DRN-4937830

Complaint

Mr S is unhappy that State Bank of India (UK) Limited ("SBI UK") didn't refund transactions from his account that he says he didn't make or otherwise authorise.

Background

In April 2023, transfers were made from the account Mr S holds with SBI UK. The security credentials for his online banking facility were reset on 13 April 2023 and, shortly afterwards, the following payments were made:

1	15 April 2023	£15,000
2	15 April 2023	£10,000
3	16 April 2023	£2,000
4	16 April 2023	£1,000
5	16 April 2023	£4,000
6	16 April 2023	£2,000
7	16 April 2023	£1,200
8	16 April 2023	£100
9	16 April 2023	£2,000
10	16 April 2023	£2,000
11	16 April 2023	£3,000
12	16 April 2023	£1
13	16 April 2023	£4,000
14	16 April 2023	£803
15	16 April 2023	£2,000

These were made to several different payees. According to SBI UK's records, the IP address used to log-on each time was geolocated in India. Mr S was in the UK at the time. He says he didn't make those transfers. He doesn't know how somebody else was able to make them. He has speculated about potential ways in which the security of his online banking could've been compromised.

Around the 16 April 2023, Mr S was assisted by a family member in scanning his mobile device and his computer with antivirus software. He provided a screenshot of the scan of his mobile device which showed one *"malicious app"* had been found. Mr S had only scanned his device using the free version of this third-party antivirus software. The paid-for version includes an audit function which allows the user to see a chronological history of the threats removed from the device.

Once Mr S realised that these payments had left his account, he emailed SBI UK to ask them how it could've allowed unauthorised transactions to go through. On 18 April, a follow-up email was sent to the bank from his address. This said *"I enquired with my wife she done the transactions its all sorted now. [sic]"* Mr S tells me he didn't send this message and, as I understand it, he lives alone. This prompted him to carry out further enquiries. He discovered that the recovery email associated with his account was an email address that had no connection to him at all.

It also came to light during the investigation that, before these events took place, Mr S had an interaction with a different bank which I'll refer to as N. Mr S holds an account with N and it blocked a couple of attempted transactions from leaving his account. In an email sent to him on 27 March 2023, that bank said *"We strongly suspect that you are being targeted by a fraudster …"*

He made a complaint to SBI UK and asked that it refund the disputed payments. SBI UK didn't agree to do so. It said there were multiple communications sent to Mr S via text message and email in relation to the resetting of his security credentials and individual transactions. Since Mr S didn't take any action in relation to these, it doesn't think it did anything wrong. Mr S says that he didn't receive any of these messages, except for one or two that came after the fraudulent activity had come to light.

SBI UK also responded to his claim that he'd been hacked by saying that the bank *"is not responsible for your internet banking log in details being compromised..."* It referred to a section in the terms and conditions of his account which sets out a customer's obligation to keep the security credentials for their account safe and to report any compromise to the bank as soon as possible. SBI UK didn't uphold the complaint, but it did offer Mr S £150 as a gesture of goodwill.

Mr S wasn't happy with the response he received from SBI UK and so he referred his complaint to this service. It was looked at by an Investigator who didn't uphold it. The Investigator thought that, on balance, it was likely that the transactions were authorised. Mr S disagreed with the Investigator's opinion and so the complaint has been passed to me to consider.

Provisional decision

I issued a provisional decision on 13 June 2024. I wrote:

> *Regulation 76 of the Payment Services Regulations 2017 (PSRs) says that:*
>
> > *"where an executed payment transaction was not authorised in accordance with regulation 67 the payment service provider must … (a) refund the amount of the unauthorised payment transaction to the payer; and (b) where applicable, restore the debited payment account to the state it would have been in had the unauthorised payment transaction not taken place."*
>
> *There are exceptions to this. I'll discuss these later in this decision. However, the starting point is that, if Mr S made these disputed transactions himself or authorised for them to be made on his behalf, it wouldn't be fair and reasonable to ask the bank to refund them. He insists that he had no involvement. The question I need to determine, therefore, is whether SBI UK has provided adequate evidence to justify its decision to hold him liable for the payments.*
>
> *It can only refuse to refund disputed payments if it can show Mr S authorised them, but it can't say that the use of correct security credentials conclusively proves that the payments were so authorised. The regulator, the Financial Conduct Authority (FCA) published guidance on the application of the PSRs and that document says:*
>
> > *"To avoid doubt, it is not sufficient for the PSP [payment service provider] to assert that the customer "must have" divulged the personalised security features of the payment instrument, and to effectively require the customer to*

prove that he did not. The burden of proof lies with the PSP and if a claim that a transaction is unauthorised is rejected, the rejection must be supported by sufficient evidence to prove that the customer is guilty of fraud, gross negligence or intentional breach and the reason for the rejection must be explained to the customer." [1]

