocurrency exchange	Transfer	£900
25	08/08/2023	Cryptocurrency exchange	Transfer	£500
26	08/08/2023	Payee 1	Card payment	£593.34
27	08/08/2023	Payee 1	Card payment	£20.46
28	09/08/2023	Miss F's bank account	Transfer	£1,000
29	09/08/2023	Miss F's bank account	Transfer	£500
30	09/08/2023	Cryptocurrency exchange	Card payment	£500
31	09/08/2023	Miss F's bank account	Card payment	£20.08

32	11/08/2023	Miss F's bank account	Transfer	£980
33	14/08/2023	Payee 2	Card payment	£860
34	16/08/2023	Miss F's bank account	Transfer	£870
35	17/08/2023	Miss F's bank account	Transfer	£1,200
36	18/08/2023	Miss F's bank account	Transfer	£200
37	19/08/2023	Miss F's bank account	Transfer	£1,000
38	20/08/2023	Miss F's bank account	Transfer	£1,000
39	20/08/2023	Miss F's bank account	Transfer	£170
40	21/08/2023	Miss F's bank account	Transfer	£850
41	24/08/2023	Miss F's bank account	Transfer	£830
42	27/08/2023	Miss F's bank account	Transfer	£1,000
43	27/08/2023	Miss F's bank account	Transfer	£1,000
44	27/08/2023	Miss F's bank account	Transfer	£1,000
45	27/08/2023	Miss F's bank account	Transfer	£500
46	28/08/2023	Cryptocurrency exchange	Transfer	£1,000
47	29/08/2023	Cryptocurrency exchange	Transfer	£500
48	31/08/2023	Cryptocurrency exchange	Transfer	£780
49	20/09/2023	Miss F's bank account	Card payment	£400
50	22/09/2023	Cryptocurrency exchange	Transfer	£750

Miss F realised she had been scammed when she was unable to withdraw any profits, and reported the scam to Revolut.

Revolut didn't consider it had any responsibility for Miss F's loss. It said she had authorised all the payments, and that it had provided her with appropriate warnings. Revolut also argued it had no duty to prevent fraud and scams.

Our Investigator upheld the complaint in part. They thought that Revolut ought to have questioned Miss F in more detail about the 14th payment she made to the scam. The investigator thought that, had that happened, the scam would likely have been stopped. So, the investigator said that Revolut should refund the money Miss F had lost from this payment onwards, less a deduction of 50% in recognition of Miss F's own contributory negligence.

Revolut disagreed, so the matter has been escalated to me to determine.

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 Miss F 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 Miss F 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]

---

[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_/

- 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 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).
- Since 31 July 2023, under the FCA's Consumer Duty[5], 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

---

[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 some of the payments that are the subject 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"
[5] 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.

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"*[6].

- 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 Miss F was at risk of financial harm from fraud?

Miss F's Revolut account had been open for some time before this scam took place, but had not been used since September 2022. So, Revolut had a limited account history against which to compare the payments Miss F was making. And the initial payments Miss F made were small, so even though they were evidently payments to purchase cryptocurrency, I don't think these payments would have been an immediate cause for concern. Revolut did provide Miss F with some written warnings about some of these early payments, but given their values and the answers Miss F gave to Revolut's automated questions, I don't think more direct intervention was warranted.

However, by the time of the 14th payment to the scam, I think a pattern was emerging which should have flagged to Revolut that something untoward could be going on, and so led to it intervening in a more direct way. I say this because, by this stage, it was clear that Miss F was making increasing large and frequent payments to a payee associated with

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

cryptocurrency. And the 14th payment was the second large payment in a day to that cryptocurrency payee, with a total value sent that day of £4,000.

Given how cryptocurrency exchanges generally operate, I think Revolut could have reasonably assumed that payments Miss F was making would be to a cryptocurrency wallet held in her own name. But by July 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. And by July 2023, when these payments took place, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Miss F made in July 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

So, considering that by the time of the 14th payment Miss F made to the scam a pattern had emerged of increasing payments within a short period of time, and given what Revolut knew about the destination of the payments, I think that the circumstances should have led Revolut to consider that Miss F was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have taken steps to intervene directly in this payment before allowing it to go ahead.

