

The complaint

Mrs S is unhappy that Revolut Ltd won't reimburse money she lost to a scam.

What happened

Mrs S was searching for a job opportunity. She says she left her contact details with several online recruitment websites.

She was contacted over a popular instant messaging application by someone claiming to represent a well-known recruitment firm. They claimed to have jobs available – with part-time roles paying £35-55 per hour and full-time roles paying up to £1,100 a week. They claimed that *'no contracts or investments were involved'*.

After she expressed interest, Mrs S was contacted by a second person – "M", who claimed to represent the employer. M explained that the role would involve trying to boost the rating and ranking of applications on various app stores and that the owner of the applications would pay for this service. M provided a link to a website – "F". M said that Mrs S could, in fact, earn a salary of around £5,000 a month which would be paid in USDT (a US Dollar-linked 'stablecoin').

Over the following few days Mrs S was told how to use the website and that her job would actually involve completing assigned 'tasks' to earn commission. Mrs S opened an account on F. It displayed her tasks, 'earnings' that day and her overall 'balance'. M explained that Mrs S would sometimes be granted 'combination tasks', which required a group of tasks to be completed before any withdrawal could take place. Each combination task had a value, given in USDT. Each time a combination task was assigned, the value of the task in USDT would be deducted from Mrs S' balance on F. That would leave Mrs S with a negative balance that, it was claimed, would need to be made positive (by depositing USDT into her account at F) before any withdrawals could be made (both of earned commission and the money that she'd paid to the platform). All of the money she paid to the platform was supposedly refundable as long as the tasks were completed.

In order to add money to her account at F, Mrs S was instructed to convert her money into USDT. She principally used two cryptocurrency exchanges – "M" and "B" in order to do this. She also sent money to individuals who were selling cryptocurrency on B's 'peer-to-peer' exchange platform. Once the cryptocurrency had credited her accounts at M and B, she sent it to cryptocurrency wallet addresses provided by the fraudsters and that cryptocurrency then appeared on her account at F.

But, before Mrs S could remove her negative balance and withdraw her money, she'd be given another combination task of a greater value – meaning she'd have to complete those tasks (and therefore make another payment) before accessing her money. When Mrs S questioned this, she was told that she couldn't cancel the tasks, they had to be completed and if she didn't resolve the negative balance on her account she'd lose all of her money – both the commission she'd earned and the money she'd paid.

The assignment of these combination tasks was apparently random and fortunate (given that Mrs S would be paid more for completing combination, rather than regular, tasks). In fact, it is these tasks which are integral to the scam. It is that dynamic that leaves a withdrawal always just out of reach and the scam tends to go on for as long as the fraudsters are able to persuade the victim to keep making payments. Mrs S appears to have recognised the problem with this arrangement prior to making any of the larger payments on 18 August 2023 as she asks the fraudster whether her account at F will be put into a negative balance again by a combination task. The fraudster assures her that the assignment of combination tasks is random.

In this case, as is common with this type of scam, the initial payments were modest in value, before increasing significantly. A table of payments from Mrs S' Revolut account is below.

| Payment number | Date and time | Type of payment | Amount | Recipient |
|----------------|-----------------------|-------------------------------------|------------------|---|
| 1 | 13 August 2023, 21:27 | Debit card payment | £12.04 | Mrs S' cryptocurrency account at M |
| 2 | 15 August 2023, 20:12 | Transfer (to Revolut sister entity) | £36 | Unknown third-party 1 (peer-to-peer purchase of cryptocurrency) |
| 3 | 17 August 2023, 16:04 | Transfer ('push-to-card' payment) | £78.54 | Unknown third-party 2 (peer-to-peer purchase of cryptocurrency) |
| 4 | 17 August 2023, 17:58 | Transfer ('push-to-card' payment) | £68.00 | Unknown third-party 3 (peer-to-peer purchase of cryptocurrency) |
| 5 | 17 August 2023, 18:16 | Debit card payment | £48.02 | Mrs S' cryptocurrency account at M |
| 6 | 18 August 2023, 14:05 | Debit card payment | £1,788.83 | Mrs S' cryptocurrency account at B |
| 7 | 18 August 2023, 16:13 | Debit card payment | £3,408.51 | Mrs S' cryptocurrency account at B |
| | Total | | £5,439.94 | |

On 18 August 2023, just hours after the final two payments, and after it became clear she'd need to pay even more money to F, Mrs S reported the matter to Revolut as a scam. It said that it couldn't refund the payments in dispute. In relation to the card payments, it said that as a service had been provided (the provision of cryptocurrency) it could not raise a chargeback. It said that one of the transfers had gone to its sister entity in another country and it couldn't recover the payment without the consent of the account holder or local authorities. It explained that the other payments were 'push-to-card' payments which could not be disputed through the chargeback scheme or recovered. Push-to-card payments allow money to be sent directly (and normally instantly) to a person's bank account via a linked debit card without the need to exchange an account number and sort code.

