complaint

Mr G is unhappy with TSB Bank plc's decision to not refund him after he lost money as a result of a scam.

background

I set out the background to this complaint in the provisional decision issued on 22 March 2019. The facts of the case and available information haven't changed since then so I won't repeat the detail here. A copy of the provisional decision is attached at the end of this final decision.

Since issuing the provisional decision both parties have responded. Mr G has said he broadly agrees with the findings and is happy to accept the outcome I set out.

TSB responded and agreed to refund the disputed transactions and pay interest at the account level for the period Mr G was without the funds. It accepted Mr G was likely unaware of the transactions being carried out. It was silent on the payment of the £300 compensation.

my findings

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

Mr G and TSB have both accepted the outcome as explained in my provisional decision and so there's no need for me to go over the details again.

TSB didn't comment on the £300 compensation I set out in my provisional decision. I don't take that to mean it's necessarily disagreed. But there wasn't an explicit acceptance of that part of the redress and so I'm confirming here that it should pay the £300. There've been no new arguments put forward by either party on the issue and so there's no need to revisit my reasoning on that part of my determination. I've already set out why it should be paid.

my final decision

I've found that Mr G didn't authorise either of the transactions and he didn't, where applicable, act with gross negligence. And as such the complaint should be upheld.

My final decision is that TSB Bank plc should:

- refund £4,600 to Mr G's account;
- reconstruct the account as if the money had never left adjusting any fees, charges and interest accordingly;
- if Mr G's account would have been in a credit balance at any time following these adjustments TSB should pay the interest the account would have benefited from; *and*
- pay compensation of £300 to Mr G. This has been a very worrying time for him, not receiving a refund for a transaction he didn't authorise, after having been the victim of the scam.

If TSB considers that it's required by HM Revenue & Customs to withhold income tax from any interest award, it should tell Mr G how much it's taken off. It should also give Mr G a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 3 June 2019.

Ben Murray
ombudsman

Copy of Provisional decision

complaint

Mr G is unhappy with TSB Bank plc's decision to not refund him after he lost money as a result of a scam.

Mrs G – Mr G's wife – has been involved in this case and so I'll refer to her involvement where appropriate.

background

Mrs G received a call on the home landline on 10 October 2017 from someone saying they were from a telecoms provider. It was the same telecoms provider Mr and Mrs G were genuine customers of. The caller said they were getting in touch as they suspected Mr and Mrs G's broadband was under threat from hackers and viruses.

Mrs G was somewhat suspicious of the caller and asked how they might verify themselves. Mrs G has explained how they already knew some details about her and her husband but the caller also offered to send an email which would verify they were genuinely calling from the telecoms company.

The email was received by Mrs G and having looked at it she was satisfied it was genuine. So she went on to discuss her broadband account and whether there had been any problems with it. The caller offered to increase the level of protection on Mrs G's computer.

I think it's fair to refer to this caller as 'the fraudster' from this point. All parties agree there's been a scam with a fraudster (or fraudsters) involved.

This led to Mrs G allowing remote access to her computer and the fraudster then took control. A link for downloading teamviewer – a piece of software which allows remote access – had been provided in the email sent to Mrs G. Mrs G has explained that she was aware someone was gaining remote access, but believed it was for the purpose of protecting her computer.

The fraudster said they could also check Mrs G's bank account to make sure it hadn't been subject to any attack. Mrs G was persuaded to log in to her online account, held with a different bank; not TSB.

The fraudster said they'd not been able to see any attempts to attack or access Mrs G's bank account. These points form part of the overall circumstances of Mr G's complaint. I'm not actually dealing with what happened to Mrs G or her accounts. But the circumstances are relevant. Mrs G has said there were no losses from her account.

The fraudster then asked Mrs G if there was anyone else in the household that might also benefit from a security check of their own computer and accounts. Mrs G explained that her husband – Mr G – was at home and so the call was passed on to him.

Mr G has told us that the fraudster said they needed access to his computer, as they had with Mrs G, in order to clear it of viruses. Mr G has explained he doesn't regularly use computers or his internet banking and so isn't particularly confident with either. He's told us he knew someone else was accessing his computer, though thought it was only so they could carry out security checks. It isn't clear whether Mr G downloaded teamviewer himself, to his own computer, or whether he used Mrs G's computer on which access had already been given. What does seem to be the case, and accepted by both parties, is that the fraudster did have remote access to the computer Mr G was using at the time.

