complaint

Mr and Mrs W complain that TSB Bank Plc won't refund a payment of £6,400 taken from their bank account, which they say they didn't authorise.

background

Mr W was the victim of a scam in February 2019. He received a phone call from a third party that was able to gain access to his mobile device and internet banking where a payment of £6,400 was made from his joint account with Mrs W, which he says he didn't authorise. Mr W wants this money returned to his account.

It's not in dispute that what happened was an act of fraud. So I have used the term "fraudster" throughout to refer to the third party involved.

Mr W says he was contacted by telephone on 27 February 2019 by the fraudster who was purporting to be from the telecoms provider BT. The fraudster said that his IP address had been compromised and was showing as being located in Amsterdam rather than the UK. Mr W said he checked his IP address and that it did specify the location as 'Amsterdam' as the fraudster had said. He also says that Openreach (a subsidiary of BT) had maintained his broadband connection in the past, so he believed the call to be genuine.

The fraudster told Mr W that every time he went onto the internet, others would be able to see what he was doing. Mr W was asked which websites he usually visits and he gave some examples. The fraudster told Mr W that he could see over 100 instances of somebody having accessed his internet connection where they were able to view the websites he was visiting. Mr W was told that he could resolve this issue by downloading certain apps to his smart phone and running a programme.

Mr W was asked to download a CMD Terminal Emulator app, as well as an 'add-on' programme to his mobile device. When he opened these apps, he said it showed him all the websites he had visited, along with corresponding warnings and error messages. The fraudster asked Mr W to enter the words "security check" where the warning messages were displayed. Mr W then says it displayed a message saying "security check OK", which he believed was helping to make his internet secure.

The fraudster then asked Mr W to check his laptop computer. While he was waiting for it to load, Mr W says he logged onto his internet banking on his mobile device to check his accounts were safe. He says he wasn't asked to do this by the fraudster, but says he was worried his accounts could have been accessed as a result of his IP address being compromised. But having checked his internet banking, he saw that all of the accounts were showing the correct balance.

Mr W says the fraudster then asked him to download 'Team Viewer' (a remote access programme) to his laptop so they could show him how slowly it was operating as a result of other people accessing his connection. He was shown figures relating to his download and upload speed and was asked to take over ten separate readings, after which point he was told that he could log off as everything was now secure, but that he shouldn't use his internet over the next 24 hours.

Mrs W returned home shortly after Mr W had spoken with the fraudsters. She discovered two text messages from TSB on her mobile phone which stated that two of their accounts held

insufficient funds, so she contacted TSB as she didn't think this was correct. TSB asked whether Mr or Mrs W had made any payments, as £6,400 has been paid to a personal account. When Mr and Mrs W said they hadn't, they were advised to contact the fraud department as they had fallen victim to a scam.

TSB have said that the following activity occurred on Mr and Mrs W's accounts on 27 February 2019:

Date	Time	Event	Amount
27/02/2019	13:30	£1,500 transferred from Mr and Mrs W's joint Classic Plus account to joint Classic Enhance account.	
	13:30	Alert sent to the registered mobile phone in relation to the joint Classic Plus account: *"TSB A/C5360. 27 Feb. As you're near your limit, please make sure you have enough in you're a/c to pay for upcoming transactions*".	
	13:32	£1,500 transferred from Mr W's sole Classic Plus account to joint Classic Enhance account.	
	13:32	Alert sent to the registered mobile phone in relation to Mr W's sole Classic Plus account: *"TSB A/C5468. 27 Feb. As you're near your limit, please make sure you have enough in you're a/c to pay for upcoming transactions*".	
	13:53	A one-time passcode (OTP) is sent to the registered mobile phone: "*Hello TSB here. Use your One-Time Password ****** to confirm payment of £6,400 to a/c ending 7663. Didn't request this? Please call us on the number on the back of your card or in our mobile app. DO NOT SHARE THIS OTP WITH ANYONE.*	
	13:54	OTP confirmed and £6,400 transferred out of Mr and Mrs W's joint Classic Enhance account to a third-party account ending 7663.	£6,400
			Total: £6,400