Revolut has made a number of other arguments to support its position, which I've summarised below:

- 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.
- It would not be required to reimburse ‘self-to-self’ transactions even if it were a signatory to the Lending Standards Board’s Contingent Reimbursement Model Code (“CRM Code”). Our service appears to be treating Revolut as if it were a signatory to the CRM Code.
- The Payment Service Regulator’s (“PSR”) mandatory reimbursement scheme will not require it to refund payments made in these circumstances either.
- ‘Self-to-self’ payments don’t meet either the Dispute Resolution Rules (“DISP Rules”) or CRM Code definition of an APP scam.
- Mrs S was grossly negligent by ignoring the warnings it gave. The PSR’s mandatory reimbursement scheme will allow it to decline claims where a consumer has been grossly negligent, taking into account any warnings a firm has provided.
- Mrs S’ loss did not take place from her Revolut account as she (largely) made payments to her own cryptocurrency wallet before transferring that cryptocurrency to the fraudster. It’s unfair and irrational to hold Revolut responsible for any of the loss where it is only an intermediate link in a chain of transactions. Other firms will have a better understanding of the destination of the funds and/or Mrs S’ finances and account activity.

Mrs S referred the matter to our service through a professional representative. One of our Investigators looked into the complaint but didn’t uphold it. The Investigator thought that Revolut should have provided a written warning for the second payment (the card payment of £3,408.51) on 18 August 2023 – “the Final Payment”, but their view was that warning should have covered off the most common scam risk associated with cryptocurrency payments – cryptocurrency investment scams. As Mrs S wasn’t falling victim to a cryptocurrency investment scam, the Investigator didn’t think such a warning would have made a difference to Mrs S’ decision to go ahead with that payment. So, they didn’t uphold the complaint.

Mrs S, now represented by a different professional representative, disagreed. She said that scams of this nature (that is ‘job scams’) were commonplace around this time and Revolut ought to have provided a warning that was specific to that risk.

On 29 February 2024 I issued a provisional decision on this complaint. I wanted to give both parties a chance to submit any further evidence and arguments before any final decision. In summary that provisional decision said:

- When Mrs S made the Final 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 cryptocurrency related scam Mrs S was at risk from.
- If Revolut had done this, the scam would more likely than not have been stopped and the loss Mrs S incurred from the Final Payment would have been prevented.

- In the circumstances of this complaint, Mrs S should bear some responsibility (50%) for the loss she suffered from the Final Payment.
- So, Revolut should pay Mrs S £1,704.26 together with interest on £704.26 of that amount at 8% simple per year calculated from the date of the Final Payment to the date of settlement.

Mrs S accepted my provisional decision. Revolut didn't agree and provided further submissions. I've summarised its response below.

- In a multi-stage fraud, the Financial Ombudsman ought to only consider complaints about the financial institution that was the point of loss (in this case, a cryptocurrency exchange) or the origin of the funds (in this case, Mrs S' bank and that of her friend). It was irrational to consider the complaint only against it – an intermediate link in a chain of transactions.
- If the Financial Ombudsman decides that Revolut can be responsible for a customer's loss in such circumstances, it is unfair not to consider the role of the other financial institutions involved and, where appropriate, to apportion liability between them (even where no complaint has been, or even could be, considered by our service).
- In this case, no consideration has been given to the actions or inactions of any of the other financial institutions involved in the payments Mrs S made. Instead, Revolut is arbitrarily being held responsible for the loss owing to Mrs S' decision to complain against it rather than any of the other parties involved.
- Revolut shouldn't be responsible for Mrs S' loss simply because B sits outside of the Financial Ombudsman's jurisdiction. If, hypothetically, a complaint could be considered against B, then it assumes that it would no longer be considered responsible, in the same way that the financial institutions that funded Mrs S' account at Revolut have been deemed not to have any responsibility for her loss.
- While I may not be able to compel a consumer to refer a complaint about another financial institution, I do have the power under DISP 3.5.2 to inform a consumer that they could make such a complaint.
- Even if a consumer chooses not to make complaints about other financial institutions, this should not prevent the Financial Ombudsman from attributing a portion of responsibility to those institutions, even if we cannot impose liability on them.
- It cannot, under the relevant card scheme rules, delay a card payment. It can only decline or accept the payment. So it was irrational for the provisional decision to suggest it should have done this.
- High street banks don't agree they are responsible for multi-stage fraud. Those banks frequently direct scam victims to Revolut, rather than dealing with the claims themselves. The Financial Ombudsman ought to be instructing them not to do this.
- My provisional decision simultaneously accepts that, in law, Revolut doesn't have to consider the wisdom of its customer's payment instruction, but also states that it can't assume that a payment going to a customer's own account doesn't carry a risk of fraud. This appears to be a misapplication of the FCA's Consumer Duty and suggests that it puts a higher standard on Revolut than exists in law and imposes a higher burden on firms to scrutinise 'self-to-self' payments than it does for transfers to third parties. There is no obligation for it to look beyond the destination account and the suggestion that it should is unworkable and irrational.
- The Financial Ombudsman has not taken a consistent position on whether it should consider cryptocurrency payments to be at higher risk of fraud. Although my provisional decision suggests that banks were freely allowing customers to purchase cryptocurrency prior to 2022, we've also decided that it and other firms are responsible for cryptocurrency losses prior to the start of 2022.