Mr G explains he was then shown a series of screens which seemed to indicate that his computer was under attack from hackers. On the back of this Mr G was persuaded to log in to his online banking as he was told that could also be under attack. But he couldn't see anything that was happening on screen; the person accessing the computer appears to have been obscuring what was going on. Mr G describes what he could see as lines and lines of numbers, which the fraudster said showed hacking attempts. He says the fraudster prompted him to enter numbers on the computer, but he couldn't see what was actually happening. He says he was aware he was logging into online banking though.

Mr G says the fraudster told him to turn off his mobile phone, which he says he did, putting it in the kitchen as instructed. He's provided copies of his mobile phone bills to show he didn't make any calls that day. Although there is an outbound call to a landline just before the fraudulent transfer, but Mr G has said he didn't make it.

The call ended with Mr G believing he'd secured his account. He says he didn't know any money had left his account at this time.

On 17 October 2017 Mr G received a letter from the bank saying that he was overdrawn. He couldn't understand how that was possible as he'd recently received a statement showing a credit balance.

Mr G contacted the bank the same day and discovered that he'd been the victim of fraud. Two payments had left his account totalling £4,600. The first was for £3,800 and took Mr G's account into an overdrawn position. The second was for £800, further increasing the overdrawn balance.

Mr G says he didn't make or authorise those payments. The money had gone to a new payee set up on the day. Mr G said he didn't set up that new payee and believed it'd been the fraudster that set it up and made the transfers. The fraudster also transferred £1,100 between Mr G's accounts in order to facilitate the fraud.

Mr G asked TSB to look into what had happened and refund him the money. The bank investigated and said it wouldn't be able to give Mr G his money back. It said he'd authorised a new payee and allowed access to his internet banking.

TSB explained when the new payee had been set up there'd been an automated security call to Mr G's mobile phone. TSB says the call had been answered with a security code then being entered into the phone. The code would have been displayed on the screen of the computer being used for the online banking and payee set up. It said it had also sent Mr G a text about the new payee.

TSB has provided us with the message that plays during the automated security call:

"This is an automated call from TSB to confirm you are setting up a new online payment. You're currently setting up a new payment to account ending xxxx for amount £x and xpence. Please key in or say the four digit code now. If you're not expecting this call or haven't set up this payment please press star now".

The security code referred to is displayed on the online banking screen whilst the payee is being set up. The code has to be typed into the mobile phone while on the call. TSB has said this call was made to Mr G's mobile number and was answered successfully and it has provided evidence which it says supports that.

TSB has also provided the message contained in the text sent to Mr G's mobile phone. It reads:

*You set up a new recipient on 10/10 at 13:48:51 from account ending ****. If this wasn't you please call 0345******* or +4420******** from abroad.*

TSB has said this text was sent to Mr G's mobile number and was received by him less than a minute after it was sent. It has evidence to show the time the text was sent and received.

TSB has relied on the call and the text message as evidence that Mr G knew a new payee was being set up and payment being made. It says, contrary to what Mr G has said about his mobile being switched off, he must have answered the call and entered the code to authorise the first payment to the new payee. It also says he must have received the text message when it was sent as its records show it was received less than a minute after it was sent.

TSB has provided some notes taken at the time the fraud was reported which say:

"BT Scam - Loss. Teamviewer, customer authorised [security call] under the pretence of securing account"

And separately:

"[Mr G] was going to make enquiries into what calls were received by him, on his phone, that day. His intention to provide evidence he did not approve any funds to leave his account by taking the [security call]"

TSB has relied on this evidence in declining to refund Mr G.

Mr G wasn't happy with TSB's response. He acknowledged he'd given over access to his online banking but he said he'd not taken a call from the bank or input a code into his phone. He also said he didn't receive a text and said his phone had been off at the time the fraud was underway.

TSB didn't change its position and so the complaint was brought to us for investigation. One of our investigators looked into what had happened and thought the complaint should be upheld in part.

He felt Mr G hadn't authorised the transactions in question as he hadn't known there were payments being made. He said Mr G had authorised the setting up of a payee but that wasn't the same as authorising a payment.

