complaint

Mr B complains that Metro Bank PLC won't refund three payments totalling £4,600 made from his account, which he says he didn't authorise.

background

I attach my provisional decision, which forms part of my final decision. In my provisional findings, I said I intended to uphold Mr B's complaint. Mr B contacted us to say he is willing to accept my provisional findings in settlement of his complaint. Metro Bank has also been in touch to say it also accepts the conclusions set out in my provisional decision.

my findings

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

As both parties agree with my previous findings, I see no reason to change my conclusions as set out in my provisional decision.

my final decision

So, for the reasons I've explained, I uphold Mr B's complaint against Metro Bank PLC.

putting things right

In putting things right for Mr B, I direct Metro Bank PLC to:

- refund the disputed transactions to Mr B's current account totalling £4,600;
- refund any fees or charges that Mr B may have incurred on his current account that directly resulted from the withdrawal of the disputed payments;
- pay interest on that amount at the account interest rate, from the date of the withdrawals to the date of settlement. If Metro Bank deducts tax from the interest element of this award, it should provide Mr B with the appropriate tax deduction certificate; and
- pay Mr B the sum of £750 in respect of the distress and inconvenience caused by Metro Bank's handling of the matter.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 14 March 2019.

Stephen Dickie
ombudsman

copy of my provisional decision

complaint

Mr B complains that Metro Bank PLC won't refund three payments totalling £4,600 made from his account, which he says he didn't authorise.

background

In September 2017 Mr B was a victim of a scam known as "*smishing*" (this is where a fraudster sends an SMS text message to a customer and it appears to come from their bank). 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.

At the time, Mr B held a current account with Metro Bank. He says that, on the morning of 28 September 2017, he was leaving his house on the way to a business meeting when he received a text message, which came up on his phone as being from 'Metro Bank'. He doesn't typically give out his mobile number, and thought it unlikely someone other than Metro Bank would know both his mobile number and that he banked with Metro Bank.

Mr B therefore assumed that the message had in fact been sent by Metro Bank. The message asked whether Mr B recognised a recent transaction for £699. It said if he did he should reply 'Y', and if not he should call a number. He says he didn't recognise the transaction so he called the number without delay.

When he rang the number shown on the text, Mr B says the call mirrored a normal call to Metro Bank. Mr B says he was given the same automated options as when he normally called Metro Bank. He says the 'hold music' used was the same as Metro Bank's, and that what he was told exactly matched the call scripts he was used to hearing when he spoke to Metro Bank. He says he was convinced he was speaking to a staff member at Metro Bank to resolve the problem with the transaction.

This was the reason he passed on his details to the female he was speaking with, who unfortunately turned out to be a fraudster. Mr B says he was asked three or four questions. He recalls this included his security number, two of the characters from his passcode and his mother's maiden name. Mr B says that the questions were the sort of questions he was used to answering when he called most banks, including Metro Bank. So, again, he says he did not suspect there was anything amiss.

Mr B says the person he was speaking to went on to identify three or four transactions he'd made over the past week. He recognised these and confirmed they were genuine. However, she then mentioned a payment for £699 which he didn't recognise. Mr B says she confirmed this was a fraudulent transaction and that she would stop it.

He recalls asking how the transaction could have happened. He says he was told there were sometimes security breaches, and was instructed to delete his mobile banking app and not reinstall it for 24 hours. He accepted this as a genuine request from his bank, and so he followed it. He then proceeded to his meeting.

It seems that whilst talking to Mr B, the fraudster accessed Mr B's online banking facility and through that his account. Metro Bank says that in order to access Mr B's account the fraudster would've needed his 12 digit customer number, 3 digits from his security number, and 3 characters from his password. When Mr B initially reported the fraud he recalled being asked for characters from his password and his security number.

Whilst in Mr B's online account, the fraudster set up the account details for a new payee. The bank says this generated a One Time Passcode (OTP) message to Mr B's mobile phone. Metro Bank says this message read:

"Your Metro Bank one-time passcode to setup a new payee is XXXXXXXX. If you did not setup a new payee then please call us on XXXXXXXX".

