DRN-5000092

The complaint

Ms K complains that Revolut Ltd won't refund money she lost when she fell victim to an investment scam.

Ms K is being represented by solicitors in this complaint.

What happened

The detailed background to this complaint is well known to the parties and has been previously set out by the investigator. I'll only provide an overview and focus on giving my reasons for my decision.

The complaint concerns several debit card payments totalling around £19,400 which Ms K made from a newly created Revolut account between March and June 2023. They were made in connection with an investment opportunity she came across on a popular social media platform. After leaving her details, Ms K was contacted by a representative of the company who said they were her account manager.

Under the instructions of her manager, Ms K set up an e-money account with Revolut and transferred funds from her account with her existing bank "M" to the new account. The money was then used to purchase cryptocurrency from a well-known cryptocurrency provider, before being sent to cryptocurrency wallets as instructed.

Encouraged by profits made, Ms K made a few more payments. When she requested a withdrawal, she was asked to pay withdrawal fees. Ms K did what she was told, and after a excuses about the payment to her bouncing back she was asked for a further payment to release her investment. Eventually, the communication stopped and that is when Ms K discovered that she had been scammed.

The following payments, made using Ms K's Revolut debit card, are being disputed –

	Date	Amount
Payment 1	27 March	£999.21
Payment 2	31 March	£998.93
Payment 3	6 April	£997.85
Payment 4	6 April	£997.93
Payment 5	12 April	£499.39
Payment 6	25 April	£500.15
Payment 7	12 May	£987.82
Payment 8	19 May	£986.81
Payment 9	26 May	£2,991.35
Payment 10	2 June	£2,001.55
Payment 11	2 June	£2,729.30
Payment 12	7 June	£4,519.60
Payment 13	7 June	£206.97

	Total payments	**£19,416.86**

Revolut declined to refund any of the disputed payments, saying that Ms K had authorised them. Unhappy with this, she referred her complaint to our service.

Our investigator concluded that Revolut ought to have provided a written warning tailored to cryptocurrency investment scams when Ms K made Payment 11. Had it done so, the investigator was persuaded that Ms K would have stopped in her tracks and losses prevented. They asked Revolut to refund her losses (along with interest) from that payment onwards but with a 50% deduction for contributory negligence.

Ms K accepted the investigator's findings. But Revolut asked for the complaint to be decided by an ombudsman. In summary, it said the payments were self to self and the scam didn't occur on its platform.

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.

I'd like to start by thanking both parties for their continued patience while waiting for the complaint to be reviewed by an ombudsman.

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 Ms K modified the starting position described in Philipp, by – among other things – 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"* (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial

Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I'm satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I'm required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

While the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should, at the time of these payments, 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.

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'm mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud[1];
- 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.

For example, it is my understanding that in March 2023 (when these payments started), Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I'm 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

[1] 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_/

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)[2].

- 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 don't 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).

- 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.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So, it was

[2] 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.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

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 March 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.

While I'm required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I'm satisfied that to comply with the regulatory requirements that were in place in March 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Ms K was at risk of financial harm from fraud?

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

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that most of the disputed payments would be credited to a cryptocurrency wallet held in Ms K's name.

By March 2023, when these transactions started, 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[4]. And by March 2023, when these payments started, further restrictions were in place[5]. 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'm satisfied that by the end of 2022, prior to the payments Ms K made, 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.

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 the payments in this case were going to an account held in Ms K's 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 Ms K might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the payments were going to a cryptocurrency exchange (the merchant involved was a well-known cryptocurrency exchange). I don't think there was anything particularly unusual about Payments 1-10 such that I consider Revolut should have had cause for concern. The payments were spread out and relatively low in value. Ms K hasn't disputed my findings on this point.

By the time Ms K authorised Payment 11 (which was on the same day at Payment 10), given the increased cryptocurrency activity that day, including the amount, I think that the circumstances should have led Revolut to consider that she was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

What did Revolut do to warn Ms K?

Revolut didn't provide any scam warnings to Ms K before executing her authorised instructions in relation to any of the disputed payments.

---

[4] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.
[5] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

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 many payments that look very 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 good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, when Ms K attempted to make Payment 11, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of 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 – cryptocurrency investment 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; an 'account manager', 'broker' or 'trader' acting on their behalf; returns that are too good to be true; the use of remote access software; and a small initial deposit which quickly increases in value but withdrawals are met with excuses.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Ms K by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Ms K suffered from Payment 11 onwards?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Ms K's payments, such as an advertisement on social media, being assisted by a broker, a small initial investment making big gains, and requests for withdrawals being met with demands for further payments.