The investigator did feel Mr G had been grossly negligent with his security information. He'd allowed someone pretending to be from a telecoms provider access to his online banking and had divulged personal information. He explained that meant TSB could hold Mr G liable for the transactions up to the point where the overdraft was being used. At that point the provisions of the Consumer Credit Act 1974 applied and so Mr G couldn't be held liable for the loss on the basis he'd been grossly negligent. In light of that he said the bank should refund that portion of the transactions.

Mr G and TSB were unhappy with the outcome. Mr G maintained that he'd had no call from the bank.

TSB initially said it shouldn't be responsible for any planned overdraft cost; it didn't believe the CCA applied for a pre-arranged overdraft. It later changed its position to say that it believed Mr G authorised the transactions and so it shouldn't be responsible.

TSB also pointed to the various warnings it gives to customers about scams and provided screenshots of its online banking pages where such warnings are displayed.

As neither party has agreed with the outcome the complaint has been passed to me for a decision. In conducting my review I've put together a timeline of what happened on 10 October 2017, including all relevant events. I've constructed this using the electronic records TSB has been able to provide.

time (hour: minute: seconds)	event
13:27	Mrs G receives scam BT email
13:34:38	online banking accessed
13:39:27	£1,100 transferred between Mr G's accounts
13:45	outbound call from Mr G's mobile
13:47:22	a new payee's details are created online
13:47:39	the system searches for Mr G's details in order to make the security call
13:48:49	the security call is successfully made to Mr G's mobile phone with the security code being entered
13:48:51	text sent to Mr G's phone confirming the new payee
13:48:52	payment of £3,800 made to the new payee
13:51:38	payment of £800 made to the same payee
13:51:52	log off from online banking

my provisional findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. I'll consider any further submissions from either party but at present I'm minded to uphold this complaint.

Mr G's health has significantly deteriorated since the events subject to this complaint. And so Mrs G has been handling the complaint for him. This change in Mr G's health, and the time that's passed since the scam, has meant some details have been difficult to confirm. And so the background above represents my best understanding of what happened at the time. There may be some points in the timeline above which one party or the other disagrees with. But the overall circumstances described above appear to be accepted by all.

The rules of our service mean that I have to determine this complaint by reference to what I consider to be fair and reasonable in all the circumstances of the case. When considering what is fair and reasonable, I am 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.

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 October 2017, so of particular relevance to my decision about what is fair and reasonable in the circumstances of this complaint, are the *Payment Services Regulations 2009* (the PSRs 2009) which apply to transfers like the ones made from Mr G's account. Among other things the PSRs 2009 say:

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

55.—(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***

"*57.—(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.*

(2) 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***

"*60.—(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 57."

"***Payment service provider's liability for unauthorised payment transactions***

"*61. Subject to regulations 59* [Notification of unauthorised or incorrectly executed payment transactions] *and 60, where an executed payment transaction was not authorised in accordance with regulation 55, 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***

"*62.—(1) Subject to paragraphs (2) …, the payer is liable up to a maximum of £50 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 57."

consent

If a payer denies authorising a payment the PSP must prove that it was "authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency" (PSR 60). In other words, the PSP must show, from a technical point of view, that the steps needed for authorisation were taken. But authentication of a payment is not enough to amount to authorisation by the payer. The payer must also have consented to a payment transaction taking place.

PSR 55 doesn't elaborate on what constitutes consent beyond saying that 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 PSR2009 implement) doesn't explain what consent means here, but says "In the absence of such consent, a payment transaction shall be considered to be unauthorised." And the FCA's
2013 guidance on the PSR2009 didn't say anything further about what consent means.

TSB's terms and conditions from the time don't give a definition of what it considers consent to mean.

It's commonly understood that giving consent means giving permission for something to happen. It follows that, in the context of payment transactions, consent requires the payer to have knowledge that a payment transaction will be executed. So a payment services user who is unaware a payment is being made can't rightly be said to have given their consent to make a payment.

