DRN-4723162

The complaint

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

Mr G is being represented by a third party. To keep things simple, I will refer to Mr G 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 G was browsing online when he found an advertisement for a company, I will call X offering an investment opportunity which appeared to be endorsed by a well-known celebrity.

Interested in the opportunity Mr G started communicating with X. X gave a background to the company and further information about the investment opportunity. As part of the investment process Mr G was required to download remote access software and open a cryptocurrency account, as well as an account on X's platform, and one with Revolut.

Mr G recalls X's platform appearing very professional, and that X confirmed it would be making trades on Mr G's behalf, but that he could login at any time to see how his investment was performing.

Mr G and X stayed in contact via phone and occasionally by email speaking multiple times every week. X advised Mr G that he would be able to double his investment if he invested £2,000, Mr G agreed.

Mr G tells us that around a week later X asked him if he would like to withdraw some of his funds, which Mr G confirmed he would. But when Mr G attempted to withdraw his money, he was asked to make further and further payments first.

Having made multiple payments to retrieve his funds without success Mr G realised he had fallen victim to a scam.

Mr G made the following payment in relation to the scam:

Payment	Date	Payee	Payment Method	Amount
1	24 March 2023	Wirex	Debit Card	£41.82
2	21 April 2023	Moonpay	Debit Card	£900.00
3	10 May 2023	Moonpay	Debit Card	£2,000.00
4	22 May 2023	Moonpay	Debit Card	£2,500.00
5	22 May 2023	Moonpay	Debit Card	£2,700.00
6	31 May 2023	Moonpay	Debit Card	£2,489.00
7	31 May 2023	Moonpay	Debit Card	£2,513.00
8	9 June 2023	Moonpay	Debit Card	£2,500.00
9	9 June 2023	Moonpay	Debit Card	£2,497.00
10	15 June 2023	Moonpay	Debit Card	£2,500.00

Our Investigator considered Mr G's complaint and thought it should be upheld in part. Revolut didn't agree, in summary Revolut said:

- 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.
- Mr G was grossly negligent when making the payments.
- The payments were self- to-self payments and therefore the loss did not occur from the Revolut platform.
- FOS' recent reliance on R (on the application of Portal Financial Services LLP) v FOS [2022] EWHC 710 (Admin) is misconceived and amounts to a legal error. As a preliminary matter, the judgement is a permission decision only, and such decisions do not ordinarily create precedent, even for a court.

As an informal resolution could not be agreed this complaint has now 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 G 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 March-June 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]

[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_/

- 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-June 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 (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

[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"

- 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 March-June 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.

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

Should Revolut have recognised that Mr G was at risk of financial harm from fraud?

It isn't in dispute that Mr G has fallen victim to a cruel scam here, nor that he authorised the payments he made to his 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 Mr G to make the payments using his 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 information available to it upon which to discern whether any of the payments presented an increased risk that Mr G might be the victim of a scam.

Firstly, I don't think that Revolut would reasonably have had concerns about the first four payments Mr G made in relation to the scam as they were not of such a significant value and were spread across several days.

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.

By March 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[4]. And by March 2023, when these payments took place, 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 am satisfied that by the end of 2022, prior to the payments Mr G 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.

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 March-June 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 the payments in this case were

---

[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

going to an account held in Mr G'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 Mr G might be at a heightened risk of fraud that merited its intervention.

When Mr G made payment 5, he was making a second payment the same day totalling more than £5,000 to a well-known cryptocurrency exchange. Considering the increased risk associated with this type of payment that Revolut would have been aware of at the time I think it should have had concerns at this point and provided an intervention proportionate to that risk.

What did Revolut do to warn Mr G?

Revolut has confirmed that Mr G made the payments in relation to the scam using his debit card. Mr G was required to confirm it was him making the majority of the payments using 3DS secure verification, but other than this no intervention was carried out.

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 primary duty to make payments promptly.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifyingthe specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by March-June 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored, effective warnings relevant to that scam for both APP and card payments. I understand in relation to Faster Payments it already had systems in place that enabled it to provide warnings in a manner that is very similar to the process I've described.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by March-June 2023, on identifying a heightened scam risk, a firm such as Revolut should have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew that the payment was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave.

Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation and investment scams.

Taking that into account, I am satisfied that, by March-June 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mr G made

payment 5, Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment he was making – have provided a scam warning tailored to the likely cryptocurrency related scam Mr G was at risk from.

In this case, Mr G was falling victim to an investment scam.

As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Mr G gave. I'd expect any such warning to have covered off key features of such a scam, such as the use or remote access software, finding the investment via social media and having to pay large sums without being able to make a withdrawal. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've not seen enough to indicate that Mr G wouldn't have done so here.

I accept that there are a wide range of scams that could involve payments to cryptocurrency providers. I am also mindful that those scams will inevitably evolve over time (including in response to fraud prevention measures implemented by banks and EMI's), creating ongoing challenges for banks and EMI's.

In finding Revolut should have identified that payment 5 presented a potential scam risk and that it ought to have taken steps to narrow down the nature of that risk, I do not suggest Revolut would, or should, have been able to identify every conceivable or possible type of scam that might impact its customers. I accept there may be scams which, due to their unusual nature, would not be easily identifiable through systems or processes designed to identify, as far as possible, the actual scam that might be taking place and then to provide tailored effective warnings relevant to that scam.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr G suffered from payment 5?

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 G's payments, such as finding the investment through an advertisement endorsed by a celebrity, being assisted by a broker and being asked to download remote access software so they could help him open cryptocurrency wallets. I have also not seen enough to say that Mr G was given any convincing backstory or would not have been honest when questioned.

Therefore, on the balance of probabilities, had Revolut provided Mr G 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 at the investment before proceeding, as well as making further enquiries into cryptocurrency scams and whether X was regulated in the UK or abroad. I'm satisfied that a timely warning to Mr G from Revolut would very likely have caused him to take more care before making any further payments and uncovered the scam.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr G paid money using his Revolut account to another account in his own name, rather than directly to the fraudster, so he remained in control of his money after he made the payments, and there were further steps before the money was lost to the scammer.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr G might have been at risk of financial harm from fraud when he made payment 5, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mr G 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 Mr G's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr G's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr G 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 G could instead, or in addition, have sought to complain against those firms. But Mr G 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 G's compensation in circumstances where: the Mr G has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr G's loss from payment 5 (subject to a deduction for consumer's own contribution which I will consider below).

Revolut has addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I have not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I do not intend to comment on it. I note that Revolut says that it has not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it is asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved.

I have considered that payments were made from another of Mr G's accounts to his Revolut account before being forwarded to the scammer. The originating bank did not intervene when those payments were made and as Mr G didn't raise a complaint against that provider, I've only looked into the case brought to us against Revolut.

Should Mr G bear any responsibility for his losses?

Despite regulatory safeguards, there is a general principle that consumers must still take responsibility for their decisions (see s.1C(d) of our enabling statute, the Financial Services and Markets Act 2000).

In the circumstances, I do think it would be fair to reduce compensation by 50% on the basis that Mr G should share blame for what happened. There was negative reviews about X available online at the time he started making payments and I think it would have been reasonable to expect Mr G to carry out reasonable due diligence, and at least a basic online

search before agreeing to make payments. Mr G was also promised too good to be true returns on his investment (doubling an initial payment).

I think there were clear red flags Mr G should have taken notice of, and he should have taken more care. If Mr G had taken more care he could also have prevented his loss.

Could Revolut have done anything to recover Mr G' money?

The payments were made by card to a cryptocurrency provider. Mr G sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds.

In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute the cryptocurrency was provided to Mr G, which he subsequently sent to the fraudsters.

Putting things right

To put things right I require Revolut Ltd to:

- Refund 50% of the payments Mr G made in relation to the scam from payment 5 onwards.
- Pay 8% simple interest on the amount it pays Mr G from the date of the loss to the date the refund is made (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 G to accept or reject my decision before 27 March 2025.

Terry Woodham
Ombudsman