I've given the evidence careful consideration and I'm satisfied that it suggests Mr S did not authorise these payments. I say that because:

- *The IP address records show they were carried out by someone in India, and Mr S wasn't in India at the time.*
- *It seems improbable that Mr S would be carrying out such a high volume of online banking activity in the middle of the night.*
- *The suspicious email that was sent from his email address to the bank after the scam had taken place is also consistent with the claim that a third-party managed to take control of his account.*
- *Finally, the testimony he has provided to this service is that he didn't make the payments. He's been consistent in his version of events and his explanation is in keeping with someone struggling to make sense of how it was possible for their money to be stolen.*

I can't know for sure how a third-party was able to access his online banking. Despite my efforts, I've not been able to identify precisely where the breach occurred. Nonetheless, he has provided evidence that shows that his mobile phone was home to a malicious app around the time that these transactions took place. I've also seen evidence showing that he was attempting to register for the SBI app around this time and received text messages that related to that process. SBI UK has told me that these messages were sent from a telephone number in India because Mr S was inadvertently attempting to register with the bank's app that is provided for customers in India, rather than the UK. It's plausible that malware installed on his device had a keylogging functionality that was used to steal passwords or other security credentials. These could then be used as tools to gain access and control of the victim's online banking. I accept that this would mean that the software used by these fraudsters was sophisticated. Nonetheless, we do know that such capabilities exist and it's a more plausible explanation as to how Mr S sustained these losses than any other that has been offered.

As far as I can see, the crux of SBI UK's argument is that it sent Mr S multiple notifications and one-time passcodes by email and text message. It's not clear if it's arguing that his failure to respond to those messages was careless or that it indicates that he did authorise these payments. In any event, if malware had enabled a fraudster to take control of his device, it's not inconceivable that they'd have the ability to redirect messages or delete them before Mr S noticed them.
SBI UK has also argued that it would be atypical for a fraudster to gain access to a victim's account and not empty it at once. I'm not convinced. I can only speculate about why the fraudsters acted as they did. However, it's possible that the money was transferred this way because moving the entire balance in one go would trigger fraud prevention systems at SBI UK. It's also apparent that the fraudsters were using multiple receiving accounts to launder his funds and so needed to be mindful of the risk of alerting fraud detection systems at those banks too.

[1] "Payment Services and Electronic Money – Our Approach", https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

SBI UK has said that it can't be held responsible for the fact that someone was able to hack the security credentials for his account. But the PSRs are quite clear about what the expectations on the bank are where transactions haven't been authorised. The requirement to pay a refund isn't contingent on the bank being at fault for allowing unauthorised transactions to take place.

There are some exceptions to this set out in the PSRs. In summary, Mr S was expected to take reasonable steps to keep the security credentials for his account safe. If he failed to do so (either with intent or with gross negligence), SBI UK doesn't need to refund him. However, I don't think I have any reasonable grounds for saying any of these exceptions applies. Mr S tells me that he didn't voluntarily share this information with anyone else. He lives alone and no other person has access to the security credentials for his account.

SBI UK has argued that, since malware has to be downloaded onto a person's device, only Mr S can be considered responsible for what happened here. It's also argued that he should've taken action in response to the email from N. That email, it argues, put him on notice that he was at risk of fraud.

However, the question I have to address here is whether or not Mr S has displayed signs of "gross negligence" and so failed to comply with regulation 72. The FCA guidance I referred to earlier in this decision says:

> *"…we interpret "gross negligence" to be higher than the standard negligence under common law. The customer needs to have shown a very significant degree of carelessness."*

Relevant case law suggests the term covers conduct undertaken with "actual appreciation of the risks involved" or "serious disregard of or indifference to an obvious risk." [2]

I accept it's likely that malware ended up on Mr S's device as a result of some action he took. That doesn't mean he acted carelessly. By its very nature, malware attempts to infect devices by being packaged with something seemingly legitimate. I don't know for sure what that was in this case, but even if I thought Mr S had acted carelessly (and I'm not persuaded that he did), that would still fall short of meeting the bar for gross negligence.

