complaint

Miss B complains that Metro Bank PLC refuse to refund transactions totalling £5,440 which she says were taken from her account, without her knowledge, by a fraudster. Metro Bank has recovered £3,701.26 from the recipient's bank account, and returned this to Miss B. Miss B wants the remaining £1738.74 refunded. She's also unhappy that Metro Bank's account monitoring systems didn't spot and prevent the transfers.

background

Miss B had an account with Metro Bank (Metro) since 2015. On 21 August 2017 she received a text message closely followed by a phone call, from someone saying they were from Metro's fraud department. It's not in dispute that Miss B was the victim of a scam here, so I'll use the term 'fraudster' throughout to refer to the third party involved. The text message read:

"*Miss B, You've successfully added a new payee. If you did not setup a new payee then please call us on 03** *** ***88*."

Miss B says that when he called, the fraudster referred to the text message he'd sent and asked her if she'd set up a new payee. She confirmed that she hadn't. She was told that the payee would be cancelled and she'd be sent a new customer number to keep her account secure.

Miss B says that the fraudster asked her a lot of questions during the call. She also received a genuine text from Metro while the fraudster was on the phone. This text came through in the same message thread as the fraudster's text, and contained a one-time passcode (OTP). It 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 03** ** ** *00*."

Miss B says she doesn't think she gave this OTP to the fraudster. Miss B's told us the fraudster was very convincing and, "*All the while* [she] *was not aware that this was a fake call from a fraudster*".

On 19 September 2017 Miss B received another text message, which looked like it had come from Metro but wasn't. It read:

"*We have identified some unusual activity on your online banking. Log in via this secure link XXXX*"

Instead of clicking on the link Miss B called Metro using the telephone number on the back of her debit card. She explained that she'd not had access to online banking since what happened on 21 August 2017, because she'd been waiting for a new customer number. The call handler explained that the text message Miss B had received on 19 September was not genuine. He then offered to check Miss B's transaction history. When he read out her balance, it became clear that it was much lower than Miss B was expecting. The call handler confirmed that £4,900 had been transferred out of the account on 21 August. Miss B said she hadn't made the transaction. Nor had she made another transaction for £540 on that day. The fraudster who'd called her on 21 August had managed to login to Miss B's online banking, set up a new payee and make these transfers.

Miss B explained that she'd received a text message on 21 August 2017 asking her if she'd set up a new payee, followed by a call, from a "private number", from someone saying they were from Metro. She said the fraudster "asked questions", told her they would stop the payee, that they were "blocking everything", and that they would send her a new customer number. She explained that she didn't know her customer number "by heart" and didn't have it with her when the fraudster called. The call handler told Miss B the case would be referred to the fraud team to investigate.

The following table lists the events relevant to this case. It's been compiled using Metro's internet banking audit, its OTP audit, and screenshots provided by Miss B of the text messages she received.

Date and time	**What happened?**
20/08/2017 21:33	Failed login from IP address 2**.***.***.134
20/08/2017 21:33	Account logged into from 2**.***.***.134 and viewed.
21/08/2017 16:15	Account logged into from 2**.***.***.230
21/08/2017 16:19	Miss B received a text message from the fraudster which read: *Miss B, you've successfully added a new payee. If you did not set up a new payee, then please call us on 03** *** **88*
21/08/2017 time uncertain	Miss B answered a phone call from the fraudster.
21/08/2017 16:24	Payee created
21/08/2017 16:24	Miss B received a genuine text message from Metro which 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 03** ** ** *00*.
21/08/2017 16:27	Payee created
21/08/2017 16:27	£4,900 transferred to newly created payee
21/08/2017 16:28	£500 moved from a joint account Miss B held with her daughter to Miss B's sole account.
21/08/2017 16:28	£540 transferred to newly created payee
21/08/2017 16:29	Account logged out
21/08/2017 16:30	3 failed logins from 2**.***.***.230
21/08/17 time uncertain	Miss B received a text message from the fraudster which

	said: *Thank you for completing the restoration process. Your online account is now under safeguard and you will be issued with a new secure link XXXX to avoid account suspension.*
26/08/2017 15:22	Failed login from 2**.***.***.113
30/08/2017 00:17	Failed login from 2**.***.***.117
08/09/2017 11:52	Failed login from 2**.***.***.81
19/09/2017 16:33	Miss B received a text message from a fraudster which read: *We have identified some unusual activity on your online banking. Log in via the secure link XXXX to avoid account suspension*.
19/09/2017 approx. 17:00	Miss B called Metro and discovered that her balance was much lower than she expected.

Following its investigation, Metro refused to refund Miss B. In her complaint about that decision Miss B said she had been "*deceived into giving some of* [her] *details out to someone who turned out to be a fraudster*". She said the caller "*behaved as though they were calling from Metro Bank*", and any information she gave was because she thought the caller was taking her through a "*security verification process*". She also said:

"*One thing the caller didn't do was to ask for my customer number or my one-time passcode*."

