DRN-4853066

The complaint

Mrs S complains that Revolut Ltd (Revolut) is refusing to refund her the amount she lost as the result of a scam.

Mrs S is being represented by a third party. To keep things simple, I will refer to Mrs S throughout my decision.

What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, due to Mrs S's financial situation at the time she had started to look at potential investment opportunities. Mrs S found an online advert for a business (That I'll call X) where she completed a data caption form expressing her interest.

Mrs S then received a call from X where the opportunity to invest was explained in more detail, and she was invited to a webinar. Mrs S was also allocated what X described as an account manager.

Mrs S tells us she completed online research into X before committing to the investment and found positive reviews. Mrs S also tells us that she was required to provide identification documents to X.

Part of Mrs S's research found that X was not registered with the FCA and she challenged X about this. X was able to provide an explanation for this that put Mrs S's mind at rest. In summary it said it had never been registered with the FCA as the FCA does not regulate the crypto market and it is not a requirement. Instead, X said it was registered with the UK government as a financial organisation. X then provided a link to what appeared to be take Mrs S to its registration on Companies house.

Mrs S was also required to download remote access software so that X could help her with the process. This made Mrs S feel confident that X was a genuine business offering a genuine investment opportunity.

Mrs S made an initial investment of £1,000 and attended a webinar event where she was offered investment packages that came at a higher price. This enticed Mrs S to make the second larger payment of £14,000 which she was required to top up to £15,000 the following day. This investment package appeared to come with a guarantee and offered a gain of on average 6% per day if traded for 15 days.

Mrs S could see her investment was doing well when she was offered another opportunity to invest, X told Mrs S that the more he invested the more profit she would make. As Mrs S was running low on funds X convinced her to apply for a loan, which she did via another bank giving the reason for the loan as home improvement and secured £20,000 which she used to invest with X. Mrs S tells us that X told her to give

Mrs S made the following payments in relation to the scam from her Revolut account:

Payment	Date	Payee	Payment Method	Amount
1	7 July 2023	Wallbitex	Credit Card	£1,000
2	12 July 2023	Payward Ltd	Transfer	£14,000
3	13 July 2023	Payward Ltd	Transfer	£1,000
4	3 August 2023	Payward Ltd	Transfer	£20,000

Having made additional payments into the scam via an account elsewhere Mrs S attempted to make a withdrawal from the investment. At this time X explained that Mrs S would have to make a further payment first, and she realised she had fallen victim to a scam.

Our investigator considered Mrs S's complaint and thought it should be upheld. Revolut disagreed, in summary it argued that:

- No further interventions would have made a difference as Mrs S confirmed on several occasions that she was sending funds to her own personal account
- Most high street banks are telling customers that when they are not liable for self-to-self transactions, and we should be looking at where the funds originated from before going to Mrs S' Revolut account
- It has no legal duty to prevent fraud and it must comply strictly and promptly with valid payment instructions. It does not need to concern itself with the wisdom of those instructions. This was confirmed in the recent Supreme Court judgement in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25
- There are no legal obligations, regulatory obligations, industry guidance, standards or codes of practice that apply to Revolut obliging it to refund victims of APP fraud.
- Mrs S was grossly negligent by ignoring the warnings it gave. The PSR's mandatory reimbursement scheme will allow it to decline claims where a consumer has been grossly negligent, taking into account any warnings it has provided

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 Mrs 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 Mrs 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 transfers 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 transfers.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in July 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[2]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

---

[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 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).

- 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

[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 a some of the payments listed above pre-date the Consumer Duty so it will not apply to those payments.

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

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 Mrs S was at risk of financial harm from fraud?

It isn't in dispute that Mrs S has fallen victim to a cruel scam here, nor that she authorised the payments she made by transfer or card to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out the circumstances which led Mrs S 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 Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mrs S might be the victim of a scam.

The payments Mrs S made in relation to the scam were being made to well-known cryptocurrency exchanges that Revolut would have been aware of at the time, so I think it's reasonable to say Revolut what have been aware that the payments made were in relation to cryptocurrency.

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 customers' 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[5]. And by July 2023, when these payments took place, further restrictions were in place[6]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mrs S 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.

In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and

delivering warnings before it processed such payments.

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 Mrs S might be at a heightened risk of fraud.

The first payment Mrs S made in relation to the scam was of a relatively low value and I don't think a heightened risk of fraud was present. So I don't think it was unreasonable that Revolut didn't intervene when this payment was made.

Payment 2 was for the very high value of £14,000 and presented increased potential of causing financial harm. It was clearly going to a cryptocurrency provider. It was larger than any other payment that had debited Mrs S' account in the previous six months.

Taking that into account, as well as what Revolut knew about the destination of the payment, I think when Mrs S attempted to make this sizeable payment, it should have considered that Mrs S could be at heightened risk of financial harm from fraud and, in line with good industry practice, warned its customer before the payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, I think it was a combination of the characteristics of this payment and that the payment went to a cryptocurrency provider that ought to have prompted a warning.

What did Revolut do to warn Mrs S and what should it have done?

As expected Revolut did stop payment 2 with a warning that there was a significant risk. A chat conversation between Revolut and Mrs S then took place.

Mrs S provided a photo of herself to prove her identity and then confirmed several pieces of information.

Mrs S said:

- she was making the payment to X via a cryptocurrency account
- she was making a payment to her personal trading account
- she was making a payment to her cryptocurrency account

Revolut gave Mrs S a warning about safe account scams and checked she had not recently been contacted by a third party asking her to move funds to a safe account.