Overall, where a payer denies making a payment I need to be persuaded that the payment was authenticated and that the payer consented to a payment being made from their account.

gross negligence

Negligence is often referred to as a failure to exercise reasonable care. So, the starting point here is to consider whether Mr G failed to exercise reasonable care i.e. whether a
reasonable person in Mr G's position acting reasonably would have acted as Mr G did. But I also need to consider, if Mr G was negligent, whether it is fair and reasonable to say that her negligence amounts to *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 PSR 2009 nor in the first 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 neither of these is directly relevant to this complaint, they are of value as a relevant consideration in the absence of contemporaneous interpretative guidance, and because they inform the meaning of a concept that has 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] 2 Lloyd's Rep 547, 586 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 of or indifference to an obvious risk."

I think it fair and reasonable to conclude (and I note the FCA expressed a similar view in its document), the use of "gross negligence", rather than mere "negligence", suggests a lack of care that goes significantly beyond ordinary negligence.

considering credit

Where credit is involved in cases like this the PSRs make provision for the Consumer Credit Act (CCA) 1974 to apply in place of certain sections of the PSRs. These provisions can't be excluded by the account terms. The relevant sections of the CCA here involve a credit facility.

credit facilities

Where a credit facility has been used the relevant legislation is Section 83 of the CCA 1974. It states:

83 Liability for misuse of credit facilities.

.

(1) The debtor under a regulated consumer credit agreement shall not be liable to the creditor for any loss arising from use of the credit facility by another person not acting, or to be treated as acting, as the debtor's agent.

the General Terms & Conditions of Mr G's account at the time

The following extracts from the general terms and conditions of Mr G's current account are relevant to this case. These terms and conditions broadly reflect the provisions contained in the PSRs 2009.

4.3 You must:

a) follow instructions we give you, which we reasonably consider are needed to protect you and us from unauthorised access to your accounts;

b) not let anyone else use any of your cards or Security Details, not even someone sharing a joint account with you as he or she will have his or her own;

c) keep your cards and Security Details secure and protect cards from damage;

d) do all you reasonably can to make sure no one finds out your Security Details, for example by not:

i. choosing obvious passwords or codes(such as your date of birth) as part of your Security Details;

ii. writing your Security Details on, or keeping them with your cards or banking documentation;

iii. writing down your Security Details in a way that is recognisable; or

iv. letting anyone listen in to your calls with us, or watch you entering or making use of your Security Details;

e) not let anyone else give instructions, or have access to information, on your accounts unless he or she has a separate arrangement with us to do so, or you have authorised him or her to do so under condition 13;

4.6 You must tell us as soon as you can (see the contact details section) if you:

(a) notice any errors;

(b) find our services are not working;

(c) think any cards or Security Details have been lost, stolen, damaged or are being misused; or

(d) think someone may be accessing your accounts without your authority or that someone has discovered your Security Details.

15.2 You will not be liable for any payment instructions you did not give yourself, even if they were given using your card or Security Details, unless we can prove either:

(a) *that you have acted fraudulently in which case you will be liable for all payments from the account that we have been unable to stop; or*

(b) *that you have been grossly negligent with your card or Security Details. Depending on the facts of the case and any legal requirements that apply, you may be liable for payments from your account but only until you have told us that your card or Security Details have been lost, stolen or could be misused.*

If you are not liable for a payment, we will refund the amount of the payment and any charges or interest you paid as a result of it, and pay you any interest we would have paid you on that amount, and will not have any further liability to you.

key questions

Taking all the relevant considerations into account, including those set out above, I think there are three questions that are particularly relevant to my consideration about what's fair and reasonable here.

1. Were the disputed transactions authorised by Mr G?

2. If they weren't, what are the implications of the CCA?

3. If the provisions of the CCA don't apply, did Mr G fail with intent or gross negligence to comply with the terms and conditions of the account?

Though there is naturally some overlap of events when answering these two questions, I will approach them in this order.

were the disputed transactions authorised by Mr G?

Mr G had been convinced by the call he received from the fraudster. That much is clear. He's been the victim of a social engineering scam. I don't know the exact details of what was discussed with Mr G and his wife. I can't now know what it was that convinced him to take the course of action that he did.

We have asked for some more detail from Mr G here but little more about the sequence of events has been forthcoming, which is understandable given what I've said about Mr G's health and the time that's passed. But all parties seem to accept Mr G was tricked by fraudsters into doing what he did and I'm satisfied that was the case too. I think it's worth noting here that, at this point, I'm considering whether Mr G authorised the transactions himself; not whether he was grossly negligent.

