DRN-5175262

## The complaint

Miss M complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by a safe account scam, or to help her recover the money once she'd reported the scam to it.

## What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

On 15 November 2023, Miss M was contacted by someone who I'll refer to as "the scammer", who claimed to work for Bank B. The scammer said her accounts with Bank B, Bank M and Bank S had been compromised. He knew Miss M's personal details, including her full name and date of birth, and told her to verify he was genuine by checking that the telephone number he was calling from matched with the contact number on Bank B's website, which it did.

The scammer told Miss M to check her account and she saw there was a £5 payment to an unknown payee. He said Bank B, Bank M and Bank S were all affiliated and as there was a fraudulent payment from Bank B, her other accounts were also at risk, so she'd need to send all her money to R to ensure it was safe. She then received a call from someone who claimed to be calling from Revolut who talked her through how to transfer funds from Bank B, Bank M, and Bank S to her Revolut account, telling her it needed to be done quickly to avoid losing her funds. The scammer asked her to provide the details of her virtual card and explained that she'd receive a notification in the Revolut app, which she confirmed. Unfortunately, in doing so, she authorised the transfer of £5,130 from her Revolut account to a cryptocurrency account to which she didn't have access.

Miss M realised she'd been scammed when the scammer hung up the phone and she was unable to contact him. She complained to Revolut, but it said there was no fraudulent activity on the account and the transactions were approved via its 3DS authentication system, so there was no valid chargeback under the card scheme rules.

She wasn't satisfied and so she complained to this service arguing that Revolut should have stopped the payments because she rarely made large payments from the account and hadn't previously sent payments to cryptocurrency merchants. She also said she wanted compensation for the poor customer service she'd received, complaining Revolut was rude and unhelpful, and she was only offered communication via live chat, which caused upset and anxiety.

Revolut said its controls were proportionate and appropriate and it had acted promptly to recover any potential losses. It said there were no chargeback rights because the transactions were authenticated via 3DS, and it had been performed to a genuine merchant that had provided a specific service. It said the fraudulent activity didn't take place on the Revolut platform because it was used as an intermediary to receive funds from Miss M's main bank account and then transfer on to legitimate external cryptocurrency accounts, from where she lost control of the funds.

It said there was no spending history it could have used to determine normal account activity, and Miss M should have done more due diligence before making the payment, commenting that she wasn't taken through security and the in-app notification would have shown the name of the payee, which should have raised concerns.

Revolut also cited the Supreme Court's judgment in Philipp v Barclays Bank UK plc [2023] where it was held that in the context of APP fraud, where the validity of the instruction is not in doubt, no inquiries are needed to clarify or verify what the bank must do. It argued that the transaction was to an account in Miss M's own name, and for this service to effectively apply the reimbursement rules to self-to-self transactions is an error of law, and there's no rational explanation as to why it should be held responsible for Miss M's loss.

Our investigator recommended that the complaint should be upheld, explaining that Revolut knew the payment was to a cryptocurrency merchant, so it should have questioned Miss M about the payment in an attempt to narrow down the specific scam risk. And once the risk had been identified, it should have provided a warning covering off the key features of the risk.

She said she'd have expected Revolut to ask why she was sending funds to a cryptocurrency merchant and as Miss M didn't realise she was paying a cryptocurrency merchant, she was satisfied this would've raised concerns. She also thought it was likely Miss M would've mentioned that she was moving funds to a safe account in response to which Revolut would have warned her about safe account scams.

Our investigator concluded that Revolut should refund the money Miss M had lost, and she explained she didn't think there should be a reduction for contributory negligence because even though she should've known that banks don't ask customers to share sensitive information, the scammer had her personal details, there was a £5 payment pending from Bank B and the scam occurred in less than 30 minutes, so she didn't have time to consider what she was being asked to do. So, she didn't think it was unreasonable that she fell for the scam.

Finally, our investigator accepted the service Revolut provided could've been better, but she didn't think it would've lessened the impact of the scam because most of the distress Miss M experienced was caused by the scammer. So, she didn't think she was entitled to any compensation. And she didn't think Revolut had acted unfairly when it considered Miss M's chargeback request.

Revolut has asked for the complaint to be reviewed by an Ombudsman. It has argued that Miss M paid a legitimate cryptocurrency account in her own name, so the fraudulent activity didn't occur on the Revolut platform. It explained it is an Electronic Money Institute (EMI) and, typically, this type of account is opened and used to facilitate payments of a specific purpose and often not used as a main account, so the payment wasn't out of character or unexpected.

It has further argued that this service's recent reliance on R (on the application of Portal Financial Services LLP) v FOS is misconceived and amounts to a legal error, and as the funds originated in Miss M's own external accounts, other bank interventions are relevant.