Metro Bank has provided records showing this was sent to Mr B's usual mobile phone number. However, Mr B says he doesn't recall receiving that message.

Shortly afterwards, three payments totalling £4,600 were transferred out of Mr B's account to the newly created payee.

It was only when Mr B says he attempted to withdraw cash at an ATM some hours later, that he realised his account balance had been taken and that he had been scammed. He says he called Metro Bank straightaway to report what had happened.

Below is a list of these events:

Between 10:30-11:00	Mr B received a text message that looked as though had come from Metro Bank.
11:15-11:56	Mr B called the number given in the text message and gave over security information during the call
11:56	The fraudster made a failed attempt to login to Mr B's online banking
11:58	The fraudster successfully logged on to Mr B's online banking
12:03	Metro Bank sends Mr B an OTP by text message
12:05	New payee created
12:05	Payment of £100 sent to the new payee (the payee created at 12:05)
12:07	Payment of £1000 sent to same new payee
13:07	Payment of £3000 sent to same new payee
15:00	Mr B logs in and views the account
15:02	Mr B calls Metro Bank to say he believes he's been scammed and that someone has cleared his bank account

Mr B reported the scam at 15:02 on 28 September 2017. This was just under two hours after the last of the transfers had been sent. Metro Bank contacted the recipient bank at 15:47 that day.

The recipient bank responded at 17:11, confirming the transferred money had all been withdrawn or transferred out, and that no money remained in the receiving account.

my provisional findings

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's 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.

I've summarised below what I consider to be the relevant regulations and account terms, and I've taken them into account when deciding this complaint.

relevant considerations

Metro Bank, as an FCA regulated firm, provided a current 'deposit' account. As such the FCA's overarching Principles for Businesses apply including the requirement to pay due regard to a customer's interests and treat them fairly (Principle 6).

The transfers from Mr B's account were made in September 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 (PSR 2009). I think these sections of PSR 2009 are of particular relevance here:

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 transactions

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

Regulation 55 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 PSR 2009 implements) says "*In the absence of such consent, a payment transaction shall be considered to be unauthorised*." But neither PSR 2009 nor the FCA's 2013 guidance on PSR 2009 provide a definition of "consent".

I therefore think it's fair, when considering whether consent was given, to 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 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."

Negligence is often referred to as a failure to exercise reasonable care. But as I have described above, gross negligence suggests a lack of care that goes significantly beyond ordinary negligence. So I have to consider whether what Mr B did fell so far below the standard expected of a reasonable person that it would be fair to say he failed with gross negligence to keep his personalised security details safe or to comply with the Terms and Conditions of the account.

the Terms & Conditions of Mr B's account

Metro Bank has provided a copy of the terms and conditions that applied at the time the transfers were made from Mr B's current account. In its submissions, Metro Bank has highlighted certain sections. I also consider section eight to be relevant to my consideration of this case. It outlines:

"8.1 Transactions you didn't authorise
We will be responsible for any payment transaction that you did not authorise, unless:

- *you have acted fraudulently;*
- *you allowed another person to use your card, PIN or other security details who is not authorised by you…;*
- *you suspect your chequebook or cards have been stolen or lost (or intercepted before being delivered to you) and you deliberately or with gross negligence have not told us;*
- *you have revealed to someone else, or written down, your PIN number or other security details used for online, mobile and telephone banking;*
- *you didn't tell us that your mobile phone which is registered for SMS updates or mobile banking has been stolen;*
- *you allow someone else to use your mobile phone or personal computer;*
- *you change your mobile phone number, email address or other details which we use to contact you and do not update us;*
- *(in the case of a cheque) you failed to take reasonable care when writing the cheque; or*
- *you have entered the incorrect details when making a payment.*

We will issue you with an immediate refund if you tell us that you did not authorise a payment transaction, unless the facts suggest that we may not be responsible for it and that it is appropriate for us to investigate the transaction further. We will investigate the transaction and decide as quickly as possible whether we are or may be responsible. You should tell us as soon as you notice any suspicious or unauthorised activity on your account in line with the section on 'Telling us about problems early'…

If we issue you with a refund, we will pay you the amount of the unauthorised transaction and any resulting interest and charges applied to your account. If we have investigated the transaction, we will make sure that you do not suffer any loss because of the delay in reaching our decision.

