DRN-4903315

The complaint

Mr J complains that Revolut Ltd (Revolut) is refusing to refund him the amount he lost as the result of a scam.

Mr J is being represented by a third party. To keep things simple, I will refer to Mr J 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, Mr J tells us he found an advertisement online for an investment business I will call (X). It claimed to use a tool to enter many trades and benefit from the rise in prices quickly. Interested in the opportunity Mr J visited X's website which he tells us had all the hallmarks of a genuine website and was very convincing.

Mr J completed an online form and received a call from X who talked through the investment opportunity including that he would need to open an account with Revolut and that he would be contacted via WhatsApp. At this point Mr J opened his account with Revolut and made the first initial payment of £250.

Mr J was then contacted via WhatApp and offered further investment opportunities with the promise of very good returns. X explained that it would work on Mr J's behalf and would be paid via commission on the profits Mr J would make. Mr J made a payment of £500 which returned over £700 profit, and a larger payment of £5,000 from which he was able to see significant profits via X's trading platform.

As part of the investment process Mr J was required to give X access to his device via the remote access software AnyDesk.

X continued to pressure Mr J to make further payments with the promise of ever-increasing profits, but he explained he had no further funds he was able to invest.

X then explained that Mr J would need to make a payment in relation to the commission it was due from Mr J's profits before a withdrawal could be made. Mr J had made a profit of €22,938.91 from his initial deposit of €5,710.00 according to the invoice he received and so was required to pay €2,293 (10%). Mr J was also required to show liquidity by making a further payment of £7,500 (25% of the withdrawal).

After making both payments X asked again for further payments to be made but Mr J refused explaining he had made various payments without receiving any funds back. It was at this stage Mr J realised he had fallen victim to a scam.

Below is a list of the payments Mr J made in relation to the scam from his Revolut account:

Payment	Date	Payee	Payment Method	Amount

1	17 April 2023	Onlineprotrading.com	Debit Card	£250
2	3 May 2023	Nevadaex_simplex	Debit Card	£500
3	30 May 2023	Binanceltgbpecom	Debit Card	£5,000
4	21 June 2023	Binance	Debit Card	£2,293
5	21 June 2023	Binance	Debit Card	£5,000
6	21 June 2023	Binance	Debit Card	£2,500

Our Investigator considered Mr J's complaint and thought it should be upheld in part. Neither Mr J nor Revolut agreed.

Mr J said it was unfair to hold him partially responsible for his loss as there was not sufficient information available in the public domain that would have made him aware of the investment being a scam.

Revolut said:

- Several points it has raised have not been covered when considering the complaint.
- The law has not been applied correctly when the complaint has been considered.
- There are no legal obligations, regulatory obligations, industry guidance, standards or codes of practice that apply to Revolut that oblige it to refund victims of authorised push payment ("APP") fraud. By suggesting that it does need to reimburse customers, it says our service is erring in law.
- 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.
- Where Revolut is merely an intermediate link, and there are typically other authorised banks and other financial institutions in the payment chain that have comparatively greater data on the customer than Revolut, but we have not held them responsible in the same way as Revolut.

As an informal resolution could not be reached this complaint has been passed to me to decide.

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 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 Mr J 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 am 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 am 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.

Whilst 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 in April 2023 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 am 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;

[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_/

- 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 April 2023, 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 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)[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 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).
- 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

[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"

(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 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 April 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 Mr J was at risk of financial harm from fraud?

By April 2023 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[4]. And by April 2023, when these payments took place, further restrictions were in place[5]. This left a smaller number of payment service providers, including

[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

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 Mr J made in April 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, 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.

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 Mr J might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the payments Mr J made in relation to the scam were going to a cryptocurrency provider, but the first two payments were low in value, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

Payment 3 was clearly going to a cryptocurrency provider and was significantly higher in value (£5,000). Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr J 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 warned Mr J before this payment went ahead.

What did Revolut do to warn Mr J?

Revolut has explained that Mr J confirmed the payments vis 3DS secure which confirmed he was making the payments. But it did not give Mr J any warnings when he made the payments in dispute.

