DRN-4987622

The complaint

Mr G complains that Revolut Ltd hasn't protected him from losing money to a scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In brief summary, I understand that between February and April 2023 Mr G made numerous payments totalling nearly £117,000 from his Revolut account as a result of what he thought was a legitimate investment.

Mr G subsequently realised he'd been scammed and got in touch with Revolut. Ultimately, Revolut didn't reimburse Mr G's lost funds, and Mr G referred his complaint about Revolut to us. As our Investigator couldn't resolve the matter informally, the case has been passed to me for a decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to

decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with 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 February to 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;
- 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 February to April 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could

[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_/

(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.

- 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

[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"

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 February to 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 G was at risk of financial harm from fraud?

It isn't in dispute that Mr G has fallen victim to a scam here, nor that he authorised the payments he made to the cryptocurrency wallets (from where that cryptocurrency was subsequently transferred to the scammer).

I'm aware that cryptocurrency exchanges like the ones Mr G paid 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 these payments would be credited to a cryptocurrency wallet held in Mr G's name.

By February to April 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 further restrictions were in place[5], leaving 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 in February to 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.

To be clear, it is the specific risk associated with cryptocurrency in February to April 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, 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 going to an account held in Mr G's name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone on to 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. And I think that because of what I've said about cryptocurrency above, Revolut ought to have recognised Mr G was at heightened risk of fraud that merited its intervention when he instigated the first payment from his Revolut account to the scam on 28 February 2023, which was for £5,149.50 to a cryptocurrency provider. Mr G instigated a second payment to the same crypto provider just two minutes later for £10,299 and I think at this point Revolut's concern ought to have increased and for the nature and robustness of its intervention to have escalated.

What did Revolut do to warn Mr G?

---

[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.

I understand from the information provided by Revolut that Revolut didn't intervene in Mr G's payments until 27 and 28 April 2023. Revolut has explained that when Mr G set up the new payee he paid on those days, he would have received a standard warning: *"Do you know and trust this payee? If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others and we will never ask you to make a payment."* I understand Mr G was also asked the payment purpose for two or three payments on 27 April 2023 to which he stated "cryptocurrency" and Revolut consequently provided Mr G, in-app, with tailored written warnings about cryptocurrency investment scams. Revolut has also explained that on 28 April 2023, one of Mr G's payments triggered for human intervention and Mr G was invited to an in-app chat to discuss that payment. It says Mr G had selected "safe account" as the purpose for that payment, and that this was then discussed in-app and Mr G was given appropriate warnings.

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 these ones 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 that Revolut ought, when Mr G instructed his first payment which was for £5,149.50, knowing the payment was going to a cryptocurrency provider, to have provided, at a minimum, a warning (whether automated or in some other form) that was specifically about the risks of cryptocurrency scams, given how prevalent they had become by the end of 2022.

I think 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. 'Fees' becoming payable to initiate withdrawals that then don't fully materialise or are restricted would also be a common theme.

I recognise that a warning of this 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 G.

Having thought carefully about the risk Mr G's second payment, which was for £10,299, presented, I think this warranted an escalation in intervention – I think a proportionate response to this risk would be for Revolut to have attempted to establish the circumstances surrounding this second payment before allowing it to debit Mr G's account. I think it should have done this by, for example, directing Mr G to its in-app chat to discuss the payment further.

If Revolut had provided warnings of the type described, would that have prevented the losses Mr G suffered from the point of the first or second payments?

I note Revolut's interventions on 27 and 28 April 2023. Whilst, in my view, these didn't come nearly early enough, I take on board that Mr G was provided with some warnings, in-app, about cryptocurrency scams. This didn't cause Mr G to change his mind about making the payments on 27 and 28 April 2023, and I don't think it's unreasonable to conclude, like our

Investigator did, that such warnings, if they'd been provided to Mr G when he made his first payment on 28 February 2023, as I think they should have, probably wouldn't have made a difference then. I've not seen anything that persuades me Mr G would have reacted to such a warning on 28 February 2023 differently to what he later appears to have. So I think if Revolut had intervened in Mr G's first payment on 28 February 2023 as I'd reasonably expect it to, this likely wouldn't have prevented Mr G from making that payment.

I do agree with our Investigator, however, that on the balance of probabilities I do think it would have made a difference if Revolut had intervened appropriately when Mr G made the second payment, which was for £10,299, that same day. Now in deciding this, I take on board that Mr G's final payment was discussed with him in-app on 28 April 2023 and this didn't make a difference, and also that the in-app warning about cryptocurrency investment scams hadn't made a difference. However, Revolut's in-app intervention on 28 April 2023 was focused on the possibility of Mr G falling victim to a safe account scam. Mr G was open in the chat with Revolut that the payment was to his own account to purchase cryptocurrency. But Revolut didn't probe or warn Mr G about cryptocurrency investment scams within this chat.