As far as the email from N is concerned, my understanding of the wider context is that N were concerned Mr S was at risk of falling victim to what's known as an authorised push payment ("APP") scam. In those scenarios, a customer is duped into authorising a transfer to another person. The fact that Mr S appeared to be at risk of such a scam in March 2023 wasn't an indication that the security credentials for his SBI UK account had been compromised.

> *Fraud prevention*
>
> *In addition to the obligations set out above, good industry practice required that SBI UK be on the lookout for payments that were out of character or unusual to the extent that they might have indicated a fraud risk. On spotting such a payment, I'd expect it to intervene in a manner proportionate to the risk identified.*

---

[2] Red Sea Tankers Ltd v Papachristidis [1997] 2 Lloyd's Rep. 547

I'm satisfied that the first payment that was transferred from the account was out of character. It was significantly larger than other payments from this account and was being made to a new payee. This pattern of account activity is consistent with several potential scam types. The bank ought to have been concerned that Mr S might be at risk of financial harm due to fraud.

SBI UK shouldn't have processed that first payment without first making enquiries with Mr S to satisfy itself that he wasn't at risk. If it had done so, it's more likely than not that all of Mr S's losses could've been prevented. Even if I were to make a different finding on the question of authorisation that I've set out above, I'd still be inclined to uphold this complaint on the grounds that the bank needed to do more to prevent the fraud.

Addendum to the provisional decision

Mr S responded to query whether SBI UK would be expected to pay additional compensation for distress and inconvenience. He set out in writing his reasons why he considered it should. On 4 July, I emailed SBI UK to explain that I agreed:

" … DISP 3.7.2R gives an ombudsman the power to make four separate types of money award, whether or not a court would make an award in the same circumstances. My provisional decision set out my intention to make an award for financial loss, but I'm also able to make awards for "distress or inconvenience." Mr [S]'s email asks me to award additional compensation in those categories. So I've considered whether I'm minded to make such an award.

To be clear, any award would not be designed to reflect the totality of the distress he has experienced. I'm mindful of the fact that, while he clearly has suffered tremendously, the overwhelming majority of that is the fault of the fraudsters, not the bank.

I don't make any finding on some of the claims [Mr S] has made, such as the allegation that SBI UK has inadequate fraud prevention measures in place and that it failed to fully cooperate with the law enforcement authorities. I don't know if his characterisations are fair. Nonetheless, these are regulatory matters and are an issue for the Financial Conduct Authority. I also think that some of the losses he's referred to … weren't reasonably foreseeable to SBI UK. I don't think it would be reasonable to award additional compensation in connection with it.

However, I do have concerns about the way things were handled. For the avoidance of doubt, I think [Mr S] was a vulnerable customer at the relevant time. I've considered the FCA's guidance on treating vulnerable customers fairly (FG 21/1). His age and his significant health problems certainly made him potentially vulnerable. But he'd also fallen victim to a devastating crime which is frequently psychologically harmful to customers who don't have these other personal factors.

The bank is entitled to defend itself and to make the argument that he's partially responsible for what happened. However, [Mr S]'s vulnerability meant it needed to make sure it responded to the complaint carefully and with empathy.

I quoted an FCA guidance paper in my provisional decision which was most recently updated in November 2021. That guidance says that, in cases such as these, the burden of proof is on the bank and that "if a claim that a transaction is unauthorised is rejected, the rejection must be supported by sufficient evidence to prove that the customer is guilty of fraud, gross negligence or intentional breach and the reason for

the rejection must be explained to the customer." However, SBI UK's response to the complaint didn't make clear what the bank's position was. I don't think [Mr S] understood whether the bank was saying that he authorised the payments or that it accepted he hadn't done so, but had been grossly negligent in respect of the account's security credentials. That put [Mr S] in a difficult position in terms of presenting his case.

