DRN-5124815

The complaint

Miss F complains Revolut Ltd didn't do enough to protect her at a time she was falling victim to a scam and that it hasn't refunded her since that scam was revealed.

What happened

The background to this complaint is well-known to both parties and so I'll summarise events here.

Miss F saw what she believed to be a legitimate, celebrity endorsed advertisement for cryptocurrency investment on social media. She clicked on the advert and submitted her contact information. She was soon contacted by someone claiming to be a broker for the advertised firm. But Miss F had in fact been contacted by a fraudster, pushing an investment scam.

The scammer explained that the brokerage used AI to monitor markets and to identify trades. Miss F has explained how she was shown a genuine looking investment platform and decided to proceed.

Whilst Miss F started with a small sum, the amounts she was sending to the supposed investment quickly grew. Over the course of a month Miss F made more than a dozen payments. Most of these were to a cryptocurrency platform, with the final two being sent to named current accounts. The smallest of these payments was for £1,000, the largest £25,000. The total sent to the scammers from Revolut was £145,223. Much of that sum had been financed by way of lending that Miss F had taken out at the scammer's instruction.

The money didn't start off in Miss F's Revolut account. Instead, she'd sent money from her existing current account with what I'll refer to as Firm A, to another current account (newly opened at the scammer's instruction) with Firm B. It was then sent from Firm B to Revolut, before being sent on again to Miss F's cryptocurrency wallet. The funds were ultimately lost when forwarded from the cryptocurrency wallet, with Miss F believing she was crediting her trading account.

Miss F realised something was wrong when she lost all access to the platform. She reported what had happened to Revolut, Firm A, and Firm B. All three considered what had happened but said they wouldn't refund Miss F's loss. She then referred complaints to our service.

One of our investigators considered the three complaints together and recommended all be upheld. She recognised that the payments had all been authorised and that at every stage they had been made to one of Miss F's own accounts, remaining in her control, and only being lost once sent on from the cryptocurrency wallet at the end of the payment journey.

But she considered the activity had become unusual enough, and consistent with the characteristics of a typical cryptocurrency investment scam, that each firm ought to have intervened to question what Miss F was doing.

Our investigator noted there had been interventions along the way from the three firms. But she didn't believe those interventions had gone far enough and were not proportionate to the scam risk that was being presented. She felt that had each firm acted as it fairly and reasonably ought to have done, Miss F's losses could have been prevented. Her findings were then that each firm ought to bear some responsibility for Miss F's loss.

But she also found that Miss F's actions hadn't been reasonable throughout and that she ought to bear some responsibility herself, on the basis of contributory negligence. Some of the key points referred to here were:

- Miss F had been encouraged by the scammer to take out multiple loans to fund ongoing investment;
- The returns supposedly being generated were too good to be true;
- Miss F had confirmed being unable to find much about the broker online which ought to have caused concern given the apparent endorsement and success of it. And she thought a greater degree of care ought to have been taken into finding out more about the company, given she went on to send over £140,000;
- She was told to open new accounts, with the reasons for that being necessary not really adding up;
- There appears to have been no documentation (agreements to sign, terms and conditions etc.) provided by the scammer;
- Toward the end, Miss F was told to send money to unknown businesses with no apparent connection to what she'd been doing previously.

The investigator's overall findings were then that all parties ought to equally share responsibility for the outstanding loss, taking into account £23,500 that Revolut had been able to recover.

Firm A agreed with the findings right away. Firm B initially disagreed but has now accepted the recommended outcome. Revolut disagreed and has maintained its position. And so, it's now for me to issue this final decision.

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 November 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).

- 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).

- 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[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

---

[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] 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.

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 November 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

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

It isn't in dispute that Miss F has fallen victim to a cruel scam here, nor that she authorised the payments she made by transfers to third parties and to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in detail in this decision the circumstances which led Miss F to make the payments using her Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less

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

information available to it upon which to discern whether any of the payments presented an increased risk that Miss F might be the victim of a scam.

By November 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 November 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.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

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 November 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.

To be clear, I'm not suggesting as Revolut argues that, as a general principle (under the Consumer Duty or otherwise), Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees.

As I've set out in some detail above, it is the specific risk associated with cryptocurrency in November 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements (including the Consumer Duty), Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. 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.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Miss F' own name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Miss F might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the first two payments a were going to a cryptocurrency provider (the merchants being well-known provider), but they were low in value, and I don't think Revolut should reasonably have suspected that they might be part of a scam. Though I do note Revolut did take some action here, actions I'll come to address later in this decision.

The third payment (£13,560) made by Miss F was clearly going to a cryptocurrency provider. It was significantly larger than any other payment that had debited Miss F' account in the previous twelve months. And it came within an hour of the previous payment. Given what Revolut knew about the destination of the payment, and its significant value, I think that the circumstances should have led Revolut to consider that Miss F was at heightened risk of financial harm from fraud.

I've also taken account of the fact Miss F's Revolut account wasn't used very often, and so Revolut had limited historical account behaviour upon which to base risk scoring or to assess the decision on whether to intervene or not. But the characteristics of the payment I've already covered lead me to the same conclusion that the identifiable risk was significant enough for Revolut to intervene in any case.

