DRN-4769270

The complaint

Mr A is complaining about Revolut Ltd because it declined to refund money he lost as a result of fraud.

What happened

Sadly, Mr A fell victim to a cruel job scam. He says he received a WhatsApp message from someone offering what he believed to be a genuine employment opportunity. He was required to complete sets of tasks that he had to pay up front (using cryptocurrency) to access on the promise of greater returns once the tasks were completed. Mr A received a small payment at the start but the scammers kept asking him to pay more and more money to recharge his account. When he tried to withdraw, he was told he needed to pay fees and taxes and this is when he realised he'd been scammed.

On the instruction of the scammers, Mr A set up an account with Revolut on 29 May 2023. He then used this account to make the following payments to the scammers that form this complaint:

No	Date & time	Amount £	Type	Payee	Notes
1	29/5 @ 18.32	85	Transfer	crypto provider 1	
2	31/5 @ 12.41	70	Transfer	individual	
3	3/6 @ 12.02	290	Transfer	individual	
4	3/6 @ 13.14	1,000	Transfer	crypto provider 2	Purpose - crypto
5	3/6 @ 14.53	1,000	Transfer	crypto provider 3	Purpose - crypto
6	3/6 @ 16.20	920	Transfer	individual	Purpose – crypto
7	3/6 @ 17.59	2,345	Transfer	crypto provider 3	Purpose - crypto
8	3/6 @ 19.30	650	Card	individual	Purpose - crypto
9	3/6 @ 20.17	1,711.90	Card	individual	Purpose - crypto
10	3/6 @ 20.21	1,711.90	Card	individual	Purpose - crypto
11	3/6 @ 20.24	100.70	Card	individual	
12	3/6 @ 21.33	3,030	Card	Andrii Peltek	Purpose - crypto
13	4/6 @ 5.23	400	Transfer	crypto provider 1	

I understand the payments to individuals were peer-to-peer cryptocurrency purchases. The notes section records that Mr A was asked a number of times about the purpose of the payments and, as shown, he consistently said he was purchasing cryptocurrency.

Mr A tried to make a further payment of £2,035 on 4 June but this was declined by Revolut.

Our investigator recommended the complaint be partly upheld. He felt Revolut should have contacted Mr A to discuss the purpose of the payments he was making before processing payment 7. If it had done, he felt the scam would have been stopped and he proposed Revolut should refund payments 7 to 13 with a deduction for Mr A's contribution to his losses.

Revolut didn't accept the investigator's assessment and made the following key points:

- It did provide warnings, including each time a new payee was entered and when Mr A said he was purchasing cryptocurrency.

- It has a duty to process payment instructions promptly and isn't required to assess their wisdom or the potential for loss.

- Its duty to protect customers has been overstated and the procedures it has in place are adequate for this purpose.

The complaint has now been referred to me for review.

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.

Having done so, I've reached the same overall conclusions as the investigator, and for broadly the same reasons. In deciding what's fair and reasonable, I'm 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. I haven't necessarily commented on every single point raised but concentrated instead on the issues I believe are central to the outcome of the complaint. This is consistent with our established role as an informal alternative to the courts.

In this case, there's no dispute that Mr A authorised the above payments.

In broad terms, the starting position at law is that an Electronic Money Institution (EMI) such as Revolut is expected to process payments a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of their account. In this context, *'authorised'* essentially means the customer gave the business an instruction to make a payment from their account. In other words, they knew that money was leaving their account, irrespective of where that money actually went.

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 A modified the starting position described in Philipp*,* by expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks" (Section 20).*

So, Revolut was required by the implied terms of its contract with Mr A and the Payment Services Regulations to carry out his instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

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

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

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

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with *"due skill, care and diligence"* (FCA Principle for Businesses 2), *"integrity"* (FCA Principle for Businesses 1) and a firm *"must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems"* (FCA Principle for Businesses 3)[3].

---

[1] The Payment Services Regulation 2017 Reg. 86(1) states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

[2] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018:https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

[3] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*

- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code[4], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in May 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;
- 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; and

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

- 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).

Taking these points into account, I need to decide whether Revolut acted fairly and reasonably in its dealings with Mr A.

This analysis is focussed on the situation regarding transfers as this was the nature of the payment where I think Revolut should have been able to stop the fraud for reasons I'll come to. I appreciate the situation is slightly different for card payments but I haven't covered this here as the differences don't affect my view on the outcome of the complaint.

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

One of the key features of a Revolut account is that it facilitates payments that sometimes involve large amounts and/or the purchase of cryptocurrency. For payments 1 to 6, based on what it knew about the payments and the amounts involved at the time it received Mr A's instruction, I don't think Revolut had cause to intervene any further than it did and I can't say it was wrong to debit his account accordingly.

But by the time of payment 7, Mr A had made five transfers on the same day with a total value of over £6,000, all of which it could see or had been told were for the purchase of cryptocurrency. Losses to cryptocurrency fraud reached record levels in 2022 and, by the end of that year, many high street banks had placed restrictions or additional friction on cryptocurrency purchases owing to the elevated fraud risk. So, by the time this payment took place, I think that Revolut should have recognised that payments to cryptocurrency carried a higher risk of being associated with fraud.