TSB asked Mr W if he had shared the OTP with the fraudster when the new beneficiary was set up for the payment of £6,400. Mr W told TSB he had never received the text message containing the OTP, and that he couldn't now find this on his phone either. He also says that he did not share any of his security or login details with the fraudster, but that he had downloaded some apps onto his phone as instructed by them. TSB contacted the beneficiary bank but were unable to retrieve any of the funds. They considered the social engineering scam Mr W had fallen victim to, but refused to refund the amount taken from his joint account. In summary, TSB said:

- A six-digit OTP was sent via text message to the registered telephone number for Mr W held on record, which had to be entered into a screen on his internet banking to confirm the authenticity of the payment.
- While the caller may have appeared genuine, Mr W has ultimately allowed the fraudster to access his internet banking because he logged in while they had control of his device.
- A short while after Mr W logged into his account, a new beneficiary was created and verified, and the software downloaded to his mobile device has allowed the fraudster to view the OTP sent by TSB.
- Prior to making any new payments, TSB's website provides a number of warnings to all customers about social engineering scams. They had no reason to suspect that the

payment was not genuine at the time, so they had no reason to prevent it from being made.
- While they appreciate Mr W may not have authorised the payment himself, he had been grossly negligent by allowing someone to gain remote access to his computer and mobile phone by downloading their recommended software, which ultimately gave them access to his internet banking and the ability to receive the OTP to confirm the payment.
- Given that Sky was Mr W's telecoms provider, there was no reasonable explanation as to why he should receive a call from BT, so he ought to have recognised that it wasn't a genuine call.

Unhappy with TSB's decision, Mr and Mrs W brought their complaint to this service. Mr W says he was also unhappy with the way he was treated by TSB after reporting the scam. He has also explained how distressing it was to him and Mrs W to be told that they wouldn't be getting a refund of the funds that were taken.

Our investigator upheld Mr and Mrs W's complaint. He didn't think Mr W had authorised the transactions, and also didn't think he had failed with intent or gross negligence to comply with the terms and conditions of the account, or to keep his security details safe.

TSB disagreed with our investigator. They maintain that Mr W's actions had fallen below the standard of a reasonable person because he allowed remote access to his internet banking to someone who was claiming to be from BT when in fact Sky was his telecoms provider. As such, they consider he was grossly negligent. TSB requested a final decision, so the matter has been passed to me to decide.

my findings

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

When considering what is fair and reasonable, I'm required to take into account: relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time. Having done so, I've decided to uphold Mr and Mrs W's complaint.

relevant considerations

TSB as an FCA regulated firm provided a current 'deposit' account. As such the FCA's overarching principles for business apply including the requirement to 'Treat Customers Fairly'. This fraud took place in February 2019, so of particular relevance to my decision about what is fair and reasonable in the circumstances of this complaint, are the Payment Services Regulations 2017 (the PSRs 2017) which apply to transfers like the ones made from Mr and Mrs W's account. Among other things the PSRs 2017 say:

*"**Consent and withdrawal of consent***

67.—(1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to—

(a) the execution of the payment transaction; …"

Obligations of the payment service user in relation to payment instruments

72.—(1) A payment service user to whom a payment instrument has been issued must—

(a) use the payment instrument in accordance with the terms and conditions governing its issue and use; and

(b) notify the payment service provider in the agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(3) The payment service user must on receiving a payment instrument take all reasonable steps to keep its personalised security features safe…

Evidence on authentication and execution of payment transactions

75.—(1) Where a payment service user—

(a) denies having authorised an executed payment transaction; or

(b) claims that a payment transaction has not been correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency.

(2) In paragraph (1) "authenticated" means the use of any procedure by which a payment service provider is able to verify the use of a specific payment instrument, including its personalised security features.

(3) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider is not in itself necessarily sufficient to prove either that—

(a) the payment transaction was authorised by the payer; or

(b) the payer acted fraudulently or failed with intent or gross negligence to comply with regulation 72.

Payment service provider's liability for unauthorised payment transactions

76.—(Subject to regulations 74 [Notification of unauthorised or incorrectly executed payment transactions] and 75, where an executed payment transaction was not authorised in accordance with regulation 67, the payment service provider must immediately—

(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.