In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead. And in making that finding, I have taken into account that Revolut had already intervened in the previous payment.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services I addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by November 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn Miss F?

Revolut did nothing to warn Miss F about the risks when payment three was being made and it didn't stop the payment to question it.

It is the case that Revolut gave some warnings and intervened in other payments. And I'll address those later in this decision. At this stage though, it is established that Revolut ought to have intervened at payment three and failed to do so.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that some payments that look similar to this one will be entirely genuine. I've given due consideration to Revolut's 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, when Miss F attempted to make the third payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have initiated a human intervention, for example, by directing her to the in-app chat so it could be discussed.

There ought to have then been a series of open questions, with Miss F's responses being considered and probed. This then ought to have led to the provision of a warning, tailored according to the responses given, and specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022, and highlighting the key features of such scams. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of a cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams.

The warning Revolut ought fairly and reasonably to have provided should have highlighted in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

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

I said earlier that Revolut did intervene in some payments, where questions were asked, and some warnings given. And so they become relevant in considering whether intervention at payment three would have made a difference. I remain satisfied it would have.

Of importance is that, whilst some of the warnings given to Miss F touched on some features of cryptocurrency scams, and even matched her circumstances, these were presented in a largely static, storyboard format that could be clicked through. They weren't given in a live conversation, where they would have been more impactful. There should have been a back-and-forth conversation, with Miss F made to deliver more complete answers through the use of open questions.

For the questions that were asked, these were presented in a very much closed format. For a firm like Revolut to be able to properly assess such a significant risk, questions ought to be open. With the answers then being considered before tailored follow-up questions are asked. It is otherwise all to easy for a customer to respond without thinking, or in an attempt to force the transaction through in a rush. And whilst I wouldn't expect a firm to submit a customer to an interrogation, it is fair and reasonable to say that any answers given ought to be considered, tested, and probed. Especially when the identifiable scam risk is as high as it was here.

Revolut will also be aware that many customers are coached or guided through such checks, and so the need for interaction and tailored responses ought to be well-understood and designed to uncover such instances.

With this in mind, whilst there is evidence of Miss F providing answers that didn't reflect the full circumstances she was in, I'm not persuaded she could have or would have maintained a false narrative if properly questioned. It is, after all, evident she did inform Revolut that she was investing in cryptocurrency, and so she was clearly willing to discuss the nature of what she was doing. I'm then persuaded it is more likely than not she would have revealed more details about her actions if probed further. That in turn would have led to concerns for Revolut and an increasing starkness of the warnings given.

Miss F was caught up in a scam with very common features. Revolut ought to have explained all of these in detail to Miss F, checking to make sure she understood each characteristic along the way. Had that happened, so similar in nature would have been the circumstances, that I'm persuaded she would have questioned what she was doing and stopped. Such a discussion and delivery of warnings would more likely than not have been significantly more impactful than the warnings she was given at other times.

In making my findings here I have also taken account of what happened when payments were being made from Firm A and Firm B. There were other warnings and interventions along the way there, but never any that met the standard required, hence complaints against each being upheld by this service. And it's noteworthy that Firm A and Firm B weren't aware of the elevated risk linked to cryptocurrency payments; they couldn't see that detail and so it didn't factor into their risk scoring and response.

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 purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that the payments were made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from other accounts at regulated financial businesses.

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 £13,560 payment, 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/or wasn't lost at the point it was transferred to Miss F's own 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.

Miss F has complained about Firm A and Firm B. Those complaints have been upheld and the two firms share equal responsibility for the loss with Revolut and Miss F. This then fairly and reasonably addresses the role of each party involved (excepting the cryptocurrency platform, which isn't covered by our jurisdiction), and each party complained about.

Should Miss F bear any responsibility for their 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.

The outcome in this respect is largely agreed. Revolut has always considered that Miss F ought to be held accountable for her own actions. Our investigator agreed, assigning responsibility across the four involved parties, inclusive of Miss F. And Miss F accepted those findings.

For completeness, I will say I agree that Miss F should bear partial responsibility for her loss. The reasons for saying as much have been set out in the 'what happened' section of this decision. I have considered all the circumstances of the case afresh and my reasoning is broadly the same as that of our investigator. So I won't repeat those details again here.

I've confirmed in this decision that Revolut is to be held responsible for a portion of the loss, along with Firm A, Firm B, and Miss F. The fair and reasonable assignation of the loss then is for it to be split equally across the parties. That recognises the involvement, actions, and mistakes of all involved.

Putting things right

On Miss F's acceptance, Revolut must:

- Reimburse 25% of Miss F's remaining loss from the payment of £13,560 on 6 November 2023 onwards, and taking account of the money recovered. My understanding is this is calculated as:
    - £144,223 (sum lost) - £23,500 (sum recovered) = £120,723 (outstanding loss)
    - £120,723 x 25% = £30,180.75
- Pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.

My final decision

I uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms F to accept or

reject my decision before 28 May 2025.

Ben Murray
Ombudsman