- It is irrelevant that some high street banks have introduced restrictions on purchasing cryptocurrency. It offers its own cryptocurrency service and if it was to ‘throttle’ or introduce significant friction on payments to cryptocurrency providers then that might amount to anti-competitive behaviour by Revolut creating unreasonable barriers to using competitor’s products.
- What the provisional decision cites as good industry practice is, in fact, the result of the Financial Ombudsman’s own decisions. Banks and other firms have put warnings and other restrictions in place as a result of the Financial Ombudsman holding them liable for consumer losses to scams (and did so prior to the Supreme Court judgement in Philipp).
- What constitutes ‘good industry practice’ lacks sufficient clarity and certainty. It’s impossible to say what is good industry practice at any given time.
- Some of the good industry practice the provisional decision relies on has been withdrawn or isn’t relevant.
- My provisional decision goes far beyond the powers granted to our service under the Financial Services and Markets Act 2000 and the DISP Rules. Instead of deciding complaints based on what is fair and reasonable, taking into account the law and relevant regulations, the Financial Ombudsman is instead, in effect, unilaterally creating what amounts to legal and regulatory obligations.
- When significant changes to the regulatory landscape come into force, there is generally a lengthy consultation period and a significant time for firms to implement any changes. That doesn’t happen when our Investigators or Ombudsman decide that a certain, very specific action, is now ‘fair and reasonable’.

To provide additional clarification, I issued a second provisional decision on 21 May 2024. The overall conclusion remained the same, but I provisionally decided that Revolut should have declined the Final Payment in order to provide a warning to Mrs S.

Again, Mrs S accepted my provisional decision but Revolut didn’t. I have read Revolut’s representations carefully and will not repeat them all here. Briefly and by way of summary only it said:

About the law, its contract and the consumer duty

- I have misunderstood the scope and effect of the Consumer Duty.
- The Consumer Duty does not prohibit all undesirable outcomes for customers. It does not prohibit customers from making an unwise decision to transfer money. FCA guidance explicitly states that the Consumer Duty does not prevent an insistent customer from making decisions that or acting in way that a firm considers to be against their interests.
- I have wrongly assumed the Consumer Duty overrides Revolut’s primary duty to its client to promptly execute validly authorised payment instructions.
- *Philipp* gives firms the right to decline a payment instruction, rather than imposing an obligation to do so, and the Consumer Duty is not intended to override a firms’ legal obligations.
- I’ve failed to consider the implications of interpreting the Consumer Duty in this way. Such an interpretation would require it to delay or refuse a payment instruction in a vast range of circumstances. If it had to interrogate every transaction to determine

whether it may result in a bad outcome for the customer, this would result in it preventing all sorts of transactions.

About the process for making fraud checks it operated in August 2023

- I was wrong to say that it operated a process in August 2023 whereby if it identified a scam risk associated with a card payment through its automated systems, it might initially decline to make a payment, in order to ask some additional questions, was not correct. It was not able to implement that process until October 2023.
- In August 2023 it could only decline a card payment and (in theory) have tried to ask questions via its in-app chat function, but the consumer could have simply attempted to make the payment again.

About the role of Ombudsman decisions in informing good industry practice

- The Financial Ombudsman Service's approach to causation in multi-stage fraud cases has changed over time, but the relevant sources of industry guidance have not.
- In decisions issued in 2020/21 against banks, the Financial Ombudsman Service used to say that it was the onward transfer from the consumer's cryptocurrency account which caused the customer's loss, not the transfer to the customer's accounts as it now says.
- It assumes that this change of approach is down to the increase in the number of scams involving payments to cryptocurrency exchanges. An increase in the number of scams should not have any bearing on the liability of the financial institutions involved. This change has caused banks to restrict payments to cryptocurrency accounts.
- The Financial Ombudsman has 'reverse engineered' its approach to ensure that more consumers are reimbursed, rather than considering what is objectively fair and reasonable and, in doing so, it has influenced good industry practice.
- The principle of holding Revolut responsible for transactions made to the customer's own cryptocurrency account is irrational.

About the role of other financial institutions

- My reasoning is inconsistent. I have absolved the originating bank of any responsibility because it did not know the ultimate destination of the payments was a cryptocurrency account, but I have held Revolut responsible for not checking that Mrs S' funds would be moved from the cryptocurrency account to a third-party fraudster's account. Both situations relate to subsequent payments but are being treated differently.
- The role of other institutions should be taken into account when deciding what is fair and reasonable. I should not ignore the role played by other institutions in deciding Mrs S' complaint against Revolut simply because I cannot compel the consumer to complain against those institutions.

- I should attribute significant weight to the role of other firms when deciding what is fair and reasonable. The originating bank is often better placed to assess whether a payment carries risk of financial harm from fraud. If the originating financial institution had no reason to be concerned about the payment, then it's difficult to understand why Revolut ought to have been concerned either.
- The most logical approach would be to absolve it of responsibility on the basis that it was not involved in the transfer that caused the actual loss, or to apportion partial liability against Revolut taking into account the actions of all of the institutions involved and Mrs S.

