DRN-4447131

The complaint

Mrs T complains that Revolut Ltd (Revolut) is refusing to refund her the amount she lost as the result of a scam.

Mrs T is being represented by a third party. To keep things simple, I will refer to Mrs T 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, Mrs T was contacted via WhatsApp about a job role by a scammer I will call X. Mrs T had been looking for a job and uploaded her CV online, so the message was not unexpected.

The job was described as boosting products in the marketplace. Mrs T was provided with access to X's platform and was required to make deposits via a cryptocurrency exchange and complete tasks to simulate buying various products from which she would receive a commission.

However, every time Mrs T completed a task the payment needed to continue increased. The payments being requested increased further and further until Mrs T could no longer afford to continue to make them.

Mrs T found she was unable to make a withdrawal from the platform and realised she had been scammed.

Mrs T made the following payments in relation to the scam:

Payment	Date	Payee	Payment Method	Amount
1	7 February 2023	Binance	Debit Card	£100
2	7 February 2023	Binance	Debit Card	£78
3	9 February 2023	Binance	Debit Card	£350
4	9 February 2023	Binance	Debit Card	£150
5	9 February 2023	Binance	Debit Card	£20
6	9 February 2023	Binance	Debit Card	£15
7	10 February 2023	Binance	Debit Card	£350
8	11 February 2023	Binance	Debit Card	£650
9	11 February 2023	Binance	Debit Card	£1700
10	11 February 2023	Binance	Debit Card	£3250
11	11 February 2023	Binance	Debit Card	£5000
12	11 February 2023	Binance	Debit Card	£4700
13	13 February 2023	Binance	Debit Card	£5000
14	13 February 2023	Binance	Debit Card	£5000
15	13 February 2023	Binance	Debit Card	£5000
16	13 February 2023	Binance	Debit Card	£5000

17	13 February 2023	Binance	Debit Card	£3000
18	13 February 2023	Binance	Debit Card	£2000

Our Investigator considered Mrs T's complaint and thought it should be upheld in part. Revolut disagreed, in summary Revolut said:

- Not all the points raised by Revolut have been covered in the assessment made by the investigator
- While the FOS is permitted to depart from the law, if they do so they should say so in their decision and explain why [R (Heather Moor & Edgecomb) v Financial Ombudsman Service [2008] EWCA Civ 642, [49] (Stanley Burnton LJ)]. If the Ombudsman purports to apply the law, or legal duties, they must do so correctly and if they err in law, "they are susceptible to judicial review on grounds of error of law in relation to their identification of what the relevant law is, as well as perversity and irrationality in relation to their substantive decisions." - [See further R (on the application of Shawbrook Bank Ltd) v Financial Ombudsman Service Ltd; R. (on the application of Clydesdale Financial Services Ltd (t/a Barclays Partner Finance)) v Financial Ombudsman Service [2023] EWHC 1069 (Admin), [13]]. Revolut does not believe that this case has been properly adjudicated.
- 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.
- 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.

As this complaint could not be resolved informally it 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 Mrs T 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 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;

[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_/

- 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 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 customers' 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 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 February 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Mrs T was at risk of financial harm from fraud?

It isn't in dispute that Mrs T has fallen victim to a cruel scam here, nor that she authorised the payments that she has disputed.

Whilst I have set out in detail in this decision the circumstances which led Mrs T to make the payments using her 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 Mrs T might be the victim of a scam.

The first payments Mrs T made in relation to the scam were not of such a significant value that I would have expected Revolut to have had any concerns.

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Mrs T's name.

By February 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 February 2023, when these payments took place, further restrictions were in place. 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 Mrs T made in February 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, I'm not suggesting as Revolut argues that, as a general principle, 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 February 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 Mrs T'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 Mrs T might be at a heightened risk of fraud that merited its intervention.

---

[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.