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 to have been good industry practice

at the time this payment was made.

Taking that into account, I think Revolut ought, when Mr J attempted to make payment 3, 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, 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.

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 Mr J 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 cryptocurrency investment scam warning, would that have prevented the losses Mr J incurred after that point?

Mr J funded the payments made from his Revolut account from another account he held in his own name. It doesn't appear that any interventions were carried out by the operator of his other account.

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 Mr J's payments, such as being allocated an account manager, starting with a small initial payment followed by larger more significant payments with the promise of higher returns. Mr J was also asked by X to download remote access software. By the time Mr J made payment 3 he had also seen significant returns of around 100% on his initial investment in a short space of time

Therefore, on the balance of probabilities, had Revolut provided Mr J with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He could have paused and looked more closely into X before proceeding. I'm satisfied that a timely warning to Mr J from Revolut would very likely have caused him to pause for thought and prevented his further losses.

Is it fair and reasonable for Revolut to be held responsible for Mr J's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr J made payments into his Revolut account from an account he held elsewhere and purchased cryptocurrency which likely credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his 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 Mr J might have been at risk of financial harm from fraud when he made payment 3, and in those circumstances Revolut should have provided a proportionate warning before processing it. If it had done that, I am satisfied it would have prevented the losses Mr J suffered. The fact that the money used to fund the scam wasn't lost at the point it was transferred to Mr J's own account does not alter that fact and I think Revolut can fairly be held responsible for his 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 Mr J 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 Mr J could instead, or in addition, have sought to complain against those firms. But Mr J has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr J'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 Mr J's loss from payment 3.

Should Mr J bear any responsibility for his losses?

I've thought about whether Mr J should bear any responsibility for his 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 Mr J should share responsibility for his loss and the compensation rewarded to him reduced by 50%.

There were some convincing aspects of the scam such as a professional looking website and trading platform, as well as convincing conversations Mr J had with the scammer.

But the returns that Mr J made prior to the third payment should have led him to make further enquiries about the firm. Had he done that, he would have found that there were negative reviews about it online at the time.

I think the above should have caused Mr J serious concerns and he should have taken more care. Had Mr J taken notice of the red flags explained above he could also have prevented his loss.

Recovering the payments Mr J made in relation to the scam

Mr J made payments into the scam via his debit card. When payments are made by card the only recovery option Revolut has is to request a chargeback.

The chargeback scheme is a voluntary scheme set up to resolve card payment disputes between merchants and cardholders. The card scheme operator ultimately helps settle disputes that can't be resolved between the merchant and the cardholder.

Such arbitration is subject to the rules of the scheme, meaning there are only limited grounds and limited forms of evidence that will be accepted for a chargeback to be considered valid, and potentially succeed. Time limits also apply.

Mr J was dealing with the scammer, which was the business that instigated the scam. But Mr J didn't make the debit card payments to the scammer directly, the majority of the payments he made were paid to separate cryptocurrency exchanges. This is important because Revolut was only able to process chargeback claims against the merchants he paid, not another party.

The service provided by the exchanges would have been to convert or facilitate conversion of Mr J's payments into cryptocurrency. Therefore, they provided the service that was requested; that being the purchase of the cryptocurrency.

The fact that the cryptocurrency was later transferred elsewhere – to the scammer – doesn't give rise to a valid chargeback claim against the merchants Mr J paid.

Revolut has explained it attempted chargebacks for each of the payments Mr J made and on each found that a genuine service had been provided.

With the above in mind, I don't think Revolut had any other reasonable options available to it to seek recovery for the payments Mr J made.

Putting things right

To put things right I require Revolut Ltd to:

- refund 50% of Mr J's total loss from payment 3 onwards less any recovered funds
- add 8 % simple interest per year to the amount it pays Mr J from the date of loss to the settlement date (less any lawfully deductible tax)

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr J to accept or reject my decision before 29 November 2024.

Terry Woodham
Ombudsman