About whether Mrs S should share responsibility for her losses

- My findings do not go far enough. I found that the scam was implausible, the consumer should have realised that she could not have obtained the returns with so little input and my provisional finding was (it says) that Mrs S probably realised that she was being scammed before making the final payment.
- A 50% deduction (which it says is widely applied by the Financial Ombudsman) is arbitrary and encourages customers to take additional risk – knowing that they will not bear full responsibility should they lose their money. It is not clear why deductions are not higher.
- It thinks that a 75% deduction would better reflect Mrs S' negligence in this case.

About the information available to Revolut

- I recognise that cryptocurrency scams have become increasingly varied, but at the same time the effect of my findings is to expect Revolut to have designed a comprehensive set of questions that would be triggered after a declined payment and probe whether a customer had fallen victim to an exhaustive list of every possible scam type.
- I have not referred to industry guidance or practice that suggests such a system is in place at any financial institution, particularly for debit card payments, and it is not clear whether such an approach was even feasible at the time.
- Neither I nor the customer has presented evidence about the prevalence of 'job scams' in August 2023, or that the consumer's payment pattern was suggestive of such a scam. It has simply been assumed that Revolut were aware of this type of scam at the time.
- The expectations go far beyond the systems and controls that it was required to have in place and it is unfair to decide what is fair and reasonable on the basis of a hypothetical system that I've decided would have prevented this type of scam.

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.

I will limit my considerations to those relevant to the determination of this complaint. It follows I will not comment on Revolut's broader concerns about how other firms might be treating complaints about multi-stage fraud, nor can I comment on other decisions issued by the Financial Ombudsman Service.

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 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 Mrs S and the Payment Services Regulations to carry out her 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 August 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.

This does not mean, as Revolut submits, that I have wrongly assumed that the Consumer Duty 'overrides' or 'trumps' the implied duty on banks to promptly execute validly authorised payment instructions. That misunderstands the Supreme Court's judgment in *Philipp* and the importance of the applicable terms and conditions.

Rather, my finding is that Revolut agreed – through an express term of the contract – to modify the implied duty, so that it must refuse or delay a payment instruction given by Mrs S under certain circumstances, including if regulatory requirements mean that it needs to carry out further checks.

The Consumer Duty is one such regulatory requirement which – 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 to 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 do not accept that I have misunderstood *Philipp*. In *Philipp* the Supreme Court considered whether Barclays' terms of business altered the starting implied position (that where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly). In *Philip*, Barclays' terms and conditions said that it did not have to follow the customer's instruction where "we reasonably think that a payment into or out of an account is connected to fraud...".

While *Philipp* said that having the right to decline a payment in the way set out in Barclays' contract was not the same as being under a duty to do so, I note Revolut's terms purport to expressly *require* it to decline a payment under certain circumstances (rather than just permitting it to do so). In other words, Revolut's standard terms and conditions placed it under a greater onus than did the Barclays terms and conditions 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 August 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.

In my second Provisional Decision, I referred to Revolut's own processes as an example of a bank or EMI taking these steps. I said:

For example, it is my understanding that in August 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.

Revolut says that it "was unfortunately not able to implement this process until October 2023 (i.e. this process was not operational at the relevant time)". It says in August 2023 if it determined a payment was unusual it could only decline the payment and could "in theory have tried to ask questions via the chat".

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/

I accept Revolut's representations about the limitations of the processes it had in place in August 2023 and the changes it made to its system in October 2023. But those representations do not alter my view that Revolut should, in August 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 saying that, I am mindful that in practice – as I have set out above – the card payment system rules meant that Revolut could not delay a card payment, it could only refuse (that is decline) the payment if it needed to make additional checks. Revolut's own representations confirm it could have taken that action in August 2023.

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 Code², 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 Duty³, 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*

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.

*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 cryptocurrency⁵ 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.
- And, as Revolut has explained – 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 August 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 including in relation to card payments in the way I have set out above); 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 August 2023, Revolut should in any event have taken these steps.

In response to my provisional decisions, Revolut made a number of representations (set out above) about my findings in relation to what I consider to have been good industry practice at the time. I have considered those representations carefully, but I am not persuaded by them.

I don't accept Revolut's argument that the good industry practice I've set out is actually only a result of the decisions that our service has made. I've set out above in some detail what I consider to be good industry practice in August 2023 and how my view about that (and about the steps Revolut should as a matter of what is fair and reasonable have been taking) is derived from a number of sources which are unrelated to decision making. And, while I accept that good industry practice evolves over time and that evolution might, naturally, create some uncertainty for firms like Revolut, that process is gradual and should not be fairly compared to the consultation periods that accompany significant changes in the law or regulatory framework, as Revolut has sought to do in its representations.

Nor do I accept Revolut's assertion that the Financial Ombudsman Service has 'reverse engineered' its approach to ensure that customers are reimbursed, rather than deciding what is fair and reasonable. I've explained, and will go on to explain, in some detail the basis on which I consider it to be fair and reasonable for Revolut to be held responsible for some of Mrs S' loss and about what is fair compensation in the circumstances of this complaint, taking into account the representations of both sides. As my analysis and reasoning shows I have not reached this conclusion on the basis that it would produce a more favourable outcome for Mrs S.

