DRN-4963953

## The complaint

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

## What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Miss S tells us she was expecting a delivery from a delivery company and received a message asking her to rearrange the delivery. Miss S says the message was convincing and appeared to come from a genuine number associated with the delivery company. Miss S says she followed a link in the message and inputted her card details as requested.

Miss S then received a call from a scammer (X). The call appeared to come from a number associated with Revolut. Miss S tells us the caller knew her full name and address, her phone number, and the last digits of her bank card. Miss S says this helped convince her that she was receiving a genuine call.

X asked Miss S to confirm she had received a message from the delivery company about a missed delivery. Miss S confirmed she had, and that she was expecting a delivery. Miss S gave a description of the message she had received and said she had clicked the link in the message and inputted her card details as requested.

X explained that Miss S was being targeted in a common scam and provided Miss S with a link outlining the scam details.

X asked Miss S to confirm several transactions that it had stopped leaving her account. Miss S confirmed she had not made the payments and that she could not see them on her Revolut app. X explained Miss S would not be able to see the payments as it had managed to stop them being processed.

X explained that her phone and Revolut app including her savings had been compromised. X provided a code via a message that appeared to come from a Revolut number once again to confirm she was on a safe call.

X then explained to Miss S that it would need to set up a safe account for her money to be moved to until a new account had been setup for her. Miss S says X was very convincing and walked her through the process in detail. X even appeared to be seeing the same screens Miss S was seeing at the time.

Miss S tells us she then received a payment request from a crypto exchange for the value of £8,795. X told Miss S that this was a safe account that only Revolut had access to. Miss S says she found this explanation convincing and confirmed the payment.

Miss S was asked to make several other payments that appeared to be blocked by the

Revolut App. After the unsuccessful attempts X stopped communicating with Miss S and she realised she had fallen victim to a scam.

In total Miss S has lost £8,795 to the scam via one card payment made on 28 October 2023.

Our Investigator considered Miss S's complaint and thought it should be upheld. Revolut disagreed. In summary it argued:

- The payment in question cannot be considered unusual as Miss S had made a previous large payment from her account the month before.
- Revolut is bound by contract, applicable regulations, and the common law to execute valid payment instructions.
- 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.
- Our service appears to be treating Revolut as if it were a signatory to the CRM Code.
- 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 an informal agreement could not be reached, the complaint has been passed to me for a final 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 Miss S 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*".

In this respect, section 20 of the terms and conditions said:

> *"**20. When we will refuse or delay a payment***
> *We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:*
> - *If legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks;*
> - *…"*

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

I am satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in October 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.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment, and I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp*.

I have taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I am also mindful that in practice, whilst its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But 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 October 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 do 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 October 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).
- 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

[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_/

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[2], 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).
- Since 31 July 2023, under the FCA's Consumer Duty[3], regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"*[4].
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[5] 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 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 October 2023 that Revolut should:

---

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

[3] Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

[4] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

[5] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

- 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 acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- 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 October 2023, Revolut should in any event have taken these steps.

*Should Revolut have recognised that Miss S was at risk of financial harm from fraud?*

The payment Miss S authorised was for a significant value and although Miss S had made a previous large payment, it was being made to a well-known cryptocurrency exchange, which in October 2023 I consider carried additional risk of financial harm from fraud, despite the fact the payment may have credited a cryptocurrency account held in Miss S' own name. In addition, Miss S had not made crypto related payments before, so the activity was not typical for her account. I think that the combination of the unusually high value payment and the recipient should have led Revolut to consider that Miss S was at a heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Miss S before this payment went ahead.

*What did Revolut do to warn Miss S?*

Revolut provided an in-app payment confirmation screen that provided the name of the payee and the option to confirm the payment. While this confirmed Miss S was agreeing to make the payment, it did not highlight any possible risks related to it.

While I don't discount the above entirely, it is very general in nature and it's difficult to see how it would resonate with Miss S or the specific circumstances of the transaction in question. I don't think that providing the above in relation to the payment was a proportionate or sufficiently specific mechanism to deal with the risk that the payment presented. I think Revolut needed to do more.

*What kind of warning should Revolut have provided? And would that have prevented the losses Miss S suffered?*

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.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

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 identifying the 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 October 2023, when this payment 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 October 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.

Taking that into account, I am satisfied that, by October 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Miss S made the payment, 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 she was making – have provided a scam warning tailored to the likely scam Miss S was at risk from.

In this case, Miss S was falling victim to a 'safe account scam' – she believed she was sending money from her account to keep it safe.

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 Miss S gave. I'd expect any such warning to have covered off key features of such a scam, such as being asked to move money to a safe account because the account was compromised in some way.

I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Miss S 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 the payment 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.

But I am not persuaded that 'safe account scams' would have been disproportionately difficult to identify through a series of automated questions (as demonstrated by Revolut's current warnings – which seek to do exactly that) or were not sufficiently prevalent at the time that it would be unreasonable for Revolut to have provided warnings about them, for example through an automated system.

I accept that under the relevant card scheme rules Revolut cannot delay a card payment, but in the circumstances of this case, I think it is fair and reasonable to conclude that Revolut ought to have initially declined the payment in order to make further enquiries and with a view to providing a specific scam warning of the type I've described. Only after that scam warning had been given, if Miss S attempted the payment again, should Revolut have made the payment.

*Should Miss S bear any responsibility for her 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.

In the circumstances I don't think it would be fair to say Miss S contributed to the loss. I say this because Miss S had been expecting a delivery when she received the initial message, and all the correspondence Miss S received appeared to come from legitimate sources with X using spoofing techniques.

X was also very convincing walking Miss S through the screens she was seeing on her own device, on the Revolut App.

I can't see that in the circumstances and under the pressure placed on Miss S by the scammer, that she would have considered anything to be a red flag.

However, had Revolut stopped the payment and found that it was being made in relation to a safe account I think it is likely that Revolut would have stopped the payment altogether, as it should have, and that once given a warning about the specific circumstances of the payment likely being a scam, that Miss S would also have stopped attempting the payment.

**Putting things right**

To put things right I require Revolut Ltd to:

- refund the payment Miss S made in relation to the scam
- Pay 8% simple interest per annum (less tax lawfully deductible) on the refunded amount, from the date of loss to the settlement date.

## 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 Miss S to accept or reject my decision before 15 November 2024.

Terry Woodham
**Ombudsman**