Payer's liability for unauthorised payment transaction

77.—(1) Subject to paragraphs (2) … the payer is liable up to a maximum of £35 for any losses incurred in respect of unauthorised payment transactions arising—

(a) from the use of a lost or stolen payment instrument; or

(b) where the payer has failed to keep the personalised security features of the payment instrument safe, from the misappropriation of the payment instrument.

(2) The payer is liable for all losses incurred in respect of an unauthorised payment transaction where the payer—

(a) has acted fraudulently; or

(b) has with intent or gross negligence failed to comply with regulation 67.

consent

Regulation 67 says that the payer must give consent, and it *"must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider"*. The payment services directive itself (which the PSRs 2017 implement) says *"In the absence of such consent, a payment transaction shall be considered to be unauthorised."* Neither the PSRs 2017 nor the FCA's guidance on PSRs 2017 provides a definition of "*consent*".

Therefore, when considering whether consent was given, I'll apply the common definition of consent, which is to give permission for something to happen.

gross negligence

Whether a customer has acted with "gross negligence" is something that can only be assessed on a case by case basis taking into account all the circumstances. The term is not defined in the PSRs 2017 or in the Payment Services Directive. However, recital 72 of the second Payment Services Directive provides as follows:

"In order to assess possible negligence or gross negligence on the part of the payment service user account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness, for example keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties..."

Reflecting this, the FCA, in its document setting out its role under the Payment Services Regulations 2017, says:

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

Although not specific to this case, the FCA's interpretation is of value as a relevant consideration in the absence of contemporaneous interpretive guidance, and because it informs the meaning of a concept that had been in place for some time in the Banking Code.

When considering gross negligence in a commercial contract context, Mance J in Red Sea Tankers Ltd v Papachristidis (The "Ardent") [1997] said:

"If the matter is viewed according to purely English principles of construction, ... "Gross" negligence is clearly intended to represent something more fundamental than failure to exercise proper skill and/or care constituting negligence... as a matter of ordinary language and general impression, the concept of gross negligence seems to me capable of embracing not only conduct undertaken with actual appreciation of the risks involved, but also serious disregard [sic] of or indifference to an obvious risk."

Negligence is often referred to as a failure to exercise reasonable care. And, as I have described above, the use of 'gross negligence', rather than mere 'negligence', suggests a lack of care that goes significantly beyond ordinary negligence or carelessness.

So I have to consider whether Mr W's actions fell so far below the standard of a reasonable person that he failed with gross negligence to keep his personalised security details safe or to comply with his account terms and conditions.

intent

Intent is not defined in the PSRs 2017 nor in the Payment Services Directive. I'll therefore apply the natural meaning of intent - that being: something you want and plan to do, a deliberate act.

This is also consistent with the FCA's 2013 guidance on the PSRs 2009, which gives a helpful indication of the regulator's view of what it means, and refers to:

- 8.108 a customer who *"deliberately …failed to comply"* with their obligations.
- 8.116 a customer who *"has intentionally …not complied with their obligations...the burden of proof lies with the payment service provider … the rejection must be supported by sufficient evidence to prove that the customer is guilty of … intentional breach".*

The guidance also gives an indication of the regulator's view of what's meant by taking all reasonable steps to keep a payment instrument's personalised security features safe at Regulation 57(2) PSRs 2009:

- 8.97 *says "What constitutes reasonable steps will depend on the circumstances, but payment service providers must say what steps they expect customers to take in their pre-contract disclosure information."*

I think what the PSRs 2017 mean, is that when considering whether a payment service user failed to comply with their obligations with intent, the test I need to consider is whether they appreciated that by taking the actions or inactions they did, they would be failing to meet these obligations.

the terms and conditions of Mr and Mrs W's account

The following are extracts from the general terms and conditions applicable to Mr and Mrs W's account at the time. These terms and conditions broadly reflect the provisions contains in the PSRs 2017.

"You must always keep your cards, chequebooks and security details safe at all times."

"Don't let anyone know your security details. You can prevent this by:

- *Not choosing obvious passwords or codes like your name or date of birth.*
- *Not writing down your security details in a way that can be understood by someone else.*
- *Not letting anyone hear or see your security details. They could overhear a call you have with us or see you entering your PIN at a cash machine."*

"Don't let anyone either use your account or have access to information about your account, unless you've allowed them to do so in a way agreed with us."