If we then prove that we are not in fact responsible for an unauthorised transaction, we will explain to you how we have reached this decision and we may take from your account the amount of any refund or other payment we have made to you."

key questions

In my view, the above relevant considerations mean that if the transactions were unauthorised, it would be fair and reasonable for Metro Bank to refund the amount stolen from Mr B, unless Mr B with intent or gross negligence, failed to comply with the Terms and Conditions of the account and the obligations set out in Regulation 57.

Metro Bank says in its final response to Mr B's complaint that:

> *"the monies were paid away in reliance of the correct security information being provided, and in such situations we are unable to provide a refund due to the circumstances, as it is reasonable for us to assume that the disputed transaction was either authorised by you or that you have not taken adequate care of your security details, contrary to our terms and conditions (5.2). As such, we are not obliged to provide a refund on this occasion."*

I therefore think there are two key questions relevant to my consideration about what is fair and reasonable in the circumstances:

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

2. If they weren't, can Metro Bank demonstrate that Mr B failed with intent or gross negligence either to comply with the Terms and Conditions of his account or to keep his personalised security details safe?

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 B?

On the balance of evidence, I'm not persuaded that Mr B authorised these transactions from his current account. I'll explain why.

I don't know exactly what was discussed between Mr B and the fraudster, but it appears as though he gave the fraudster enough information for them to gain access to his online banking. And this was all in the context of protecting his account and trying to stop a payment rather than authorise one.

Mr B doesn't accept he received an OTP. Metro Bank says it sent the OTP in a text message to Mr B's mobile number. It's provided records showing the time that text was sent, the wording of the message and the number to which it was sent, amongst other things. But I haven't seen anything confirming the specific device to which the OTP was sent.

Mr B suggests that the mobile number linked to his account may have been changed by the fraudster. He says perhaps this caused the text message to be diverted to the fraudster. Having reviewed the records provided by Metro Bank, I don't see any evidence to suggest that is what happened here. The number to which the disputed message was sent is the same as that which had been used on previous occasions, seemingly without issue.

Mr B doesn't report having had any issues with his mobile phone at the time. And the fraud relied on him receiving the fraudster's initial text message. So I think it's unlikely the fraudster directly intercepted the message sent to his mobile phone number. But I will consider any further evidence on this point from Mr B or Metro Bank in response to this decision.

There is limited information for me to rely on here, and so I need to decide what I think is most likely to have happened given the available evidence.

I've listened to the calls between Mr B and Metro Bank, in particular the first call that Mr B makes to report the fraud. This seems to me the most reliable recollection of events by Mr B; it's just happened shortly beforehand. So I think it's reasonable to give weight to what he said during that call about how the scam unfolded.

On balance, I think it most likely that the OTP was received by Mr B's phone. Mr B describes the situation surrounding the call to the fraudster, and the level of trust built through what seems to have been the considerable sophistication of the scam. I think in those circumstances it would have been understandable that Mr B might have, believing he was speaking with his bank, given over the number in a message he'd been sent. That message after all would likely have been received in the same way he'd received the message that had prompted his call in the first place.

Regardless, it's clear the fraudster used the OTP code to set up at least one new payee on the account. The fraudster then transferred money out of Mr B's bank account to that new payee, a payee unknown to him.

Given the information Metro Bank has provided showing a log-in from a different IP address and knowing that Mr B provided information that enabled a fraudster to log into his account, I think it most likely that it was the fraudster rather than Mr B who input the OTP into Mr B's online banking.