There's been some commentary from the bank over how long a period of time this scam was drawn out. Mr G seems to have said there were numerous calls across a number of hours. But the bank has said the fraud took place within a short space of time, going by the times of online banking log ins and when transfers were made.

Again, I can't know exactly what happened here. But I think it's enough for me to say that Mr and Mrs G were clearly persuaded they were talking to a genuine person and that they had genuine cause for concern. And it's certainly possible, given Mr and Mrs G's account(s) of what happened, that the fraudster spent a good deal of time setting up the scam through questioning, setting up remote access and generally convincing – first Mrs G and then Mr G – of the need to act quickly to protect their accounts. I don't think the timings of the transactions themselves show the scam took place over only a short time.

Mr G doesn't dispute that he gave the fraudster access to his computer and logged into his online banking himself. He's also said he probably gave the online banking details to the fraudster. And it's clearly through these actions that the fraudster was able to gain access to Mr G's account.

But in doing so he wasn't aware that there were payments to be made from his account. He didn't know the details of any transfers that were being set up or made at this point. And

indeed with the online banking information alone the fraudster most likely wouldn't have been able to access any of the funds in Mr G's account(s).

It's important to note here that Mr G wasn't carrying out the actions on his online banking himself. And so for the purposes of the account terms and conditions, notably 15.2, it was the fraudster that was accessing the account and the fraudster that went on to set up the new payee. Mr G didn't know about and hadn't consented to those actions.

There are then two different versions of events for what happens once the new payee was set up online.

Mr G has maintained that he had turned off his mobile phone, as instructed by the fraudster. He's said he was even told to put it in a different room, which he did. He says that, having done so, he can't possibly have answered the security call made by TSB. He's also said he never received the text message it sent.

The bank says it made the call to Mr G's registered mobile number. They say it was answered and the security code was entered into the mobile phone, allowing the new payee to be set up. TSB has provided its electronic records which show this and it's confirmed it's the only way a new payee could be set up online. It's also supplied evidence of the text message being sent and received. And so it believes Mr G did have his phone on, did answer the call and did receive the text.

I have to make a finding on what I believe is most likely to have happened here.

I've considered the evidence provided by TSB. It has a step by step record of the online banking activity that day. I can see the time and date being recorded for a number of actions including the initial log in, the transfer of £1,100 between Mr G's account and the creation of the new payee. I can then also see a record of the security call being made as well as a record of it being successfully completed. All of these steps run in the sequence I'd expect to see when a new payee is successfully set up, created and paid money to. There's also confirmation of the number dialled – Mr G's genuine number, held by the bank for several years – within the electronic record.

In addition to the record of the call itself I can see the text message was sent to Mr G. And I'm satisfied it was received less than a minute later, as TSB has said. I've seen evidence from TSB to demonstrate that. It's also provided evidence of texts sent on different dates where there has been a delay in the message being received due to either there being no signal on the phone or it being switched off. So I can see there's a difference between when a text is received right away and when there's a delay.

This evidence is persuasive in showing it is more likely than not that Mr G did receive the security call from TSB, followed by the text. But before concluding that it is the most likely scenario I've gone on to consider alternatives.

I'm aware that some sophisticated fraudsters are able to have calls to mobiles diverted through various means so that a customer never receives security calls and texts like the ones in this case. Sometimes that involves what's known as a 'sim swap'. But there doesn't appear to be any evidence that's happened here.

A sim swap would normally involve the fraudster obtaining a new sim card for the target victim's normal mobile number. The fraudster then uses that new sim to receive any

incoming calls and text which allows them to pose as the customer for the purpose of security checks.

When that does happen, the original sim would normally become inactive and the customer can't make or receive calls or text messages.

Mr G has confirmed there were no significant problems with his mobile phone after the fraud. He mentioned some calls cutting out and a crackling on the line. But he'd been able to use his phone and his number normally at all times to complete calls and send text messages. That's supported by what he's told us but also by his phone bills from the time.

Mr G has also contacted his mobile phone provider form the time and it's confirmed it had no record of any issues from the time. It also confirmed no new sims were issued.