On balance, I think payment 7 is the point where Revolut should have identified the risk of fraud was increasing and attempted a more robust intervention.

What did Revolut do to warn Mr A?

Revolut has said it showed Mr A the following warning each time it registered a new payee:

> ***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.*

As outlined above, Revolut also asked about the purpose of a number of the payments. Each time Revolut says Mr A was also shown a series of warning screens, initially telling him about the amount lost to fraud each year and that fraudsters are professionals. He was then asked to confirm the purpose of the payment and, when he said he was purchasing cryptocurrency, he was shown a series of screens warning him about allowing someone else to access his account, downloading software and investing.

After reviewing these screens, I don't think the warnings provided were likely to be effective in this case. The new payee warning was very generic and the cryptocurrency warnings didn't particularly relate to the scam that was taking place. Of the options he was presented with, I'm satisfied it was reasonable for Mr A to answer that he was purchasing cryptocurrency. This is what the payments were actually for and there was no option in the list provided by Revolut for him to say he was paying money to work online.

What kind of warning should Revolut have provided?

While I think the interventions by Revolut were proportionate prior to payment 7, I believe it should have identified the likelihood these payments were associated with fraud had increased by the time of payment 7 and this is when further intervention should have been attempted.

Having thought carefully about the risk this payment presented, I think a proportionate response to that risk would have been for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mr A's account. I think it should have done this by, for example, directing him to its in-app chat to discuss the payment further.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr A suffered from payment 7?

If Revolut had spoken to Mr A via its in-app chat, it would have been able to ask open and probing questions about the payment, including what he was doing with the cryptocurrency he was purchasing.

On balance, I think it's most likely Mr A would have answered any questions truthfully. Within the limits of the questions he was asked in the app, I've already said that I believe Mr A was honest in saying he was purchasing cryptocurrency. There is evidence in his text chats with the scammer later on 4 June (after all of the above payments had been completed and when Mr A was being encouraged to pay further amounts) of the scammer telling him that banks don't like facilitating the purchase of cryptocurrency and that people normally say they're paying friends and family. But there's no evidence he was coached in this way at an earlier date. If he had been, and had been inclined to follow any advice to lie to the bank, he presumably wouldn't have said he was purchasing cryptocurrency when asked.

On the basis that he would likely have provided accurate information, I think Revolut should have been able to establish Mr A was ultimately making payments to access online work and the nature of the work he was undertaking. It should then have been able to identify that his circumstances bore many of the hallmarks of a task-based job scam and could have provided a clear and tailored warning setting out some of those common features. For example, that victims are often approach online by someone they've never met, required to pay money to access work (often in cryptocurrency), promised high returns for a limited amount of work, asked to pay increasing amounts to access that work, and additional amounts when they try to withdraw what they're owed.

If Mr A had received such a warning, I think it's likely he'd have recognised his own situation and that it would have resonated with him, leading to the scam being uncovered. Following such a warning, I think it's likely Mr A would have opted not to continue with the payment.

My conclusion on this point is reinforced by information from one of the banks Mr A used to transfer money to Revolut to fund the cryptocurrency purchases. I've listened to a recoding of a phone call with Mr A from later on 4 June (after all of the above payments were made) when he tried to transfer a further amount to Revolut. During this call, Mr A said he was purchasing cryptocurrency and, following a warning from the agent that cryptocurrency is linked to a large number of scams, he decided not to proceed with that transfer. I think this shows he was receptive to this kind of human intervention.

I think it follows that if the scam had been uncovered at the point of payment 7, payments 8 to 13 would also have been prevented.

What about the actions of Mr A's banks?

This was a multi-stage fraud that saw Mr A move money from two different banks to Revolut and then eventually onto the scammer. This complaint is about Revolut and it's not appropriate for me to comment here on whether or not the bank should have identified he was at risk of harm from fraud and whether it reacted proportionately. But to obtain a full picture of what took place, we have contacted the banks to establish if they attempted any kind of intervention before transferring his money to Revolut and, if so, how this affects my assessment of whether or not he acted reasonably in the circumstances.

Aside from one of the banks asking Mr A about the reason for one of the payments, which it says generated no further warning, both banks have told us there was no intervention attempted on any of the transfers related to this scam. Both banks have also confirmed they've not received a complaint from Mr A.

As I've said above, one of the banks did speak to Mr A on the phone about an attempted transfer to Revolut but this was after the list of payments above was concluded. But, on balance, I don't think there was any intervention by Mr A's banks before the above payments were finalised that should particularly have alerted him to the fact he was speaking to a scammer or that changes my views about how Revolut should have dealt with this situation and whether he acted reasonably in the circumstances with which he was faced.

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

In reaching my decision about what's fair and reasonable, I have taken into account that the payments either went to accounts in Mr A's own name or purchased cryptocurrency that went to account in his own name, rather than directly to the scammer, so he remained in control of the money after he made those payments, and there were further steps before the money was lost to the scammer.