I've also reviewed the written correspondence between Ms K and the scammer (though I note that she appears to have also spoken to them, not just communicated through instant messages, and I haven't heard those conversations). I've found nothing within the written correspondence that suggests Ms K was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Ms K expressed mistrust of Revolut or financial firms in general.

On the balance of probabilities, had Revolut provided Ms K with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. She could have, for instance, paused and looked more closely into her own circumstances. At the suggested trigger point, Ms K thought she was paying fees to withdraw her profits. She had found the broker through an advertisement on a social media platform and had been assigned a manager who was helping her with her trades.

Ms K could have also investigated cryptocurrency scams and the warnings published by regulators. I'm satisfied that a timely warning to Ms K from Revolut would very likely have caused her to decide not to go ahead with Payment 11.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Ms K purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the scammer. 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've carefully considered Revolut's view that the fraudulent activity didn't occur on its platform.

However, for the reasons I have set out above, I'm satisfied that it would be fair to hold Revolut responsible for Ms K's losses from Payment 11 onwards, subject to a deduction for Ms K's own contribution towards her loss (which I'll consider below). As I've explained, the potential for multi-stage scams, particularly those involving cryptocurrency, ought to have been well known to Revolut. And as a matter of good practice, I consider it fair and reasonable that Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Ms K's own account doesn't 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 K has only asked us to consider her complaint against Revolut. I'm aware that she did make a complaint to M, but it refused to refund her. But she hasn't chosen to refer her complaint about M to our service and ultimately, I can't compel her to. What I can see is that, following a request for further information, M told our service it couldn't confirm whether any of the payments Ms K made from her account with it to Revolut flagged on its system. It also couldn't confirm if an intervention took place.

I'm not persuaded that it would be fair to reduce Ms K's compensation in circumstances where: the consumer has only complained to our service about one respondent from which they are entitled to recover their losses in full; 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) and for the reasons I have set out above, I'm satisfied that it would be fair to hold Revolut responsible for Ms K's loss from Payment 11 (subject to a deduction for her own contribution which I will consider below).

Should Ms K bear any responsibility for her losses?

Ms K has already accepted that she should share equal responsibility for what happened here. But for completeness, I'll explain why I agree that it would be both fair and reasonable in the circumstances of this complaint that Revolut's liability is reduced by 50%.

There's a general principle in law that consumers must take responsibility for their decisions. I recognise that, as a layperson who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Ms K came across the

investment opportunity through an advert on social media. I haven't seen this particular advert, but I've seen other examples. In my experience, they often appear as paid adverts on social media websites and a reasonable person might expect such adverts to be vetted in some way before being published. Those adverts also can be very convincing – often linking to what appears to be a trusted and familiar news source.

I've also taken into account the provision of the trading platform (which, I understand, used genuine, albeit manipulated, software to demonstrate the apparent success of trades). I know that the scammer used the apparent success of early trades to encourage increasingly large deposits. I can understand how what might have seemed like taking a chance with a relatively small sum of money snowballed into losing a life changing amount of money.

So, I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Ms K to be reduced. I think it should.

Ms K doesn't appear to have done any research into the investment opportunity before she invested. That fact alone wouldn't necessarily be enough for me to consider that there should be a deduction to the amount awarded. But by the suggested trigger point, Ms K had sent a disproportionately large sum of money in withdrawal fees when compared to her investment. I think this fact should have given her cause for concern, enough to warrant checking that everything was above board.

Weighing the liability that I've found on both sides, I think a fair deduction is 50%.

Could Revolut have done anything else to recover Ms K's money?

Ms K sent money to a cryptocurrency provider before transferring it to the fraudster (albeit she didn't know that at the time). Revolut wouldn't have been able to recover the funds from the cryptocurrency provider, given that the funds had already been transferred out.

Putting things right

Revolut Ltd needs to refund Ms K Payments 11-13 (inclusive), making a 50% deduction to account for Ms K's role in what happened.

It also needs to add simple interest at 8% per year to the refunded amount, calculated from the date of loss to the date of settlement[6].

My final decision

For the reasons given, my final decision is that I uphold this complaint and direct Revolut Ltd to put things right for Ms K as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms K to accept or reject my decision before 5 March 2025.

Gagandeep Singh
Ombudsman

[6] If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Ms K how much it's taken off. It should also give her a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.