The way in which the fraud was set up is also not consistent with the case of a sim swap. Mrs G appears to have taken a call somewhat out of the blue. It doesn't appear as though Mr G was an intended target at the time as he wasn't asked for directly. If a fraudster had enough information to order a replacement sim card, and had taken the necessary steps to do so, I'd expect them to know who to ask for when they called to put the scam into action. They'd have needed that information and more to get the sim card in the first place. Mr G wasn't asked for immediately though; the fraudster looks to have targeted Mrs G first.

A less technical method of diverting calls from a mobile phone is to manually set it up on the handset itself. That would require call forwarding to be set up on the phone and involves taking a number of steps to do so, including putting in a forwarding phone number. Mr G doesn't recall taking such steps.

Mr G's confirmation that he could still receive calls after the scam again suggests call forwarding wasn't set up. He wouldn't have received those calls without taking steps to deactivate the call forwarding.

A further consideration here is that call forwarding won't automatically forward on text messages in the same way it forwards calls. So even if call forwarding had been set up, Mr G would still have received the text message from the bank.

If a fraudster had been able to divert Mr G's calls in some way I'd expect him to have experienced problems in using his phone as a result. That doesn't seem to have been the case, based on what Mr G has told us.

I've seen Mr G's mobile phone bills from the time and I can see there's an outbound call from his mobile at 1:45pm, the time at which the scam is unfolding, to what appears to be a number known for scams. I only say it's known in as far as internet searches reveal it as being so. But there is an outbound call and it suggests the phone was switched on, at least at that time.

Mr G has said he didn't make that call but it's difficult to see how someone else would have been able to dial out from his number. It's possible the number was called form his mobile phone in order to check the legitimacy of the incoming contact number of the fraudster. I've no way to confirm the purpose of the call or what might have been discussed, if anything.

I can also see Mr G told the bank at the time, based on its notes, that he intended to contact his mobile phone provider to ask for records about any oncoming calls. Whilst on one hand

that suggests he was confident he didn't receive any calls it also raises the question of why he didn't say at the time that his phone would have been off. It may be that he did say that to the bank and it simply isn't in their notes. But I can only go off of the available records. And I find the other factors I've mentioned above to be more persuasive in determining the likelihood of who answered the security call.

All of this persuades me it's more likely than not that Mr G did receive the security call and the text message from the bank. I can't say it is definitely what happened. Mr G's version of events may be correct and someone else was able to somehow answer the call. But the evidence I have persuades me the call was completed as TSB say.

But that conclusion in of itself doesn't mean Mr G authorised the transactions.

Mr G had clearly been convinced by the fraudster when the security call was made. I can then understand why he might have been persuaded to take the call and follow the steps at the time.

Mr G had been convinced by the fraudster that his account was under attack and that he needed to act with urgency to protect himself and his money. But there was no call to the bank to question what had happened until a week after the transactions. This suggests to me that Mr G was most likely coached by the fraudster into believing that, despite what the text and call said, there was nothing amiss. Or, alternatively, he was distracted by the fraudster so that he didn't fully hear or understand the content of the call.

The content of the call itself is an important consideration in deciding whether Mr G authorised the payments or not. It's true to say the message given is clear and it does specifically state that a payment is about to made, if the correct code is given in response.

But I don't believe Mr G truly thought money was about to leave his account. I think it's more likely the fraudster convinced him he was protecting his account and that the code needed to be entered to protect his money, rather than to send it out of his account. That's reflected by him not contacting the bank for a week, as already mentioned, along with his version of events thereafter.

Mr G doesn't ever appear to have said that he understood money was being moved out of his account at the time. The most contemporaneous record of events we have are the bank's notes which confirm Mr G told the bank at the time that he acted to secure his accounts.

I've discussed the meaning of consent in respect of authorising a payment in this provisional decision already. And I go back to where I've said a payment services user who is unaware a payment is being made can't rightly be said to have given their consent to make a payment. I'm satisfied Mr G was unaware a payment was being made when he answered the security call. That means the payment that was made following the security call was unauthorised as Mr G didn't consent to it.

Once the first payment is made the fraudster proceeds to make a second payment, this time for £800, using the same payee details. As the payee is now set up and active there's no need for a further security call or any text messages. The payment can just be made online.

I've already explained how the fraudster is in control of Mr G's online banking at this point. It's the fraudster that is carrying out all of the actions for the second payment and Mr G is unaware of what's happening.