Later on that day Mr B found he was unable to withdraw any cash from an ATM. He says he then checked his balance and noticed £4,600 was missing. At that point, he called Metro Bank to report the scam.

I've I listened to that call and thought about what had happened prior to it being made. Based on what's been made available to me, I don't think Mr B had been aware that a payment was being made from his account when he was speaking to the fraudster or immediately afterwards. He says he fully believed he was acting to prevent a fraudulent transaction, not to make a transaction. What Mr B says on the call is persuasive evidence on this point. And so, on balance, I don't think Mr B consented to or authorised a transaction to be made from his account.

So, my starting point here is that it wouldn't be fair and reasonable for Mr B to be held liable for the transactions — which I think it's more likely than not were unauthorised — unless he has failed with intent or gross negligence to comply with the terms and conditions of the relationship with Metro Bank and the obligations set out in the PSR 2009.

did Mr B fail with gross negligence either to comply with the Terms and Conditions of the account, or to keep his personalised security details safe?

It is not enough to say Mr B was grossly negligent simply because he shared security details for the account. Careful consideration needs to be given to the circumstances under which those details were shared.

Mr B was tricked by a fraudster into giving over some account security information. I think Mr B was also then tricked into handing over an OTP code, which allowed a new payee to be created. However, on the balance of evidence, I don't think it would be fair and reasonable to say that, in falling for these tricks and in failing to keep his security details safe, Mr B was grossly negligent. I'll explain why.

As I set out earlier, negligence is often referred to as a failure to exercise reasonable care. I think it is fair to say that gross negligence involves a degree of negligence that is higher than ordinary negligence. That is consistent with what has been held by the courts in a commercial contract context (as mentioned, Mance J held that ""*Gross" negligence is clearly intended to represent something more fundamental than failure to exercise proper skill and/or care constituting negligence"),* and the FCA's guidance, which says that gross negligence is a *"higher standard than the standard of negligence under common law".*

I've thought carefully about the actions Mr B took in the circumstances here, and whether what he did, fell so far below the standard of a reasonable person that it would be fair to say he failed with gross negligence to keep his personalised security details safe or to comply with the Terms and Conditions of the account.

Gross negligence isn't an abstract concept. It's important to take into account all the circumstances when considering whether an individual's actions amount to gross negligence. The scam here involved *"smishing*" and "*social engineering*", where the fraudsters use a range of sophisticated techniques to trick, deceive and manipulate their victims into giving out confidential information. Here Mr B was made to believe he was talking to his own bank and needing to act quickly to protect his bank account, which was at that very time being used for fraudulent spending. Therefore, I've thought about Mr B's actions in that context, and considered his overall actions.

Mr B has described the text message he received in detail, and he's explained why at the time he thought it was genuine. I don't doubt his account of this or of the subsequent call where he was told of genuine transactions and a fake fraudulent transaction. This is a sophisticated method used by fraudsters to trick their victims into a sense of security. It creates the sense that their victim is in a safe environment, that they are dealing with their genuine bank, and that they need to act quickly to protect their account. Mr B's detailed recollections of the ways in which the call exactly mirrored any other call he would expect to have had with Metro Bank supports this view. So I can understand why it wouldn't, reasonably, have raised any obvious suspicion from Mr B – or any reasonable person in these circumstances.

I do not think, at the time, Mr B thought anything other than that the actions he was taking were to prevent a fraudulent payment leaving his account and to secure his bank account. Rather than appreciating the risk he was taking by following the fraudster's instructions but disregarding or being indifferent to it, he was under the opposite impression that if he didn't follow those instructions he was at risk of losing money.

Mr B doesn't recall receiving the OTP code, although I think it likely the code was sent to his phone. In this case, it seems likely that the fraudsters convinced him that the code was needed in the process of protecting his money and the various stages the bank needed to go through to do that. And I wouldn't expect Mr B to know what Metro Bank's processes are for stopping a payment or to necessarily question what he was being asked to do — because he genuinely believed he was working with his bank to protect his account. He reasonably felt worried about the security of his bank account, and felt a corresponding pressure to act. In similar circumstances, I think a reasonable person would've acted in the same way that Mr B did here. Indeed this was the conclusion voiced by the Metro Bank call handler when Mr B called in to report the fraud, the call handler stating: "You've done what any person would have done, so it's not your fault at all in this situation".

