

The complaint

Mr M complains that Revolut Ltd won't refund money he lost when he was the victim of a crypto investment scam.

Mr M is represented by a firm I'll refer to as 'C'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In April 2023, Mr M saw an advert for online investing on a social media platform with a firm I'll refer to as 'F', which we now know to be a scam. Mr M considered the advert extremely professional and registered his interest via the link provided. Mr M was advised he would be contacted by a Financial Advisor in due course, who would discuss the investment options available to him and the next steps to help him start trading.

Shortly after Mr M was contacted by someone from F who introduced themselves as a Financial Advisor and explained how they would initially help Mr M trade on a one-on-one basis. Mr M was asked to sign an e-mail which was sent by way of an introduction to the platform, which would then result in F showing Mr M how to deposit funds and how to trade using the platform. F convinced Mr M he could invest as little as £100 into his trading account, and he would show him how to make a 'quick profit'.

Mr M was impressed with how professional F was and how well the Financial Advisor understood the financial market, which further convinced Mr M that the opportunity was genuine.

Mr M was convinced to open an account with Revolut and an account on a crypto platform to help him start trading.

As a result, Mr M made the following payments from his Revolut account to a legitimate crypto exchange, which he then sent onto F's trading platform. To fund the scam payments, he transferred money from his existing banking provider(s) – which I'll refer to as 'N'.

Transaction date	Type of transaction	Amount
7 April 2023	Debit card payment	£500
	(Payment 1)	
13 April 2023	Debit card payment	£4,450
	(Payment 2)	
19 April 2023	Debit card payment	£5,000

	(Payment 3)	
19 April 2023	Debit card payment	£850
	(Payment 4)	
	Total loss:	£10,800

Mr M saw a rise in profits from his investment on F's trading platform, so he requested to make a withdrawal. However, F told him it was too late in the day, and he would be contacted the following day to arrange the withdrawal.

Mr M was contacted by F the following day and was told the funds were being held and he'd need to pay an additional £6,000 to release the funds. At this point, Mr M realised he'd been a victim of a scam.

On 25 May 2023, Mr M lodged a formal complaint to Revolut via C, but Revolut didn't uphold it. It said when the complaint was made, they raised dispute chargebacks against the transactions mentioned. However, ultimately the chargebacks were unsuccessful as the payments in question were money orders, which they initiated correctly according to the details provided by Mr M.

As a result, the complaint was referred to the Financial Ombudsman Service.

Our Investigator thought it should be upheld in part. He didn't think the first payment (7 April 2023 for £500) would appear particularly concerning or suspicious to Revolut considering its low value. But he thought Revolut should've been concerned by the second payment (13 April 2023 for £4,450) as the payment was identifiably going to a crypto provider, which carries a known fraud risk, and was of a higher value. The Investigator went on to say Revolut ought to have provided a tailored written scam warning – setting out the key features of crypto scams - to Mr M before processing it.

The Investigator said if Revolut had intervened from the second payment in light of information known to payment service providers about the increasing number of scams associated with cryptocurrency exchanges, and asked Mr M to conduct further checks on F, it's likely further loss could've been prevented. Our Investigator also thought Mr M should take some responsibility for his loss too. This was because, he wasn't satisfied Mr M carried out sufficient checks on the investment opportunity or F's trading platform. The Investigator went on to say if Mr M had checked F's platform on-line before making the payment, he would've realised this was not a genuine company. Our Investigator also noted that the guaranteed returns and unrealistic profits should've led Mr M to question the legitimacy of the firm. Because of this, he thought it would be fair for Revolut to refund 50% of Mr M's loss from the second payment onwards, plus 8% simple interest.

C confirmed Mr M's acceptance.

Revolut didn't agree with our Investigator. In short, they added:

- The sole purpose of the customer's account was evidently to add money to it and then transfer it to the other cryptocurrency platforms. There was no other transactional activity in the account prior to these transactions, as it was a newly created account, or afterwards.
- There was no information available to us that we could have used to determine what can be deemed as unusual activity or not.
- The customer made the payments on different days and not all in one go or in a guick succession.
- The second payment was made to an already established payee considering that the customer made a payment to the same beneficiary a week before.
- There was no change in account's usage, no sudden increase in spending or anything else happening in the account that we should have considered as suspicious. The transactional activity in the account is therefore normal and consistent.
- This is a 'self-to-self' scenario in which Mr M owned and controlled the beneficiary account to which the payments were sent. Hence, the fraudulent activity didn't occur on Mr M's Revolut account as the payments were made to a legitimate crypto exchange before being sent to the scam platform.
- The transactions weren't out of character or unexpected with the typical way an
 electronic money institution (EMI) account is used particularly as high street banks
 have started restricting their customers from sending money to crypto exchanges
 (which is an entirely legitimate activity). Typically, this type of account is opened and
 used to facilitate payments of a specific purpose and often not used as a main
 account.
- 'Self-to-self' payments don't meet the Dispute Resolution Rules ("DISP Rules"), nor the Contingent Reimbursement Model (CRM) code or incoming mandatory reimbursement rules definition of an Authorised Push Payment (APP) scam.
- It is entirely relevant to consider possible other bank interventions as the funds originated from Mr M's own external bank account. As such, Revolut believe it should be considered by the Financial Ombudsman in tandem with this complaint. At the very least, whether Mr M was warned by their external bank is relevant to whether he acted negligently in disregarding any such warnings.
- It might be appropriate for the Financial Ombudsman to exercise its powers under DISP to inform Mr M that it could be appropriate to make a complaint against another firm if necessary.
- 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] UKSC25.
- It's irrational to hold Revolut responsible for any of the loss where it is only an intermediate link in a chain of transactions.

Our Investigator acknowledged Revolut's points, but his view remained the same. In short, he explained, even though he accepts other firms might have also missed an opportunity to intervene or failed to act fairly and reasonable in some other way, as this complaint is against Revolut, we can only make an award against Revolut.

Revolut remained in disagreement with our Investigator and so, the matter has been passed to me for a final decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Firstly, I want to clarify that I've taken into account the detailed submissions from both parties in reaching my decision. However, if there's something I've not mentioned, it isn't because I've ignored it. I haven't. Rather, I've focused on setting out what is key to my decision.

In broad terms, the starting position at law is that an EMI such as Revolut is expected to process payments and withdrawals that a customer authorises them 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 Mr M modified the starting position described in Philipp, by – among other things – expressly requiring Revolut to refuse or delay a payment "if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks" (section 20).

So Revolut was required by the terms of their contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of their customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where they suspected their customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R)

taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in April 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

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

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

For example, it is my understanding that in April 2023, Revolut, whereby if they identified a scam risk associated with a card payment through their automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through their in-app chat).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3).
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the "Financial crime: a guide for firms".
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to 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, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions particularly unusual or out of character transactions that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving crypto when considering the scams that their 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 crypto 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 crypto 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 they 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 having been good industry practice at the time, I consider it fair and reasonable in April 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 their customers were at risk of fraud (among other things). This is
 particularly so given the increase in sophisticated fraud and scams in recent years,
 which firms are generally more familiar with than the average customer.
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment (as in practice Revolut sometimes does); and
- have been mindful of among other things common scam scenarios, how the
 fraudulent practices are evolving (including for example the common use of multistage fraud by scammers, including the use of payments to crypto accounts as a step
 to defraud consumers) and the different risks these can present to consumers, when
 deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in April 2023, Revolut should in any event have taken these steps.

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

By April 2023, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency (that is scams involving funds passing through more than one account controlled by the customer before being passed to a fraudster) 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 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 transactions¹. And by April 2023, when these payments took place, further restrictions were in place². 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 the vast 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.

So, taking into account all of the above, I am satisfied that, by the end of 2022, prior to the payments Mr M made in April 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. In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payments in this case were going to an account held in Mr M's own name should have led Revolut to believe there wasn't a risk of fraud.

I accept that the account was newly opened therefore Revolut did not have information on Mr M's account activity that it could use to identify whether the payments were unusual for him. Nevertheless, Revolut did have information about the payments themselves which it ought to have taken into consideration.

I think Revolut should have recognised that the payments were to a cryptocurrency provider

¹ 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.

² In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

and were all of a significant value such that it ought to have been concerned that Mr M might be at a greater risk of fraud and for it to have intervened.

While Revolut should've identified the payments were going to a crypto provider (the merchant is a well-known crypto provider), the first payment (£500 payment on 7 April 2023) was relatively low in value. And so, I don't think there would've been enough reason for Revolut to suspect Mr M was at risk of financial harm from fraud.

The second payment (£4,450 payment on 13 April 2023), which again would've been identifiable as going to a crypto provider, was significantly greater in value than the first payment. I understand Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions. But given what Revolut knew about the destination of the payment, I think the circumstances should have led Revolut to consider that Mr M was at a heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Mr M before this payment went ahead.