Mr G has no knowledge that the fraudster is making a second payment to the same payee. And so I don't believe it can be said Mr G authorised that payment either.

I'm satisfied that neither payment from Mr G's account was authorised. And so I need to go on to consider the next key question.

what is the impact of the CCA on the transactions?

A partial amount of the first transaction (£158.72) and the full amount of second transaction (£800) was the bank's money. That is to say it was money taken from an overdraft which is a form of credit facility.

Section 83 says a customer isn't liable for any transactions from a credit facility unless they were authorised by the customer or someone acting as their agent. And it applies in place of the PSRs in this instance.

Mr G neither authorised the transaction himself nor had someone acting as his agent. His divulging of security details, his granting of remote access to his computer or any other of his actions can't be fairly said to have established the fraudster as his agent. That isn't something Mr G understood to be happening and it's not something he consented to. And so TSB can't hold him liable for any loss of funds from the credit facility. There is no test of gross negligence that applies when payment is made from a credit facility and so I don't need to make a finding as to whether his actions were grossly negligent for the purpose of the second transaction or a portion of the first.

TSB appears to have been under the impression, at least for a time, that such provisions would only apply to an unarranged overdraft. But that's not true and the CCA makes no reference to that being the case.

TSB's terms and conditions are silent on section 62 of the PSRs where liability for the first £50 of any loss is covered. And so it isn't able to withhold that £50 from the refund.

That leaves the remaining £3,641.28 of Mr G's own money to be considered under the final key question.

did Mr G fail with gross negligence to comply with the terms and conditions of his account?

I've talked about what I think is most likely to have happened as the scam unfolded. And I'm carrying those findings through into my assessment of whether I think Mr G acted with gross negligence. That is to say, I believe it's more likely than not he did answer the security call himself. I won't go on to repeat my reasoning for believing that to be the case.

Mr G can't be said to have been grossly negligent solely on the basis that he gave away security information to a third party or that he answered a security call from the bank. I have to consider the circumstances in which that information was disclosed and what led Mr G to take the actions he did in order to reach a fair and reasonable outcome.

Mr G has been the victim of a sophisticated fraud. And the circumstances in which he fell victim include the fraudster having already convinced Mrs G that there was a genuine need for him to speak with a genuine representative of their telecoms provider.

Mrs G herself has said the fraudster already knew some details about her. They were able to discuss information about her broadband account. She still challenged the fraudster and that's what led to the email being sent to her. It was at this stage she was persuaded the call was genuine.

I think it's worth commenting here that I have seen the email sent to Mrs G and I can see how she and Mr G, or indeed a reasonable person in the same circumstances, would have thought it to be genuine. The email address looks like a genuine one for the telecoms provider the fraudster claimed to be calling from, as does the content. And it links through to the company's genuine website. There is another link within the email which prompts the download of teamviewer. I can see how, in the circumstances, that would appear normal. The fraudster said remote access was required and the apparently genuine email contained a link to download the appropriate software. So all seemed to be in order.

Mr G then takes over the call once the fraudster has had Mrs G log in to her own online banking. It seems likely – though it's important to remember I make no findings on this point – that the fraudster had been attempting to obtain funds from Mrs G's own accounts. This looks to have been unsuccessful. And so when the phone is passed to Mr G he's accepted Mrs G's belief – whether explicitly stated or not – that the call is genuine. I think a reasonable person in the same circumstances would act as Mr G did. An important point to note here then, is that the fraudster didn't have to convince Mr G of where they were calling from and why.

It's unclear whether Mr G allowed remote access to his own computer or whether he took over from Mrs G on her computer, with access already established. I've not been able to confirm the sequence of events. But whether access to the computer came as a result of Mrs G downloading the software or Mr G doing so himself doesn't appear to be particularly relevant to the outcome. I think it's enough to know that Mr G was aware that someone else was accessing his computer at the time he was logging on to his online banking.

Once remote access was established and Mr G logged into his online banking, the scam was able to unfold. The fraudster was able to set up a new payee. Following that, Mr G was then persuaded to respond to the security call which allowed the first payment to go through.

I don't believe though that, on balance, Mr G has been grossly negligent in falling for the tricks of the fraudster. In concluding this I need to address the initial log on and then the call.