However, I'd expect Revolut to have been agile and dynamic in its responses, and Revolut has previously said itself that it's in-app chat is intended to be highly effective at uncovering scams. I think it's most likely Mr G would have been open in such an in-app chat with Revolut on 28 February 2023. I say this because he was upfront with Revolut on 27 and 28 April 2023 that his payments were for cryptocurrency. I've also listened to a recording of a telephone conversation Mr G had with a third-party bank, "Bank H", on 28 April 2023. The money Mr G lost from his Revolut account originated from his account with Bank H. And during this call on 28 April 2023, Bank H asked Mr G about the nature of his intended payment and Mr G said he had made an investment and he was trying to get it back, so he needed to buy some cryptocurrency to get it back. Mr G told Bank H that his broker was asking him to make the payment. I've also seen nothing in this call or elsewhere that makes me believe Mr G was being coached on what to say by the scammers, or that he was otherwise so under the spell of the 'investment' or scammers that he wouldn't have been open to an appropriately positioned warning that was impactful and pointed. But unfortunately I can't see that Mr G was provided with such a warning about the red flags he was being scammed.

I appreciate Revolut has pointed out that in its chat with Mr G on 28 April 2023 Mr G said he hadn't been asked to install any remote access software when this was apparently incorrect. But this could likely be influenced by the fact that Revolut's discussion with Mr G at that stage was about safe account scams. Revolut said, *"Have you been asked to install any apps (such as AnyDesk or TeamViewer) on your computer or phone?"*, and Mr G said, *"No, the account is mine. It's not a scam!"*. I think Mr G's focus was likely on his payment being to his own crypto account which he viewed as safe, not from a position of knowingly trying to mislead Revolut.

But on 28 February 2023, I think Revolut's intervention ought reasonably to have impactfully warned Mr G and uncovered a number of concerning red flags. Such that Revolut probably would have learnt that Mr G was making his payments for cryptocurrency as an 'investment opportunity'. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr G's payments – such as finding the investment on social media, being assisted by a 'broker', being asked to download remote access software. And this would be a large amount of money for Mr G to lose. So I think Revolut ought to have given Mr G robust warnings that the chances he was being scammed were very high indeed, such that its warnings in the in-app chat ought to have been robust.

In circumstances like this, I need to make up my mind based on the balance of probabilities, and I think it's fair to say that had this happened as I think it should have, it's more likely than not that such appropriately impactful warnings about cryptocurrency investment scams and information about how he could protect himself from the risk of fraud would have resonated with Mr G. He could have paused and looked more closely into the 'broker' or 'platform' before proceeding further, spoken to family or friends, as well as making further enquiries into cryptocurrency scams. I note there were some unfavourable reviews of the broker that Mr G would probably have seen had he been concerned enough to research more deeply at the time – which Revolut's impactful warnings most likely would have caused him to do. So whilst I acknowledge I can't be certain about things, I think it's more likely than not that a timely and impactful warning to Mr G from Revolut would most likely have caused him to take steps that would then have prevented his further losses to the scam from the second payment onwards.

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 the funds that Mr G lost from his Revolut account originated from his account with a third-party bank, "Bank H".

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 two (the one for £10,299), 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 from that point onwards. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mr G's own crypto accounts 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: Mr G has only complained about one respondent from which he is entitled to recover his 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 the second payment onwards (subject to a deduction for Mr G's own contribution which I will consider below).

Should Mr G bear any responsibility for his loss?

I've thought about whether Mr G should bear any responsibility for his losses, which from the second payment onwards amount to £111,829.12 In doing so, I've considered what the law

says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I agree with our Investigator about this. I don't think it's unfair to say Mr G wasn't as careful with these payments as I'd reasonably expect. Whilst I do think appropriate and timely warnings from Revolut would probably have made a difference, the fact remains that Mr G really ought to have been more careful with the payments and I would have expected him to researched things, in this particular case, more closely before sending so much money. Such that I'm satisfied that to reflect this Mr G should share equal responsibility with Revolut for the loss of £111,829.12. This means I'm satisfied Revolut should therefore pay Mr G a total of £55,914.56 (which is 50% of £111,829.12).

Recovery of funds

For completeness, I've considered whether Revolut unreasonably failed to recover Mr G's payments after they were made. But in the circumstances of this case where the payments were made to crypto accounts in Mr G's own name and then sent onto the scammers from there, before Mr G's notified Revolut that he'd been scammed, there wouldn't reasonably have been anything Revolut could have done to recover these funds for Mr G. So I can't say Revolut unreasonably missed an opportunity to recover the funds.

Interest

I consider 8% simple interest per year fairly reflects the fact Mr G has been deprived of this money. So Revolut should also pay Mr G interest on the £55,914.56 from the date of loss to the date of settlement calculated at this rate.

My final decision

For the reasons explained, I uphold this complaint in part and I direct Revolut Ltd to pay Mr G £55,914.56 plus interest on this amount calculated at 8% simple per year from the date of loss to the date of settlement. If Revolut deducts tax from this interest, it should provide Mr G with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 13 June 2025.

Neil Bridge
Ombudsman