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

It isn't in dispute that Mrs S has fallen victim to a cruel scam here, nor that she authorised the payments she made by transfers to third parties and to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in detail in this decision the circumstances which led Mrs S 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 S might be the victim of a scam.

Firstly, I don't think that Revolut would have had any reason to intervene in the small payments made to third parties (those being payments 2,3 and 4) or connect them to the payments that went to cryptocurrency providers (payments 1,5,6 and 7). I'm therefore satisfied that payments 2,3 and 4 are irrelevant and I've therefore considered the position in relation to payments 1,5,6 and 7 (which were all made to cryptocurrency providers).

I'm aware that cryptocurrency exchanges like B 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 payments 1,5,6 and 7 would be credited to a cryptocurrency wallet held in Mrs S' name.

By August 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 transactions⁶. And by August 2023, when these payments took place, further restrictions were in place⁷. 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 S made in August 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 August 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 most of the payments in this case were going to an account held in Mrs S' own name should have led Revolut to believe there wasn't a risk of fraud.

⁶ See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.

NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

⁷ In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

So I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mrs S might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that payment 1 and payment 5 were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider), but they were very low in value, in keeping with previous payments to cryptocurrency providers Mrs S had made, and I don't think Revolut should reasonably have suspected that they might be part of a scam. As I've already set out, the same is true for payments 2,3 and 4 which weren't identifiably going to a cryptocurrency provider – they were low in value and there was no obvious link between them (or the payments that followed).

Payment 6 was clearly going to a cryptocurrency provider. It was significantly larger than any other payment that had debited Mrs S' account in the previous six months (by more than 20 times) and was also being paid to a second cryptocurrency exchange in as many days. That said, Mrs S didn't use her account that frequently and, I note, she had made around 20 cryptocurrency related transactions between mid-2022 and early 2023 (though none of those transactions exceeded £25 in value). So the purchase of cryptocurrency was not entirely out of character, though the value was much higher than previous transactions. On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, and also considering the value of this payment, I don't think Revolut ought to have been sufficiently concerned about this payment that it would be fair and reasonable to expect it to have provided warnings to Mrs S at this point.

However, the Final Payment was significantly larger in value again (almost twice as large as Payment 6) and it came a little over two hours after the previous payment. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mrs S was at 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 its customer 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 (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by August 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn Mrs S?

Revolut says it provided a number of warnings to Mrs S when she set up new beneficiaries prior to making the “transfers” (I understand that it is referring to payments 2,3 and 4) but it did not provide any warning prior to the Final Payment, which was not a funds transfer but a card payment.

It says it warned Mrs S prior to each funds transfer that she might be falling victim to a scam by providing the following message:

“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”

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

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to 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 August 2023, when these payments 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 August 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 Final 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, by August 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mrs S made the Final 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 cryptocurrency related scam Mrs S was at risk from.

In this case, Mrs S was falling victim to a 'job scam' – she believed she was making payments in order to receive an income.

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 Mrs S gave. I'd expect any such warning to have covered off key features of such a scam, such as making payments to gain employment, being paid for 'clicks', 'likes' or promoting products and having to pay increasingly large sums without being able to withdraw money. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Mrs 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 Final 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 'job 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.

While Revolut says no evidence has been presented on the prevalence of 'job scams' in August 2023, I note that it has not provided any data on the prevalence of job scams to support its position and I remain satisfied that this was a sufficiently common scam. For example I'm aware, from my own experience of considering complaints involving similar scams, that:

- In March 2023, several months before Mrs S' payments, another EMI offered "paying to earn money by working online" as a payment option as part of its system designed to (i) identify the purpose of payments and (ii) provide tailored warnings to the common scam types associated with those payment reasons. Where the consumer selected this option, the EMI then provided a warning about job scams (like the one Mrs S fell for) where the consumer is asked to pay money and then start earning by

watching ads or writing reviews before then being asked to pay greater amounts over time. It encouraged the consumer to 'stop' as 'this is a scam'. Those warnings involved APP not card payments, but they support my view that job scams of this nature were sufficiently common and well known to feature in scam prevention systems in August 2023.

- Versions of job scams have been around for some years (and in many countries). For example, one such example – about which the Financial Ombudsman Service received complaints at the time – featured in an article in the Sun in March 2022 <https://www.thesun.co.uk/money/18068901/five-ways-crooks-cost-living/> and a very similar scam was described in a Which? article in June 2023 - <https://www.which.co.uk/news/article/job-scams-fraudsters-are-posing-as-employers-and-recruiters-on-indeed-and-linkedin-a7NNv8L84n97>. And data from Ofcom published in March 2023 found that of 43 million adults who have encountered scams or fraud online, 30% have come across content related to fake employment scams.
- The Financial Ombudsman Service has issued numerous final decisions relating to this type of scam, including some against Revolut, many of which relate to events which pre-date August 2023.
- Regarding the overall feasibility of providing a warning using the automated systems example I have referred to (and being mindful that other options are available to establish the purpose of a payment – including human intervention), I note:
 - Revolut itself was able to introduce a similar process in October 2023 – just two months after the payments were made.
 - Its own representations are that in August 2023 it could have declined the payment to provide warnings through its chat function (whether or not in practice it did); and
 - 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 final £3,408.51 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 Mrs S attempted the payment again, should Revolut have made the payment.