**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.

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 M 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 M 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 November 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 November 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]

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

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

For example, it is my understanding that from October 2023, Revolut operated a process whereby if it identified a scam risk associated with a card payment through its automated systems, it might initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat). If Revolut was satisfied with the response to those questions and/or it provided a relevant warning, the consumer could use the card again to instruct the same payment and Revolut would then make the payment.

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 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

[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.

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 November 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 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.

---

[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.

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 November 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Miss M has fallen victim to a cruel scam here, nor that she authorised the payment. Whilst I have set out in detail in this decision the circumstances which led her to make the payment using her Revolut account and the process by which that money ultimately fell into the hands of the scammer, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether the payment presented an increased risk that Miss M might be the victim of a scam.

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 payment would be credited to a cryptocurrency wallet held in Miss M's name.

Revolut didn't intervene before the payment was processed. By November 2023, when this transaction 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. And by November 2023, when this payment 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 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 payment Miss M made in November 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 (under the Consumer Duty or otherwise), Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees.

As I've set out in some detail above, it is the specific risk associated with cryptocurrency in November 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm. In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements (including the Consumer Duty), Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained, Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payment was going to an account held in Miss M's own name should have led Revolut to believe there wasn't a risk of fraud. I think it should have identified that the payment was going to a cryptocurrency provider and based on the value of the payment and the fact she hadn't previously made payments for cryptocurrency, I think that the circumstances should have led Revolut to intervene before the payment went ahead.

*What kind of warning should Revolut have provided?*

I've thought carefully about what a proportionate warning in light of the risk presented by this payment. 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 the payment was 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 November 2023, 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 consider that by November 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 the payment was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation and investment scams. Taking that into account, I am satisfied that Revolut ought to have attempted to narrow down the potential risk further.

I'm satisfied that when Miss M made the payment, Revolut should have asked a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making and have provided a scam warning tailored to the likely cryptocurrency related scam she was at risk from. In this case, Miss M was falling

victim to a ‘safe account scam’ – she believed she was making the payment because her other accounts had been compromised. Once the risk had been established, it should have provided a warning which was tailored to that risk and the answers she gave.

I’d expect any such warning to have covered off key features of a safe account scam. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I’ve seen nothing to indicate that Miss M wouldn’t have done so here. I also accept that there are a wide range of scams that could involve payments to cryptocurrency providers and 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 a safe account scam would have been disproportionately difficult to identify through a series of automated questions 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.

As I have explained above, the Consumer Duty (which came into force on 31 July 2023 after an extended implementation period), required Revolut to take steps to avoid foreseeable harm – for example by having adequate systems in place to detect and prevent scams from 31 July 2023. As I’ve set out, 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.

*If Revolut had provided a warning of the type described, would that have prevented the losses Miss M suffered?*

I’ve no reason to think Miss M wouldn’t have declared that she was moving money to a safe account and provided more detail about the payment if requested. I think based on the circumstances of the scam, she’d have had immediate concerns when she was warned about safe account scams, and, given she didn’t know the funds were being sent to a cryptocurrency merchant, I think she’d have realised she’d been scammed when she realised the scammer had mislead her about the nature of the payee.

*Is it fair and reasonable for Revolut to be held responsible for Miss M’s loss?*

As I’ve set out in some detail above, I think that Revolut should have recognised that Miss M might have been at risk of financial harm from fraud when she made the payment, 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 she suffered.

The fact that the money used to fund the scam came from elsewhere and wasn’t lost at the point it was transferred to Miss M’s own account does not alter that fact and I think Revolut can fairly be held responsible for the 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. Miss M has complained about Bank

B, but the complaint wasn't upheld, and, in those circumstances, I can only make an award against Revolut.

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. Rather, it is asking me to consider all the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved, which I have done.

*Should Miss M bear any responsibility for her loss?*

I've considered whether Miss M contributed to her own loss and while I accept she ought reasonably to have been alarmed at having been asked for her account details, it's significant that she was put under pressure to act quickly and that she was reassured the scammer was genuine because he knew her personal details, alerted her that there was a £5 payment from Bank B, and appeared to be calling from the number advertised on Revolut's website. Further, Miss M was tricked into authorising the payment and while I accept she could have identified the scam if she'd noticed the name of the merchant, I think the time pressure is a reasonable explanation for why she didn't notice the discrepancy. So, I don't think she contributed to her own losses.

*Recovery*

Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency merchant would have been able to evidence they'd done what was asked of them. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to raise a chargeback request was fair.

*Compensation*

While I accept that Miss M was dissatisfied with the way Revolut communicated with her when she reported the scam, I'm satisfied the main cause of her upset was the scammers who persuaded her to part with her funds and so I don't think she is entitled to any compensation.

**My final decision**

My final decision is that Revolut Ltd should:

- refund the money Miss M lost to the scam.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Miss M with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 10 February 2025.

Carolyn Bonnell

**Ombudsman**