Although Mrs S had told Revolut that her payment was being made to a well-known cryptocurrency exchange and that this would have been clear by the payee's name, Revolut gave the following warning:

"Please be aware that scammers will typically offer a price below market value to attract your attention. Social media has also become an easy way for scammers to advertise their goods and services. Please do your research on the seller and try to verify if they are a genuine seller. You should check if the seller has reviews from previous customers before proceeding. If you have any concerns, then do not proceed with the purchase."

Revolut then asked Mrs S to:

*“Kindly confirm you acknowledge that by continuing with the transfer, in the event of this being fraudulent/scam activity, we will be unable to recover these funds and any other funds you subsequently send to this beneficiary. To make this confirmation, please write: *"Revolut has warned me that this is likely a scam and are unlikely to recover my funds if I proceed with this transaction."*”*

Mrs S confirmed the above statement as requested by Revolut.

Given the information Mrs S provided to Revolut I don’t think the warnings given in this chat conversation were proportionate or appropriate. They did not cover the risk of making this type of payment.

Revolut has also provided screen shots of those Mrs S would have seen when making the payments, however none of these give a significant warning about the risk of making cryptocurrency payments, or cryptocurrency investment scams either.

Instead of providing a warning about safe account scams, Revolut should have reacted to the information that Mrs S gave to it – all of which pointed to towards Mrs S falling victim to a cryptocurrency investment scam. It also failed to ask any follow up questions about the information she provided that is likely to have elicited further information pointing towards a scam. But even on the basis of the information it did have, Revolut ought to have explained the risks of cryptocurrency investment scams and the key features of such a scam, 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 an intervention of the type described, would that have prevented the losses Mrs S suffered from payment 2 onwards?

Mrs S was experiencing a relatively common type of cryptocurrency scam, having completed an online form, been given access to an online trading platform and then being persuaded to put money into an investment via cryptocurrency. Mrs S was also required to download the remote access software. So, I think a warning of the type I’ve described would have resonated with her.

I can see that another bank Mrs S made payments from in relation to the scam did intervene after Mrs S made the disputed payments from her Revolut account, and Mrs S wasn’t honest in her responses to its questions which would have made it difficult to uncover the scam. And when Mrs S applied for a personal loan later in the scam that funded payment 4, she wasn’t honest about the loan purpose either.

But when Mrs S spoke to Revolut via the chat facility it was at a relatively early stage of the scam before she applied for the loan, and before any intervention from her other bank took place. At this time Mrs S explained she was making payments to a cryptocurrency exchange that she would then forward to a separate company for ‘trading’. This appears to be an accurate account of what Mrs S thought she was making the payment for – so it’s clear she was not misleading Revolut about the purpose of the payments. I think it’s likely that had Revolut given a clear warning at this early stage, based on the information it obtained from Mrs S she wouldn’t have gone ahead with the payments and her loss would have been prevented.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs S 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.

But as I've set out above, I think that Revolut still should have recognised that Mrs S might have been at risk of financial harm from fraud when she made payment 2, 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 Mrs S suffered. The fact that the money used to fund the scam wasn't lost at the point it was transferred to Mrs S'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 Mrs 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 Mrs S could instead, or in addition, have sought to complain against those firms. But Mrs S 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 Mrs 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 any 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 Mrs S's loss from payment 2.

Should Mrs S bear any responsibility for her losses?

I've thought about whether Mrs S should bear any responsibility for her loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint.

Having done so I think it is reasonable that Mrs S should share responsibility for her loss and the compensation rewarded to her reduced by 50%.

I can understand why Mrs S found aspects of the scam plausible including the webinar she attended and the ability to see her funds on what appeared to be a legitimate platform.

Mrs S's own research found that X was not regulated by the FCA and this caused her to have concerns. Mrs S did question X about her findings and was given a reasonably convincing answer, however she appears to have taken this on face value and not sought independent advice herself which I think would have been reasonable before investing the substantial amounts that she did.

That's particularly true given that the investment offered returns that appeared to be guaranteed and offer returns that were too good to be true offering average daily increases

of 6% for the larger investments over a short period of time. I think that the promise of guaranteed returns ought to have caused Mrs S to have significant concerns, particularly as she thought she was making investments in cryptocurrency.

Mrs S was also persuaded to take a loan to fund some of the payments I think Mrs S should have found this unusual and had concerns.

With the above in mind, I think there were clear red flags that Mrs S should have taken notice of and that should have caused Mrs S to have serious concerns. Had Mrs S taken more care she could also have prevented her loss.

Could Revolut have done anything to recover Mrs S' money?

One of the payments was made by card to a cryptocurrency provider. Mrs S sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, this was evident when Revolut attempted a chargeback in relation to the payment which was unsuccessful.

The remaining payments made in relation to the scam were sent by transfer to Mrs S's own cryptocurrency account and then sent to the fraudster. So, in these circumstances, it's difficult to see how any recovery would have been possible.

Putting things right

To put things right Revolut Ltd should pay Mrs S:

- 50% all the payments she made in relation to the scam from payment 2 onwards.
- 8% simple interest per year on that amount from the date of each payment to the date of settlement.

My final decision

I uphold this complaint and require Revolut Ltd to put things right by doing what I've said above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 22 November 2024.

Terry Woodham
Ombudsman