And as I've set out above it did have systems in place by August 2023 to decline card payments and provide warnings of a similar nature to the type I've described. So, it could give such a warning and, as a matter of fact, was providing such warnings at the relevant time.

If Revolut had provided a warning of the type described, would that have prevented the losses Mrs S suffered from the Final Payment?

I think that a warning of the type I've described would have identified that Mrs S' circumstances matched an increasingly common type of scam.

I've read the instant message conversation between Mrs S and the fraudsters. That conversation suggests that prior to the Final Payment, she already had some concerns about the scheme – she appears to have been concerned about repeatedly being assigned combination tasks. She also realised that she'd been the victim of a scam very soon after making the Final Payment which, I think, indicates that it wouldn't have taken much persuasion (that a warning could have provided) to convince her that she was falling victim to a scam prior to making that payment.

Revolut questions what steps have been taken to establish whether any other financial business involved in the payments Mrs S made might have provided warnings that she should have taken notice of.

It explained that the money Mrs S borrowed from her friend came initially from the friend's Revolut account but was ultimately funded by payments from the friend's bank account (held at a high street bank). It's difficult to see how the actions of that bank could be relevant here. There's no suggestion that Mrs S' friend was falling victim to a scam or that Mrs S would have seen any warnings that bank provided. So even if that bank did provide a relevant warning to Mrs S' friend, it's very unlikely that could have any impact on my finding as to whether Mrs S is likely to have decided not to go ahead with the Final Payment had Revolut provided a warning of the nature I've described.

While Mrs S did top-up her account at Revolut using a card issued by a high street bank, the value of those payments (the largest being £1,490), the previous transactional history (which pre-dates the scam) and the nature of those payments (being Apple Pay top-ups) make it, in my view, very unlikely that any warnings were provided by Mrs S' bank that would have alerted her to the possibility she was being scammed.

Overall, I think that a warning provided by Revolut would have given the perspective Mrs S needed, reinforcing her own developing concerns and she would more likely than not have concluded that the scheme was not genuine. In those circumstances I think, she's likely to have decided not to go ahead with the Final Payment, had such a warning been given.

Is it fair and reasonable for Revolut to be held responsible for Mrs S' loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs S 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 Final Payment was made to another financial business (a cryptocurrency exchange based in another country) and that the payments that funded the scam were made from other accounts at regulated financial businesses (though some of those accounts were not held in Mrs S' name).

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs S might have been at risk of financial harm from fraud when she made the Final 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 Mrs S 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 B does not alter that fact and I think Revolut can fairly be held responsible for Mrs S' loss in such circumstances. While I have carefully noted Revolut's comments on this point in response to my second provisional decision, I am not persuaded to reach a different view – 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.

In the alternative, Revolut argues that if I conclude it can be held responsible for a customer's loss in circumstances where it is 'only' an intermediate link in a chain of transactions, then it is irrational to only consider its role in what happened. Instead consideration must be given to the other parties involved in the multi-stage fraud to determine overall responsibility for the loss suffered by Mrs S.

I have considered those representations, including those made in response to my second provisional decision carefully, but again I am not persuaded to reach a different conclusion about what is fair and reasonable in the circumstances of this complaint.

Mrs S 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 S could instead, or in addition, have sort to complain against those firms. But Mrs S has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

As I have explained, I am satisfied that Revolut ought, taking reasonable steps, to have prevented the Final Payment. If it had done so, I am satisfied it is more likely than not that it would have prevented the loss Mrs S suffered as a consequence of that payment. So I am satisfied that the starting point is that it's fair to require it to compensate Mrs S for the losses it could have prevented by taking reasonable steps.

Whilst it is open to me to inform a complainant it might be appropriate to complain against another respondent, I do not consider it necessary or appropriate for me to do that in this case – I haven't seen evidence that persuades me that I should exercise my discretion to do this; Mrs S is aware that she could also have attempted to complain against her own bank and Revolut could itself have informed Mrs S that another firm might also be responsible (and why) when she first complained (see DISP 1.7.1R).

Revolut accepts that Mrs S has only brought a complaint against it and that while she could complain against her own bank, she could not complain about her friend's bank or B, which is an unregulated cryptocurrency exchange. It says I should:

1. decide whether the other parties involved could also be held responsible for Mrs S' loss (even if I cannot impose liability on them), and
2. if I find that they should share responsibility, I should reduce any award to Mrs S accordingly.

Essentially Revolut says it would be fair for it to pay less than the full amount because others, as well as it, might also have been at fault and could potentially also have prevented Mrs S loss.

I've considered Revolut's arguments carefully, but I am not persuaded it would be fair to reduce Mrs S' compensation for those reasons in circumstances where Revolut could have prevented all of Mrs S' losses connected with the Final Payment and Mrs S has only

complained about Revolut, as she is entitled to do. 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.