So on balance I don't think anything happened to break the fraudster's spell over Mr B. And 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.

warnings

Metro Bank refers to a number of things it has done to raise the general awareness of fraud risk amongst its customers, including specific warnings, which it says Mr B would have had to acknowledge to log on to his online banking.

But even if Mr B engaged with these things it doesn't follow that he was grossly negligent for falling victim to fraud thereafter. Nor would it necessarily be fair to say Mr B was grossly negligent if he did not engage with these things and then fell victim to fraud. I am required to consider whether what Mr B did fell so far below the standard of a reasonable person that it would be fair to say he failed with gross negligence to keep his personalised security details safe or to comply with the terms and conditions of his account.

To be clear, I'm not saying that fraud warnings by a bank aren't ever relevant at all, or couldn't, potentially, make a difference in a specific example of fraud. Nor am I condoning an individual who chooses consciously to disregard such warnings. But, by way of balance to this point, I also think it's right to appreciate and understand that, in a busy world, such messages are not always read by consumers and even if read may not, reasonably, be in a consumer's mind when faced with a sophisticated real time confidence trick of this nature sometime later. It is encouraging to hear that banks are increasingly looking at ways to provide more 'real time' and impactful fraud specific warnings with this in mind.

On the facts of this particular case, I don't believe Mr B's failure to read or heed the warnings in question is enough, on the balance of evidence, for Metro Bank to demonstrate gross negligence occurred here.

other considerations

Mr B has detailed the impact this event had on him. He's explained the toll this took on his health, and business affairs. While the bulk of this can be attributed to the actions of the fraudsters involved, I have thought about the impact Metro Bank's handling of the issue had on Mr B.

Mr B has explained the specific impact Metro Bank's response to the scam had on him, and how his individual circumstances meant this affected him more strongly. I am persuaded that the initial reassurances Metro Bank gave him, followed by the bank's eventual response that he was to blame, led him to suffer significant distress and inconvenience.

Taking account of everything that happened I consider that Metro Bank should pay Mr B compensation for the distress and inconvenience it caused him here.

putting things right

For the reasons given, I do not think it was fair and reasonable for Metro Bank not to refund the amount stolen from Mr B's current account.

I think Metro Bank should:

- refund Mr B's current account with £4,600;
- refund any fees or charges that Mr B may have incurred on his current account that directly resulted from the withdrawal of the disputed payments;
- pay interest on that amount at the account interest rate, from the date of the withdrawals to the date of settlement. If Metro Bank deducts tax from the interest element of this award, it should provide Mr B with the appropriate tax deduction certificate; and
- pay Mr B the sum of £750 in respect of the distress and inconvenience caused by Metro Bank's handling of the matter.

In considering these provisional conclusions about what would be fair compensation, I've assumed that the money taken from Mr B's current account would've remained in that account if this fraud hadn't happened. But I would invite the parties to make further representations about this in response if they have a different view.

I've noted that regulation 62 of the PSRs 2009 suggests that Mr B can be liable up to a maximum of £50 for losses incurred as a result of unauthorised payment transactions. But the terms and conditions that applied to Mr B's account don't make any provision for Metro Bank to withhold up to £50. As Metro Bank hasn't reserved this right and its terms indicate that it will pay the amount of an unauthorised transaction if it does decide to refund a transaction, I'm currently of the opinion that it would be fair and reasonable for it to refund the full amount of these unauthorised transfers.

provisional decision

For the reasons given, my provisional decision is to uphold Mr B's complaint. My current view is that Metro Bank PLC should calculate and pay compensation as set out above.

I'll wait two weeks for both parties to provide any further comments or evidence before reviewing the matter again.

Stephen Dickie
ombudsman