"If you don't keep your account safe, you may be responsible for money that is taken out of your account and payments that are made as a result."

The terms also say:

"When we won't refund you:

- *You've been acting fraudulently…*
- *You haven't kept your card or security details safe – either intentionally, or by being very careless, when your account is in credit…*
- *You've deliberately not told us that you've lost your card or security details, or you've been very careless. This applies as long as your account is in credit.*

I think, therefore, there are two key questions relevant to my considerations:

1. Were the disputed transactions authorised by Mr W? and;

2. If they weren't, did Mr W fail with intent or gross negligence to comply with his obligations under Regulation 72 of the PSRs 2017 – in particular, did he fail to comply with the terms and conditions of his account or to keep his personalised security details safe?

were the disputed transactions authorised by Mr W?

In order for a payment to be regarded as authorised, it's necessary for Mr W to have given his consent to the execution of the relevant payment transactions. In their submissions to us, TSB accept it's unlikely Mr W authorised the payment from his joint account, and that it was likely the fraudster that had intercepted the OTP as a result of Mr W downloading the apps on to his phone, which subsequently allowed them to authenticate the payment on his internet banking.

So, as it's not in dispute that the payment wasn't authorised by Mr W, I see no reason to explore this point any further. And based on the evidence I've seen, I do not think Mr W consented to this payment in any event.

did Mr W act with intent – particularly taking into account the terms and conditions of his relationship with TSB and the obligations set out in the PSRs 2017?

I don't think TSB have suggested that Mr W failed to comply with his obligation under regulation 72 with *intent,* but I will address this point briefly in any event.

The question I need to consider is whether Mr W appreciated that his actions or inactions in the circumstances meant that he wasn't complying with the terms and conditions of his account and/or he appreciated that he wasn't taking all reasonable steps to keep his personalised security features safe. But in the circumstances, I don't think Mr W failed to comply with his obligations with intent under the PSRs 2017.

Mr W said he downloaded some software onto his mobile device, but that he didn't appreciate the fraudster could see him logging on with his secure information while he accessed his online banking. He says the fraudster hadn't asked him to do this, and neither did they ask him to disclose any of his account information. But Mr W says he was worried his internet had been hacked as a result of what the fraudster had shown him. So while he was waiting for his laptop to load up, he logged into his internet banking on his phone to check on his account balances.

I accept that Mr W had downloaded certain apps to his phone at the fraudster's instruction. But he was told that this was to enable him to carry out security checks on the websites he'd visited, and in order to run a programme to make his internet secure. So I don't think it's likely Mr W knew the fraudster had the level of access to his phone that they did. But even if he *did* know they had some form of access, I don't think this means he knew that the fraudster would be able to see what he was doing, or would be able to make use of his online payment services. So I don't think he recognised there was any risk in logging on to his internet banking when he did.

Taking into account everything Mr W was told as to why he needed to download the apps to his phone, I don't think he realised or appreciated he was not complying with his account terms and conditions, or that he was failing in his obligations to take reasonable steps to keep his personal security information safe. Indeed, I consider it more likely than not that the actions Mr W thought he was taking were intended to keep his internet connection (and internet banking) secure, so I don't think he would've appreciated that his actions meant he was in fact breaching his account terms or failing to prevent his account from being accessed by an unauthorised party. It therefore follows that Mr W can't have failed to comply with his obligations under regulation 72 with intent if he did not appreciate the true nature of what he was doing.

did Mr W act with gross negligence – particularly taking into account the terms and conditions of his relationship with TSB and the obligations set out in the PSRs 2017?

I've gone on to consider whether the actions Mr W took fell so far below the standard of a reasonable person that he failed with gross negligence to take all reasonable steps to keep his security information safe or to comply with the terms and conditions of his account.

As I set out earlier, negligence is often referred to as a failure to exercise reasonable care. And the use of 'gross negligence' rather than mere 'negligence' suggests a lack of care that goes significantly beyond ordinary negligence. So I've thought about Mr W's actions and considered what a reasonable person would do in his circumstances.