I note that in *R (on the application of Portal Financial Services LLP) v Financial Ombudsman Service Ltd* [2022] EWHC 710 (Admin) the High Court was satisfied that it was rational for the Ombudsman to hold an advisor responsible for 100% of the complainant's losses, notwithstanding that 'this would not be the outcome at common law, and that the Ombudsmen were required to consider the law and give reasons for departing from it and have not done so.' The court was satisfied that it was rational for the Ombudsman to conclude that, but for the business's own actions, the loss could have been prevented and that it was open to the Ombudsman to conclude that the business should be held responsible for 100% of those losses. The High Court reached a similar conclusion in *R (IFG Financial Services Ltd) v Financial Ombudsman Service* [2005] EWHC 1153 (Admin) at paragraphs 13 and 93.

For the reasons set out above, I'm satisfied that similar considerations apply in the present case.

Where a consumer has complained about more than one respondent in connected circumstances, DISP 3.6.3G says the Ombudsman may determine that the respondents must contribute towards the overall award in the proportion that the Ombudsman considers appropriate. But that does not apply to Mrs S' situation.

The Financial Ombudsman Service was set up to determine complaints quickly and with minimum formality. Taking this statutory purpose into account, I think it would not be proportionate or appropriate for me to conduct a separate exploratory investigation into the actions of other potential respondents for the purpose of apportioning compensation between potential respondents, where: the consumer has only complained about one respondent from which they are entitled to recover their 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, that could have prevented the loss, responsible for failing to do so.

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 S' loss from the Final Payment (subject to a deduction for Mrs S' own contribution which I will consider below). As I have 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 and as a step to comply with its regulatory requirements, I consider Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

Revolut has argued that we are applying the provisions of the CRM Code to complaints against it, despite it not being a signatory and in circumstances where the CRM Code would not, in any case, apply. I do not seek to treat Revolut as if it were a signatory to the CRM Code, and I have not sought to apply it by analogy. I've explained in some detail why I think it fair and reasonable that Revolut ought to have identified that Mrs S may have been at risk of financial harm from fraud and the steps it should have taken before allowing the final payment to leave Mrs S' account. And the Financial Ombudsman Service's jurisdiction is neither the same as nor tied to the CRM Code.

I also acknowledge the PSR's proposed mandatory reimbursement scheme for authorised push payments made over the Faster Payments system would not require Revolut to reimburse Mrs S in relation to the Final Payment. However, the PSR's proposals are not yet

in force and are not relevant to my decision about what is fair and reasonable in this complaint and, in any event, will not apply to card payments like the Final Payment. I do not consider the fact that the PSR's proposals are narrower than the circumstances in this complaint means that Revolut should not compensate Mrs S in circumstances when it failed to act fairly and reasonably, as I have found was the case here.

Indeed, the PSR has recently reminded firms that fraud victims have a right to make complaints and refer them to the Financial Ombudsman Service that exists separately from the intended reimbursement rights and that APP scam victims will still be able to bring complaints where they believe that the conduct of a firm has caused their loss (in addition to any claim under the reimbursement rules)⁸. So it is not correct to suggest, as Revolut appears to do, that the proposed mandatory reimbursement scheme somehow 'occupies the field' so far as fraud and scam reimbursement is concerned.

Similarly, I consider that it is not relevant that the circumstances here do not fall under the specific definition of an APP scam set out in the CRM Code and DISP rules. Those definitions define the scope of the CRM Code and eligibility of payers to complain about a payee's payment service provider respectively. They do not preclude me from considering whether Revolut failed to act fairly and reasonably when it made the Final Payment without providing a warning to Mrs S. Revolut does not suggest that I don't have jurisdiction to consider the complaint at all, and in doing so I am required by Parliament and the DISP rules to consider 'all the circumstances of the case'. I am satisfied that if I took the more limited approach Revolut suggests I would not be discharging that duty.

Overall, considering what is fair and reasonable in all the circumstances, I'm satisfied Revolut should have made further enquiries and provided a tailored scam warning before processing the Final Payment. If it had, it is more likely than not that the scam would have been exposed and Mrs S would not have lost any more money. In those circumstances I am satisfied it is fair to hold Revolut responsible for some of Mrs S' loss.

Should Mrs S bear any responsibility for her losses?

I've thought about whether Mrs S should bear any responsibility for her loss connected to the Final Payment. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint including taking into account Mrs S' own actions and responsibility for the losses she has suffered.

I recognise that there were relatively sophisticated aspects to this scam, not least an apparently credible and professional looking platform, which was used to access and manage the user's apparent earnings and tasks. I note that Mrs S also seems to have been part of an instant messaging group with other people who claimed to be making money. I can imagine this would have given some validation to the scheme.