The provisional decision also proposed that the complaint be upheld on the grounds that the payments should've triggered an intervention by the bank and that would've enabled it to protect [Mr S] from fraud. This service's approach on that issue has been set out in several decisions issued to SBI UK. The oldest of these was issued in September 2021. Guidance at DISP 1.3.2A says that firms need to have procedures in place to ensure that "lessons learned as a result of determinations by the Ombudsman are effectively applied in future complaint handling …" In other words, I think SBI UK ought to have known that an uphold on this basis was, more or less, inevitable. It could, therefore, have made at least a partial offer to settle the complaint a year ago and minimised the distress caused to [Mr S].

Finally, there is the matter of whether [Mr S] was denied access to his money. I've only been given a partial history of the communications between the bank and [Mr S]. I can see that he emailed the bank on 9 June, said that he was now living with an acquaintance [outside London] and intended to travel to the […] branch to withdraw cash. He was only able to do so on 20 July when a senior manager accompanied him, which is an extremely lengthy delay. SBI UK has said that [Mr S] was told what he needed to do to withdraw any amount he wanted. I've not seen any evidence that he was told how to get access to his money, but the bank should send me any that it can find.

I'm likely to ask the bank to pay [Mr S] additional compensation to reflect the impact of its actions on him, rather than the impact of the scam itself … Taking into account the way this service typically approaches compensation and the evidence that has been presented so far, I think a payment of £1,500 would represent fair compensation here.

Responses to the provisional decision.

Mr S accepted the provisional decision but didn't think an award of £1,500 was sufficient. He argued that the way the bank treated him in the aftermath of the fraud greatly exacerbated the distress he experienced. He argues that it sought to put responsibility for the loss on him and denied him access to his remaining funds when he needed them.

SBI UK also disagreed with the provisional decision and the follow-up email. Its response was lengthy, but the main arguments were:

- Mr S must have written down his account credentials or saved them somewhere electronically for someone to have stolen them.
- The findings regarding malware are supposition. The fact that Mr S found a suspicious app on his phone, in itself, proves nothing.
- Mr S said that he didn't have carers visiting his home, but he's separately confirmed that someone did visit him at home to help him with things such as food preparation. His details were, therefore, potentially open to compromise.
- Prior to the theft taking place, he went into a branch of SBI UK and attempted to open a joint account with a woman significantly younger than him who was not a

relative or living with him. SBI refused the request on the grounds that it was suspicious.

- It was grossly negligent for Mr S to have taken no action in response to the email from N.
- It has provided evidence that 90 messages sent to Mr S's mobile were sent and received successfully.
- It didn't accept that the fraudsters would've had any sensible reason for transferring the funds as they did. They would, instead, have looked to move them on as quickly as possible.
- Mr S must've been grossly negligent in respect of his security credentials because they were, in fact, compromised. If that compromise was a result of malware, it could only have been a consequence of his own actions. He shouldn't be exonerated of responsibility.

It also challenged the additional findings on distress and inconvenience. It said:

- It's uncertain that Mr S was vulnerable at the material time. He's still professionally active and he said that he was writing a book. In the bank's view, there is clearly nothing wrong with his cognitive abilities.
- To assume someone is vulnerable purely based on his age is discriminatory. Mr S might qualify as vulnerable *after* the theft, but not before.
- It's not true that the bank's correspondence was ambiguous as to its reasons for rejecting the complaint and it's clear that Mr S understood them. The volume of emails he sent to the bank regarding the complaint is, in its view, evidence of that.
- It disputed that Mr S was denied access to his own money. It said it did tell him that it wasn't willing to allow him to withdraw £14,000 cash in one transaction because it would've been irresponsible to allow him to do so. However, it said that it was clear with him that he could either withdraw £500 in cash in the branch or have the funds transferred to another bank account.
- Decisions by this service aren't precedents and each case is supposed to be determined on its own merits. It's wrong, therefore, to say that SBI UK was bound to follow the decision of another ombudsman concerning a case with similar facts.

Both parties disagreed with the provisional findings and provided additional evidence for consideration. I've now considered that evidence and come to a final decision.

Findings

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

Authorisation

My understanding of the responses received from SBI UK is that it is now common ground that Mr S didn't authorise these payments. The question that remains in dispute is whether there's sufficient evidence to say that it's more likely than not that he failed to meet his obligations under the PSRs.