What did Revolut do to warn Mr M?

I haven't seen anything to show Revolut provided a warning to Mr M before processing any of the payments.

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 duty to make payments promptly, as well as what I consider having been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, when Mr M attempted to make the second payment, knowing that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr M by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a cryptocurrency investment scam warning, would that have prevented the losses Mr M incurred after and including the second payment?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case.

And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present, such as finding the investment through an advertisement, being assisted by a broker, seeing the initial deposit quickly increase in value as well as being told to expect 'quick profits'.

Based on the evidence Mr M has provided showing his correspondence with F, I've seen nothing to suggest that Mr M was asked, or agreed to, disregard any warnings provided by Revolut. I am, however, aware that N contacted Mr M regarding a transfer of funds of £5,850 on 19 April 2023. However, as Mr M was making the payment from his own account held at N to his own account held with Revolut, N's interaction with – and the warnings they provided – were focused on the common features of safe accounts scams (which wasn't relevant to Mr M's circumstances). Because of this, I haven't seen anything to show Mr M ignored any warnings relevant to his situation – that being a crypto investment scam. Nor have I seen anything to suggest – from the scam chat conversations I've seen - that Mr M was so taken in by the fraudsters that he would have disregarded a clear and specific warning.

Overall, on the balance of probabilities, had Revolut provided Mr M with an impactful warning that gave details about cryptocurrency investment scams and how he could've protected himself from the risk of fraud, I believe it would have resonated with him. He could have paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams.

Revolut could've also directed Mr M to check the FCA website about F (given the red flags). And I have no reason to believe he wouldn't have followed such advice and, in turn, he would've become aware that he was dealing with a cloned firm and being scammed.

Overall, I'm satisfied that a timely warning to Mr M from Revolut from payment two onwards would have very likely caused him to have sufficient doubt to not go ahead with any further payments – thereby revealing the scam and preventing any further loss.

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

In reaching my decision, I have taken into account that the payments were made to another financial business (a crypto exchange) and that it was funded from another account at a regulated financial business held in Mr M's name and control.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr M might have been at risk of financial harm from fraud when he made the second payment of £4,450 on 13 April 2023, and in those circumstances, they should have declined the payment and made further enquiries. If they had taken those steps, I am satisfied they would have prevented any further loss Mr M 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 Mr M's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr M's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr M 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 Mr M could instead, or in addition, have sought to complain against those firms. But Mr M has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce a consumer's compensation in circumstances 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 responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr M's loss from the £4,450 payment made on 13 April 2023 onwards (subject to a deduction for Mr M's own contribution which I will consider below). As I have explained, the potential for multi-stage scams, particularly those involving crypto, 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.

Should Mr M bear any responsibility for his losses?

I've thought about whether Mr M should bear any responsibility for his loss. 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 Mr M's own actions and responsibility for the losses he has suffered.

When considering whether a consumer has contributed to their own loss, I must consider whether the consumer's actions showed a lack of care that goes beyond what we would expect from a reasonable person. I must also be satisfied that the lack of care directly contributed to the individual's losses.

Here, I consider that there were sophisticated aspects to this scam – not least the apparently credible and professional looking platform which showed Mr M his investment growth/profit.

However, If Mr M had carried out some basic online research into F before proceeding, he would've found the FCA warning and the negative online reviews, which would've raised concerns with Mr M about the investment opportunity he was being presented, which could've helped prevent the loss Mr M suffered.

I also feel Mr M should've questioned the investment given it could be said that it sounded too good to be true and the advertisement was telling him that F could "help him earn a lot of money, so much that he will not have to work again". Another red flag should have been when the Advisor from F told Mr M "he intended to stay with him for a month and he will help him make a million and if not, he will leave him alone". I feel this should've raised further questions that the opportunity might not be genuine.

I appreciate Mr M fell victim to a sophisticated scam, nevertheless I don't think he acted reasonably for the reasons I've given. If Mr M had taken greater caution before proceeding in light of the above, then I consider he would've most likely uncovered that he was being scammed – thereby preventing his losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mr M from the second payment onwards because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%. I think Revolut should also pay 8% simple interest to recognise the loss of use of money Mr M has suffered.

My final decision

My final decision is that I uphold this complaint in part. I direct Revolut Ltd to pay Mr M:

- 50% of the payments made from the second payment onwards, which amounts to £5,150.
- Pay 8% interest from date of loss to date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 1 April 2025.

Israr Ahmed Ombudsman