I think Revolut should have identified that the payments Mrs T made in relation to the scam were going to a cryptocurrency exchange (the merchant is a well-known cryptocurrency exchange), but the first 9 payments were not of such a high value, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

However, payment 10 was for a more significant value of over £3,000 and was the third payment Mrs T had made the same day to the same cryptocurrency exchange. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mrs T 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 Mrs T before this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment which ought to have prompted a warning.

What did Revolut do to warn Mrs T?

Revolut has confirmed that the payments in dispute were 3DS authorised, but Revolut did not intervene when any of the payments were made.

What kind of warning should Revolut have provided?

Payment 10 was the third payment Mrs T had made the same day to a well-known cryptocurrency exchange, with the values of each of the payments increasing each time. I think this should have caused Revolut to have had significant concerns.

Having thought carefully about the risk payment 10 presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mrs T's account. I think it should have done this by, for example, directing Mrs T 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 Mrs T suffered from payment 10?

Had Mrs T told Revolut that she was offered a job through WhatsApp that required her to make payments via a cryptocurrency exchange to complete various tasks, it would have immediately recognised that she was falling victim to a scam. It would have been able to provide a very clear warning and, given that Mrs T had no desire to lose her money it's very likely that she would have stopped, not followed the fraudster's instructions and her loss would have been prevented.

So, I've considered whether Mrs T would have given honest answers had she been questioned appropriately. It doesn't appear that Mrs T was given a cover story by the scammer for what she should say if she was questioned about the payments, so I don't have enough to say Mrs T would not have given honest answers.

Ultimately, as Revolut didn't question the payments Mrs T made, it can provide no compelling evidence that she would have misled it about the purpose of the payments or the surrounding circumstances.

So, Revolut should, once it had established why Mrs T was making the payments, provided a very clear warning that Mrs T was likely falling victim to a scam. I think, on the balance of

probabilities, that's likely to have caused Mrs T to stop.

I'm satisfied that had Revolut established the circumstances surrounding payment 10, as I think it ought to have done, and provided a clear warning, Mrs T's loss from and including payment 10 would have been prevented.

Is it fair and reasonable for Revolut to be held responsible for Mrs T's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs T purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that the payments were made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from other accounts at regulated financial businesses.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs T might have been at risk of financial harm from fraud when she made payment 10, 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 Mrs T suffered. The fact that the money used to fund the scam came from elsewhere or wasn't lost at the point it was transferred to Mrs T's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs T'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 Mrs T 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 Mrs T could instead, or in addition, have sought to complain against those firms. But Mrs T has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mrs T's compensation in circumstances where: Mrs T has only complained about one respondent from which she is entitled to recover her 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 Mrs T's loss from payment 10 (subject to a deduction for Mrs T'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 and having done so I still find it reasonable to hold Revolut responsible for Mrs T's loss.

Should Mrs T bear any responsibility for her 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 on the basis that Mrs T should share blame for what happened.

Mrs T was sent a message via WhatsApp and offered a job opportunity without any formal interview process. No contract of employment was exchanged, and Mrs T was required to make multiple payments via a cryptocurrency exchange before she could make a withdrawal.

I don't think the above could be considered usual in any legitimate role and should have caused Mrs T to have concerns. Had Mrs T taken more care as I think she could have she could have carried out further research or sought advice and have prevented her loss.

Could Revolut have done anything to recover Mrs T's money?

As the payments were made by card and sent to a cryptocurrency account held in Mrs T's name, Revolut would not have been able to recover the funds. I don't consider that a chargeback would have had any prospect of success given there's no dispute that the cryptocurrency was provided to Mrs T, which she subsequently sent to the fraudsters.

Putting things right

To put things right I require Revolut Ltd to:

- Refund 50% of the payments Mrs T made in relation to the scam from payment 10 onwards less any payments received.
- Add 8% simple interest per year to the amount it pays Mrs T from the date of loss to the date the payment 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 Mrs T to accept or reject my decision before 21 February 2025.

Terry Woodham
Ombudsman