Gross negligence is not an abstract concept. It's important to take into account all the circumstances when considering whether an individual's action amount to gross negligence. Scams such as the one experienced by Mr W are very sophisticated, and it's likely the fraudster used a range of social engineering techniques to trick, deceive and manipulate him

into following their instructions and inadvertently allowing access to his internet banking and confidential security information.

TSB submit that Mr W ought to have known that the person he was speaking to was not genuine because BT is not his telecoms provider. As such, they say he has been grossly negligent by following their instructions and failing to terminate the call. Mr W has explained that his broadband connection is maintained by Openreach, who are a subsidiary of BT. He says they have visited his property before when he had problems with his internet signal, and on another occasion when his internet connection was lost all together. So although Sky may be his telecoms provider, he didn't think it was necessarily unusual that BT (or any of their subsidiaries) might be contacting him to discuss potential issues with his internet connection again, given his previous dealings as a customer of Openreach.

I've thought carefully about this. And in the circumstances, although BT may not have been his direct provider, I consider it's plausible that they could be contacting him about his broadband connection, particularly as he considered himself to be a customer of theirs given his past dealings with Openreach. So I don't think this is enough in itself to suggest Mr W has been grossly negligent.

As I've set out previously, the fraudster then told Mr W that his internet connection had been compromised and that his IP address was showing as being related to somewhere in Amsterdam rather than the UK. Mr W says he did not know a lot about IP addresses, but was concerned by what he heard and followed the fraudster's instructions on how to check this on his mobile device. He doesn't remember where exactly he was told to check it, but he thinks it was within the 'settings' options of his device, which did in fact display the word 'Amsterdam' as well as the name of an unknown individual the fraudster said had been accessing his connection.

Given that this matched what the caller had initially told him, Mr W says he believed the fraudster was genuinely calling from Openreach. It isn't clear what he was told to access on his phone or why it displayed his IP address as showing in Amsterdam. But seeing as Mr W was able to verify what the fraudster was telling him on his own mobile device (and taking into account his previous dealings with Openreach as outlined above) I don't think he had any reason to believe the phone call he received was not genuine.

The fraudster then convinced Mr W he had to take action as his IP address and internet connection had been compromised, such that other people could see what he was doing and the websites he was visiting. But he was told that he could remedy this by downloading some apps onto his phone that could run security checks and help secure his internet. After typing in the websites he usually visits, Mr W was subsequently shown some further alarming information in the form of warning messages, which he says suggested that that other people had gone on to certain websites at the same time as him through his connection. This further concerned Mr W because he uses his mobile device and internet connection to manage his accounts online through his internet banking with TSB.

As I've outlined earlier, although Mr W followed the fraudsters instructions and downloaded the apps to his phone that likely allowed them to take control of his device, I don't think he knew this software would allow the fraudster to do this. But given that Mr W thought he was dealing with a business he knew, trusted and had dealt with before – and given he was made to feel worried about potential illegal and fraudulent activity taking place via his internet connection – I think a lot of people would have believed what the fraudster was

saying. So I think it's most likely that Mr W thought the apps he was downloading were to help carry out checks to counteract any potential fraud.

It was in this context that Mr W took the steps that he did, such as logging on to his internet banking to check it was secure while the fraudster could seemingly access his device and see what he was doing. And I think a lot of people in a similar position would've behaved in a similar way in those circumstances. So it follows that I don't think the actions Mr W took here fell so far below the standard of a reasonable person, such that he failed with gross negligence to keep his personalised security details safe or to comply with the terms and conditions of his account.

Once Mr W had logged onto his internet banking on his mobile device, the fraudster asked him to perform a series of tasks on his laptop, where they said they were monitoring his internet speed and got him to record different readings. They also told him that he should not use his laptop or mobile phone for 24 hours. I think it's likely they asked him to do this so as to keep him distracted while they accessed his internet banking that he had recently logged on to.

Mr W also says he did not receive any text messages to his phone that contained the OTP to confirm payment to the new beneficiary set up on his account by the fraudster. TSB accept that it's likely the fraudster was able to intercept the OTP as a result of the access they had to Mr W's device. And given that it's accepted that Mr W likely didn't share any of this security information with the fraudsters, I don't need to consider whether any such actions would constitute gross negligence in the circumstances.