There remains considerable uncertainty as to how fraudsters were able to access his account. Mr S has suggested that malware was the root cause. There is some evidence to suggest that malware was a possible explanation. Nonetheless, SBI UK is right to argue that there is no definitive proof that this is what happened. However, the fact that his email

account was clearly compromised, his device had malware found on it at the relevant time, an unknown individual sent an email using his email account, and that the individuals who carried out the payments did so using IP addresses located in India does suggest that it's unlikely this was an opportunistic theft of his security credentials by someone who visited Mr S's home.

SBI UK has said that Mr S might have left information vulnerable to being found by a fraudster – for example, online banking log-in credentials stored on his PC. He says that he didn't. But if he did, while I can see that it would be careless, I'm not persuaded it would constitute gross negligence.

SBI UK has argued that Mr S was grossly negligent in not taking action after the email he received from N. As I understand it, Mr S placed an advertisement for someone to work for him. He spoke to a woman on the telephone who had enquired and had a positive impression of her. I understand she was based in another part of the country and never met Mr S in person. On 27 March 2023, he attempted to make a relatively small payment to her. N stopped him from doing so because it had concerns about the account he was paying. I understand that this woman managed to obtain some ID documents from Mr S and attempted to use them to take out loans in his name.

I think it's unlikely that this interaction alone would've enabled her to hack into his email account and gain access to files on his computer or mobile phone. On balance, I still think it's likely that this incident and the subsequent fraud weren't connected. Mr S had placed a job advert on an online forum which is notoriously rife with scammers. He was, perhaps, insufficiently cautious in his dealings with the person who contacted him, but I don't see that it played a role in the fraud that he later fell victim to. Although SBI UK has said Mr S should've acted in response to the email from N, it isn't clear to me what action he could've taken to protect himself that would've prevented the fraud that later took place.

SBI UK is concerned that I have attached too much weight to Mr S's own testimony when reaching my findings on this complaint. It has argued that his recollections ought to be treated with more scepticism. For example, it says that the zeal with which he pursued his complaint and sent lengthy correspondence to senior employees of the bank, is not consistent with a man who is suffering with dementia. However, the evidence demonstrating his vulnerability is unambiguous. Medical notes provided to me by Mr S show that he was hospitalised in late 2022 after he was found on the floor of his home by a carer. The discharge summary records that he walks using a cane, was taking donepezil (a drug used in the treatment of dementia) and had been known to the memory service at his local NHS Trust since 2012.

SBI UK has pointed out that Mr S has said that he lived alone, but an email he sent to the bank on 9 June 2023 talks about him needing to pay for carers. Furthermore, SBI UK has said that Mr S told it he had someone come into his home daily for an hour to help him prepare food. It says, therefore, that his details were open to potential compromise. But even if it were theoretically possible for someone to piece together the necessary information to take control of his online banking, he wouldn't be grossly negligent because it had been possible to do so.

Regarding the OTPs sent to him, SBI UK challenged Mr S's claim that he'd only received one SMS and that this was at the tail-end of the scam. It's highlighted that, in fact, he appears to have received two. Both were received after the scam had taken place. However, I don't think this undermines the claim by Mr S that he didn't see the messages sent while the scam activity was going on.

SBI UK has also mentioned that, on more than one occasion, Mr S visited one of its branches in the company of an unrelated younger woman and made enquiries about opening joint accounts. This doesn't cohere with his recollection. He says that he had a historically good relationship with the bank and would sometimes recommend it to acquaintances, including some of his students. He's also said that, on one occasion he visited the branch to make a generic enquiry as to whether he could nominate a third person who could access his account in the event of his death. He says he was told that there was no such nomination system in the UK, but the closest thing he could do to achieve the same objective would be to open a joint account. Since these incidents took place some time before the fraud and the woman who was involved in the N fraud case wasn't one of them, I don't think its relevance is obvious.

Finally, SBI UK challenged my argument that the fraudsters may have chosen to not move Mr S's money in one transaction for fear of triggering its fraud prevention systems. It says that the most efficient way to transfer out the funds would've been in two lump sums and that prolonging things simply increased the risk of the fraud being detected. It is undeniably true that prolonging the fraud would increase the risk of detection. However, the ultimate beneficiaries of frauds like this are usually not the people that receive the initial funds. Fraudsters use accounts belonging to other people (i.e., money mules) to launder the fraudulently obtained funds. The fraudsters would need to ensure that those accounts were available to receive them. Furthermore, anything paid into those receiving accounts would need to be moved on and the businesses operating them will also have fraud detection systems that need to be evaded.