However, for the reasons I've set out above, I'm satisfied it would be fair to hold Revolut responsible for Mr A's loss from payment 7, subject to a deduction for his own contribution towards this. 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.

I have also taken into account that other businesses were involved in the overall process that ended up with payments being made to the scammer, and that Mr A might potentially have a claim against them in in respect of their actions (although those businesses are not a party to this complaint and so I make no finding about their role here).

Whilst the dispute resolution rules (DISP) give me the power (but do not compel me) to require a financial business to pay a proportion of an award in circumstances where a consumer has made complaints against more than one financial business about connected circumstances, Mr A has not referred a complaint about any other business to me and DISP does not empower me to instruct him to make or refer a complaint to me about another business.

Should Mr A bear any responsibility for his losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I've considered the evidence carefully and, while I accept Mr A genuinely believed these payments were being made in connection with a legitimate employment opportunity, I'm not persuaded that belief was a reasonable one.

The arrangement was very different to the normal employer-employee relationship. In most circumstances, people expect to be paid by their employer, rather than the other way around. In addition, the returns being promised don't appear to have been consistent with the nature and amount of work Mr A was being asked to do – I note in the initial chats with the scammer he was told he'd only need to work for two or three hours per day. I think these issues should have aroused some suspicion about whether the opportunity was genuine.

In the circumstances, I think Mr A should have proceeded only with great caution. If he had carried out any further research, for example online searches, I think he'd have quickly discovered his circumstances were similar to those commonly associated with many job scams. Overall, I think it's fair and reasonable for Revolut to make a 50% deduction from the redress payable.

Recovery of funds

I've also looked at whether Revolut could or should have done more to try and recover Mr A's losses once it was aware that the payments were the result of fraud.

For the peer-to-peer cryptocurrency purchases, Mr A made legitimate purchases of cryptocurrency that was transferred to an account under his control, albeit briefly. In those circumstances, we wouldn't expect the business to be able to recover funds from a (most likely) genuine seller of cryptocurrency who wasn't involved in the scam.

With the other payments, Mr A transferred funds to a legitimate cryptocurrency account in his own name. From there, he purchased cryptocurrency and moved it onto a wallet address of his choosing (albeit on the scammers' instructions). If Revolut tried to recover the funds, it could only have tried to do so from Mr A's own account and it appears all the money had already been moved on and, if not, anything that was left would still have been available to him to access.

As some of the payments were card payments, I've considered whether Revolut should have tried to recover the money through the chargeback scheme. This is a voluntary agreement between card providers and card issuers who set the scheme rules and is not enforced by law.

A chargeback isn't guaranteed to result in a refund, there needs to be a right to a chargeback under the scheme rules and under those rules the recipient of the payment can defend a chargeback if it doesn't agree with the request. Unfortunately, the chargeback rules don't cover scams.

We'd only expect Revolut to have raised a chargeback claim if it was likely to be successful and it doesn't appear that would have been the case here. Mr A made legitimate purchases of cryptocurrency and would have received what he paid for. His disagreement is with the scammer, not the cryptocurrency seller and it wouldn't have been possible for Revolut to process a chargeback claim against the scammer as he didn't pay them directly.

Taking all of these factors into account, I don't think anything that Revolut could have done differently would have led to these payments being successfully recovered.

In conclusion

For the reasons I've explained, I don't think Revolut acted fairly and reasonably in its dealings with Mr A and I'm upholding this complaint in part. While I don't think it acted incorrectly in processing payments 1 to 6 in line with Mr A's instructions, if it had carried out an appropriate intervention before payment 7 debited his account, I'm satisfied payments 7 to 13 would have been prevented.

Putting things right

The principal aim of any award I make must be to return Mr A to the position he'd now be in but for the errors or inappropriate actions of Revolut, while allowing for any responsibility he should reasonably bear. If Revolut had carried out an appropriate intervention as I've described, I'm satisfied the scam would have been stopped and Mr A would have retained the money that was lost from payment 7 onwards. As outlined above, I've applied a 50% deduction to the amounts to be refunded in recognition of Mr A's own contribution towards the loss.

I can see that Mr A received modest payment back from the scam, but these amounts related to payments that pre-dated payment 7 so I haven't taken account of them here.

To put things right, Revolut should pay Mr A compensation of A + B, where:

- A = a refund of 50% of each of payments 7 to 13 outlined above; and

- B = simple interest on each amount being refunded in A at 8% per year from the date of the corresponding payment to the date compensation is paid.

Interest is intended to compensate Mr A for the period he was unable to use this money. HM Revenue & Customs (HMRC) requires Revolut to deduct tax from any interest. It must provide Mr A with a certificate showing how much tax has been deducted if he asks for one.

I'm satisfied this represents a fair and reasonable settlement of this complaint.My final decision

My final decision is that I partly uphold this complaint. Subject to Mr A's acceptance, Revolut Ltd should now put things right as I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 25 March 2025.

James Biles
Ombudsman