I've already set out how both the courts and the FCA have interpreted gross negligence and how it is a higher bar than ordinary negligence. And so I've gone on to consider Mr G's actions in the particular circumstances. I must consider whether his actions fell so far below the standard of a reasonable person that it would be fair to say he'd failed with gross negligence to keep his security information safe or to comply with the terms and conditions of the account.

Gross negligence isn't an abstract concept and must be considered with regard to what was happening at the time. Mr G was the victim of a sophisticated scam involving what is termed 'phishing' as well as 'social engineering'. Both methods are used by fraudsters to lure people into a false sense of security and to believe they're talking to a genuine company. Here, a company Mr G was genuinely a customer of.

The illusion that's created is to make the victim act with urgency, the driving force behind that being the need to protect their account. I need to consider Mr G's actions with these factors in mind.

Mr G was convinced that his computer and bank account were the subject of multiple hacking attempts. The fraudster seems to have been able to obscure what was happening on screen and show lines of code which to Mr G, a layman in computer terms, looked convincingly like hacking attempts. That in turn created the fear that his bank account was under immediate threat. The fraudster assured Mr G they could help and so he acted quickly to accept the offer of assistance by logging into his online banking. In the moment and in a sense of worry I can see how someone would be persuaded to act in the same way.

In order for the scam to be successfully carried out from this point, the security call needed to be answered. And I've found it's most likely Mr G did answer that call. I also think it's most likely Mr G was somehow coached through that call by the fraudster. I can't say how that was achieved exactly as Mr G has maintained he didn't take the call. But I still believe it's most likely as it seems the spell cast by the fraudster would have otherwise been broken had Mr G had no prompt from them and listened to the call in detail.

This service has seen many cases involving similar social engineering scenarios. And from that experience I believe it's more likely than not one of two things happened with regard to the security call. The first possibility is the fraudster was able to convince Mr G that the call he'd receive was completely normal and was to do with protecting his account. In this situation the fraudster would likely have coached Mr G to believe that, despite the wording of the message, he should follow the instructions to ensure no money left his account. I note this is supported by the bank's early notes from when the fraud was reported, so seems quite likely.

The second possibility is that Mr G didn't actually listen to the message at all after answering the phone. It's quite possible the fraudster sufficiently distracted Mr G so that he didn't hear the message and then followed the fraudster's instruction to enter the required code into the handset.

Mr G was still convinced of his need to act at this stage. The bank's notes from Mr G's reporting of the fraud refer to him acting in order to secure his account. It would seem that he said words to that effect to the bank at the time. So it seems likely the fraudster said the call would be for the purpose of preventing fraud, rather than facilitating it.

Whichever of these two possibilities may be true I'm satisfied Mr G believed he was taking the necessary steps to secure his account. The wording of the security call doesn't alter my opinion there. And so I don't find that Mr G acted with gross negligence.

TSB has pointed to the various warnings it gives on its website and in other formats. But given the situation in which this scam unfolded, and the fact those warnings weren't presented to Mr G at the time, they don't alter my view of Mr G's actions.

Given the sophisticated nature of how the scam was set up and executed I don't think Mr G acted with gross negligence. His actions didn't fall far below those of how a reasonable person might act in the same circumstances. And so TSB should refund the remaining part of the first transfer not accounted for in my earlier findings.

my provisional decision

I've found that Mr G didn't authorise either of the transactions and he didn't, where applicable, act with gross negligence. And as such the complaint should be upheld.

My provisional decision is that TSB Bank plc should:

- refund £4,600 to Mr G's account;
- reconstruct the account as if the money had never left adjusting any fees, charges and interest accordingly;
- if Mr G's account would have been in a credit balance at any time following these adjustments TSB should pay the interest the account would have benefited from; *and*
- pay compensation of £300 to Mr G. This has been a very worrying time for him, not receiving a refund for a transaction he didn't authorise, after having been the victim of the scam.

If TSB considers that it's required by HM Revenue & Customs to withhold income tax from any interest award, it should tell Mr G how much it's taken off. It should also give Mr G a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

I'll consider any further information presented by either party before issuing my final decision. Any further submissions should reach me by 29 March 2019.

Ben Murray
ombudsman