When thinking about what a reasonable TSB customer would do in Mr W's circumstances, I think it's relevant that once someone believed they're dealing with someone trustworthy, and when they believe they're acting to secure their internet connection and accounts, it can take something quite significant to break that spell. On balance I don't think anything did happen to break the spell Mr W was under at the time. I appreciate that balance alerts were sent to Mrs W's phone, but Mr W didn't receive any of these messages. And there was nothing else that would've reasonably alerted him to the fraudulent activity that was unfolding.

When under this sort of pressure, I also can't ignore that Mr W wasn't necessarily in a position to make rational and informed decisions. Mr W has not mentioned that he is experienced in IT or security related matters either (in fact, he said he did not know a lot about IP addresses at the time). So when someone in this position is made to worry that they're being hacked (such that their internet banking security and money could also be under threat) I think it's likely they'd be much more inclined to follow the instructions of those that they believe are more knowledgeable on the subject matter.

I'm satisfied that gross negligence should mean a very significant degree of carelessness, involving a serious disregard or indifference to an obvious risk. As this is a high bar, it isn't enough to say Mr W was grossly negligent simply because he downloaded certain apps to his mobile device and later logged on to his internet banking to check his account balances. And having taken all of the relevant considerations into account, I'm not persuaded that his actions fell so far below what a reasonable person would do in the circumstances to amount to gross negligence. I think in similar circumstances, a reasonable person would've acted in the same way that Mr W did here.

I acknowledge Mr W failed to keep his security details safe and failed to prevent a third-party from accessing his online accounts. But under the PSRs 2017, this in itself only means he

can be held liable for up to £35 of the losses incurred in respect of the unauthorised payments. However, this would need to be set out in the terms and conditions of Mr W's accounts, and as it isn't, I don't think it would be fair and reasonable for TSB to rely on this here.

In summary, I don't find that Mr W failed to comply with his obligations with intent or was grossly negligent. And so I conclude that it would be fair for TSB to provide a full refund to Mr and Mrs W's account.

other considerations

I've considered Mr W's submissions regarding TSB's handling of the matter once the fraudulent activity had been identified. He says they were left with very little money in both his and Mrs W's accounts, which is evident from the bank statements provided and the balance alert text messages sent to Mrs W's phone.

Mr W also says he had to contact TSB several times after being told they would get back to him with an update of whether any funds had been retrieved from the receiving bank. But I can see that he had to chase for updates on a number of occasions when he didn't hear anything.

Having just lost a significant amount of money, this was likely a very worrying time for Mr and Mrs W. And it seems that they were not kept sufficiently updated, such that Mr W felt the need to have to keep on contacting TSB to find out what was happening and whether they were going to get their money back, which I think would've only added to the stress and worry they were experiencing at the time. The investigator recommended an award of £150. But having considered TSB's actions, including the fact that they didn't refund Mr and Mrs W's money when they should have, I consider it would be fair and reasonable for TSB to pay a total of £250 compensation for the trouble and upset caused.

putting things right

My findings mean that Mr and Mrs W have been unfairly deprived of these funds since 27 February 2019. And, as I've outlined above, they were left with little money in their account following the scam, so I think it would be fair for TSB to also apply 8% simple interest per year on this amount from the date it left their account to the date it is refunded.

As I've said above, TSB should also pay Mr and Mrs W £250 compensation for the trouble and upset they've experienced.

my final decision

For the reasons given above, I uphold Mr and Mrs W's complaint and direct TSB Bank Plc to:

- Refund £6,400 to Mr and Mrs W in full;
- Pay 8% simple interest per year on that amount, from the date of the withdrawal of the funds to the date of settlement. If TSB deducts tax from the interest element of this award, they should also provide Mr and Mrs W with the appropriate tax deduction certificate;
- Refund any fees or charges Mr and Mrs W may have incurred on their accounts that directly resulted from the withdrawal of the disputed payments; and

- Pay Mr and Mrs W a total of £250 compensation in recognition of the trouble and upset caused by TSB's handling of the matter.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr and Mrs W to accept or reject my decision before 11 November 2019.

Jack Ferris
ombudsman