Distress and inconvenience

My addendum to the provisional decision explained what I was minded to do when reaching a decision on this case, but that was subject to any further representations from the parties. SBI UK responded at length to that email and, having considered the additional evidence it's submitted, I've decided to vary the amount of compensation I'm awarding here. I know that this will be greatly disappointing to Mr S, but I'll explain my reasons for doing so.

SBI UK made detailed representations about whether Mr S was vulnerable. From the evidence I've seen, SBI UK wouldn't have had any reason to know that Mr S was potentially vulnerable prior to the theft of his funds taking place. But in my view, his falling victim to fraud combined with his age and health meant he was vulnerable in the immediate aftermath. While Mr S is self-evidently an intelligent and well-educated individual, he's not an expert in the relevant law and regulations applicable to his case. It was, therefore, unhelpful that the final response issued by the bank on 2 June 2023 was ambiguous as to the bank's position.

My reading of that letter is that it suggested that, so long as the bank wasn't directly responsible for allowing a third party to access his account, it couldn't be liable under the relevant rules. However, that isn't the case. The PSRs can require that refunds be paid, even in circumstances where there is no fault on the part on the firm. I do think this ambiguous way of describing the position was potentially misleading and made Mr S's position in terms of pursuing the complaint more difficult. The fact that Mr S was able to write at length to senior employees of the bank about the full extent of his dissatisfaction is neither here nor there.

I've also considered the question of whether Mr S was denied access to his own money. In response to my provisional decision, SBI UK has provided me with several pieces of email correspondence. I gather Mr S initially wanted to withdraw his entire outstanding balance in cash, but the bank objected to him doing this. Mr S says that he did this because the police officer investigating the fraud had told him he needed to do so. I don't doubt or disbelieve

Mr S when he says that is what he was told. However, it does strike me as an unusual piece of advice. I think the bank was right to exercise some caution here and be mindful of the risk to Mr S if it allowed him to make such a large withdrawal in cash.

The other email correspondence also suggests that the bank made him aware that there would be a daily limit for withdrawals of £500. An email to Mr S on 11 June 2023 said the bank *"will transfer your money to any of your other accounts and you can withdraw £500 daily …. As indicated, SBI UK is happy to transfer funds into one of your external accounts if you can provide the Bank with these details…"* SBI UK's records also indicate that Mr S visited the branch on 16 June 2023 and asked to withdraw more than £500. A bank employee characterised his behaviour in the branch as *"very aggressive"* – I obviously can't know if that's a fair characterisation because I wasn't present. It's also understandable that Mr S would feel some anger regarding the situation. Unfortunately, I think the bank's records do suggest it was reasonably clear with him about what he needed to do to access his funds and that it struck a reasonable balance between its obligation to protect him from financial harm and not denying him access to funds that belonged to him.

I know that Mr S regards the amount of additional compensation I recommended in my email as derisory. He thinks fair compensation would need to be 15-20 times that sum. However, I must have regard to the way this service typically approaches compensation in matters like these. The information published on our external website gives anonymised examples of scenarios and the awards we've made in the past[3] and even the most egregious example on that page resulted in us only awarding £8,000.

There's no question that Mr S has suffered an extraordinary amount of distress and inconvenience as a result of these events. I also agree that the bank should've responded to the complaint in different terms. Its response was defensive, which I don't think was appropriate given the vulnerability of Mr S. Nonetheless, the email records do show that the bank took reasonable steps to enable Mr S to access his money. This was a significant reason for the award I recommended in the email of 4 July and so I have no choice but to reduce the amount of compensation I direct the bank to pay. In the light of that additional evidence, I've decided SBI UK should pay £1,250 for distress and inconvenience.

Final decision

For the reasons I've set out above, I uphold this complaint.

If Mr S accepts my final decision, State Bank Of India (UK) Limited needs to:

- Refund the unauthorised payments made from the account.
- Add 8% simple interest per annum to those payments calculated to run from the date the payments debited the account until the date any settlement is paid to him.
- Pay Mr S £1,250 in recognition of the distress and inconvenience caused.

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

James Kimmitt
Ombudsman

[3] https://www.financial-ombudsman.org.uk/consumers/expect/compensation-for-distress-or-inconvenience