But, at its heart, the scam appears to have had some features that made its plausibility questionable (though not completely so) by the time of the last payment. While I haven't seen and heard everything that Mrs S saw, the fraudster's explanation for how the scheme worked is difficult to understand in parts, and I think that on some level Mrs S ought

⁸ "The reimbursement rules and their award limit differ from the rules which govern complaints under the Financial Ombudsman Service's dispute resolution rules (DISP). PSPs should therefore inform victims of APP scams that, in addition to their right to seek reimbursement under the reimbursement rules, they have the right to bring complaints against sending and receiving PSPs if they are dissatisfied with their conduct and consider this has caused their loss. Such complaints may ultimately be referred to the Financial Ombudsman Service." PSR PS23/4 7.18

reasonably to have questioned whether the activity she was tasked with carrying out (which does not appear to be unduly time-consuming or arduous) was capable of generating the returns promised at the point at which she was required to make a further substantial payment.

As mentioned, I also think Mrs S probably recognised (and ought reasonably to have recognised) that, prior to the Final Payment, the platform could effectively prevent her from withdrawing her funds by continuing to grant her 'combination tasks' without a clear explanation of why it was assigning these tasks to her, and when and how she might be able to withdraw her funds. This fact should have been even more concerning when, as happened on 18 August 2023, the funds required to bring her account at F to a positive balance increased significantly (and unsustainably).

I recognise that the scam operates on a cruel mechanism – always making the victim believe that one final payment will allow them to get back what they've put in. But, I think Mrs S should have become increasingly aware (and to some extent appears to have recognised) this dynamic before making the Final Payment. But I also understand that in scams such as this it can be difficult for a victim to have the sort of clear view that hindsight provides when they have gone through the earlier stages of a scam that, at first instance, has credible elements. I've also borne in mind the fact that the payments in this complaint were made over a short period of five days. I can therefore understand to some extent why it did not dawn on Mrs S immediately that she was falling victim to a scam.

So, given the above, I think she ought reasonably to have realised that there was a possibility that the scheme wasn't genuine (before going ahead with the Final Payment). She did after the Final Payment, when assigned a further 'combination task', seemingly without making any additional enquiries. In those circumstances, I think it fair that she should bear some responsibility for her losses.

For the avoidance of doubt, it is not my finding that Mrs S knew that she was likely falling victim to a scam and went ahead anyway. Rather my finding is that she seems – to some extent – to have recognised that the platform could prevent her from withdrawing funds by continuously granting her combination tasks. I consider she could have realised from this and the other information available to her, that there was a possibility that the employment scheme wasn't genuine or that she might not recover her money. In those circumstances it would not be fair to require Revolut to compensate her for the full amount of her losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mrs S in relation to the Final Payment because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

I do not think that, as Revolut submits, the deduction made to the amount reimbursed to Mrs S should be greater than 50% taking into account all the circumstances of this case. I recognise that Mrs S did have a role to play in what happened, and it could be argued that she should have had greater awareness than she did that there may be something suspicious about the job scam. But I have to balance that against the role that Revolut, an EMI subject to a range of regulatory and other standards, played in failing to intervene. Mrs S was taken in by a cruel scam – she was tricked into a course of action by a fraudster and her actions must be seen in that light. I do not think it would be fair to suggest that she is mostly to blame for what happened, taking into account Revolut's failure to recognise the risk that she was at financial harm from fraud, and given the extent to which I am satisfied that a business in Revolut's position should have been familiar with a fraud of this type. Overall, I remain satisfied that 50% is a fair deduction to the amount reimbursed in all the circumstances of the complaint.

I also reject any suggestion that Mrs S may have acted with less care because of a belief that she might be ultimately partially reimbursed for her loss, and I've seen no evidence to support such a finding. It's evident that Mrs S has been through a very distressing experience which, even following this final decision, will result in her suffering significant financial loss.

Could Revolut have done anything to recover Mrs S' money?

Some of the payments were made by card to a cryptocurrency provider. Mrs S sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that B and M provided cryptocurrency to Mrs S, which she subsequently sent to the fraudsters.

The payments which didn't go to the cryptocurrency provider directly appear to have been made to individuals selling cryptocurrency who were very likely unconnected to the fraudsters. As those individuals were unlikely to be involved in the fraud, even if it were practical or possible to recover funds from them, it would be unlikely to be fair for that to happen (given that they'd legitimately sold cryptocurrency). So, I don't think it would be fair and reasonable to conclude that Revolut should have done anything more to try and recover Mrs S' money.

Interest

Mrs S has explained that the Final Payment was part funded by a loan from a friend. I can see a credit of £2,000 from that person prior to the final payment being made. Mrs S says she has not repaid her friend and they have not charged any interest. As Mrs S has not been charged any interest on that amount, it would not be fair to award interest on it. As I've decided that Mrs S should receive 50% of the Final Payment, it follows that she shouldn't receive interest on £1,000 of that amount (that is 50% of £2,000) and it should only be paid on the remaining £704.26. I consider that 8% simple interest per year fairly reflects the fact that Mrs S has been deprived of this money and that she might have used it in a variety of ways.

My final decision

For the reasons given above, I uphold in part this complaint and require Revolut Ltd to pay Mrs S:

- 50% of the Final Payment - £1,704.26
- 8% simple interest per annum on £704.26 from 18 August 2023 to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 28 August 2024.

Rich Drury
Ombudsman