What did Revolut do to warn Miss F and what should it have done?

Revolut did intervene in some of the payment Miss F made to the scam. On various occasions it asked her the purpose for payments she was making and then provided her with scam warnings relating to the payment purposes she selected. Given the limited scope of these warnings, and that at the time there was no clear option for Miss F to select a payment purpose that specifically related to the scam she was falling victim to (a job scam), I don't think these warnings could reasonably be expected to have put Miss F on notice that she was at risk of falling victim to a scam.

However, as explained above, by the time of the 14th payment to the scam, I think Revolut should have realised the potential risk posed by the payments Miss F was making, and so taken further steps to intervene.

I've thought carefully about what a proportionate intervention in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's primary duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, in line with what I consider to have been good industry practice at the time, as well as what I consider to be fair and reasonable when Miss F attempted to make Payment 14, to have attempted to establish the circumstances surrounding this payment before allowing it to debit Miss F's account.

If Revolut had attempted to establish the circumstances surrounding Payment 14, would the scam have come to light and Miss F's loss from that point on been prevented?

I've considered this point carefully. I've not seen anything to suggest that Miss F was given any cover story to use regarding the payments she was making, so I consider it very likely that, had Revolut asked her, Miss F would have been open and honest about what she was making the payments for – payments to cryptocurrency to fund a job. I note that Miss F selected various different reasons for the payments she was making, but I don't think this was as a result of any intentional dishonesty, given that the specific scam she was falling victim to was not clearly represented in the options presented to her.

I think it is likely that if Revolut had asked Miss F directly what the payment she was making was for she would have explained it was for crypto currency as part of a job promoting businesses online. And given that this is not a standard way that one would expect a job to operate, I think that would have been a clear red flag to Revolut that Miss F was at risk of financial harm, and it would have been able to explain this risk to Miss F. I think it's likely she would then have realised she was most likely being scammed and would not have proceeded with any more payments. I can also confirm that I have not seen any evidence that the other financial institutions involved in the payment journey intervened in this direct way, so there is nothing to suggest that Miss F would have not responded honestly to such intervention or that she would have ignored any direct warning about job scams had it been provided.

So, in summary, I consider that it Revolut had intervened more appropriately at the time of payment 14 then it could have prevented Miss F's loss from that point onwards.

Is it fair and reasonable for Revolut to be held responsible for Miss F's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Miss F transferred her funds to Revolut from her main bank account provider, before using the funds to buy cryptocurrency which was passed on to the scammer. I also note that some of her losses to the scam were first sent from Revolut to other banks, before being moved on to the cryptocurrency exchange and then on to the scammer.

But as I've set out above, I think that Revolut still should have recognised that Miss F might have been at risk of financial harm from fraud when she made the 14th payment to the scam, 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 Miss F suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred out of Miss F's Revolut account does not alter that fact and I think Revolut can fairly be held responsible for Miss F'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 F 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 F could instead, or in addition, have sought to complain against those firms. But Miss F has not chosen to do that and ultimately, 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 Miss F'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 F's loss from the 14th payment she made to the scam (subject to a deduction for Miss F's own contribution which I will consider below).

Should Miss F 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.

And, having thought carefully about this, I do think Miss F could have done more to protect herself from this scam. I think she ought reasonably to have had concerns about the legitimacy of the job offered, considering the requirement to send funds before she could earn any profits and the lack of any formal contract of employment or other official documents about this job she believed she had been hired to do. Because of this, I think it would be fair and reasonable to make a 50% reduction in the award based on contributary negligence in the circumstances of this complaint.

I've also thought about whether Revolut could have done more to recover Miss F's loss once it had been told of the scam. But given the nature of the payments Miss F was making, I don't think there was any reasonable prospect of Revolut recovering any of her loss, so I don't think there was any more it could have done.

Putting things right

To resolve this complaint Revolut should:

- Refund to Miss F 50% of her loss from the 14th payment to the scam onwards (inclusive).
- Pay 8% simple interest per annum on this refund from the date of each payment to the date of settlement.

My final decision

I uphold this complaint in part. Revolut Ltd should now put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss F to accept or reject my decision before 5 June 2025.

Sophie Mitchell
Ombudsman