Miss B said that she thought Metro should have spotted the payments and queried them because the activity was so unusual for her account. She said, "*I have never ever made a payment using online banking or made a transfer to anyone before, and certainly I have never before completed a transaction for such a huge amount on my account*".

In response to Miss B's complaint, Metro said it had declined her claim because she provided the fraudster with the OTP sent to her phone. It also said:

- The texts Miss B received on 21 August 2017 about unusual account activity were not sent by Metro.
- The text Miss B received on 21 August 2017 containing an 8 digit OTP was a genuine Metro text and was sent to the mobile number Miss B registered with Metro in January 2015.
- Without the OTP being entered online a new payee could not have been set up.
- In order to access online banking the fraudster would have needed Miss B's customer number (a number given to Miss B when she opened the account), 3 digits from her security number (a number she created when she registered for online banking), her password (a password she created when she registered for online banking), and 4 digits from her debit card number.
- It lets customers know through various channels that it will "never ask [customers] to disclose in full any secure information".

What Metro told us

In response to Miss B's complaint to us, Metro made a detailed 5 page submission. It said:

- Miss B revealed her security details to someone calling from a private number;
- It wouldn't refund her because she acted '*negligently*';
- The transactions were completed online using Miss B's 12 digit customer number;
- It's evident that the fraudster had all her online banking security information, which is personal to each customer, but there is no explanation as to how Miss B's online security information was known to the fraudster;
- Miss B did not contact Metro until 19 September when the fraud was realised;
- There is no indication of a SIM swap or anything concerning related to Miss B's mobile phone – "As a result it is difficult to see how the fraudster was able to obtain the OTP unless Miss B had provided this";
- There is no explanation for how the fraudster was able to obtain all of Miss B's online security information along with the OTP sent to her registered mobile number "*unless she was negligent with this information*".

Our investigator didn't uphold Miss B's complaint. He said he couldn't hold Metro responsible for what had happened because it hadn't done anything wrong. He thought it most likely Miss B had shared the OTP with the fraudster and by doing so had inadvertently helped the fraudster get round Metro's security.

Miss B didn't agree. She said she didn't give the fraudster her customer number or a "*passcode*". And she didn't have any suspicion that "*something was going on*" when she was speaking to the fraudster.

Miss B's complaint was passed to me. I came to a different conclusion to the investigator, so I issued a provisional decision on 22 January 2019 setting out my thoughts.

In that decision I acknowledged that when considering what's 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. I remain of the view that these considerations are the relevant ones. I set them out below.

relevant considerations

Metro is a Financial Conduct Authority (FCA) regulated firm, and was carrying out regulated activities. As such the FCA's overarching Principles for Businesses apply including the requirement to pay due regard to a customer's interest and treat them fairly (Principle 6).

The transactions from Miss B's account were made in August 2017. So the relevant legislation is that set out in the Payment Services Regulations 2009 (PSR 2009)[1]. I think the following sections of PSR 2009 are of particular relevance here:

"Consent and withdrawal of consent

[1] The Payment Services Regulations 2009 were replaced in January 2018, which resulted in some regulations now carrying different numbers. All references in this decision to the Payment Services Regulations mean the 2009 regulations.

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

Regulation 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 PSR 2009 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."* The FCA's 2013 guidance on the PSR 2009 also said nothing further about what consent means.

So I 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're 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 Miss B's actions fell so far below the standard of a reasonable person that it would be fair to say she failed with gross negligence to keep her personalised security details safe or to comply with the terms and conditions of the account.

the terms and conditions of Miss B's account

Metro's terms and conditions ('Our service relationship with personal customers' – 2016) contain the following sections of relevance to this complaint.

5.2 Keeping your security information safe
You will be responsible for any instructions given by you, or anyone authorised to act on your behalf, from the time that you successfully pass through security to the time that you leave the relevant service. It is your responsibility to keep details of your cards and security details, including PINs, security numbers, access codes or passwords, safe and to make sure they cannot be used by anyone else or for fraudulent purposes. For example:

• you must not reveal your security details to any other person; …
• you must not respond to an email asking for your security details, even if it looks like the email is from us (we will never send you an email like this so you should report this to us at phishing@metrobank.plc.uk); …

5.4 Internet banking
Protecting you when you are using internet banking is our priority …

• We will ask you to confirm your identity using our current security procedures. We will never ask you for more than three digits of your password …
• We use two types of authentication for setting up any new payees. If you receive a code on your mobile and you did not set up a new payee, do not enter the code into internet banking and contact us immediately …

• You should never provide your internet banking details to anyone else …
• After initial registration to our internet banking service, we will never contact you asking for you to reveal or update your security details. If you receive a request like this, even if it appears to be from us, it is likely to be fraudulent and you must not supply your security details under any circumstances. You must report any requests like this to us immediately.

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 have revealed to someone else, or written down, your PIN number or other security details used for online, mobile and telephone banking; …

8.4 Claiming back a loss from us
If you suffer a loss because of something we have done or failed to do, you will usually be entitled to claim back that loss from us. However, there are some exceptions where you will not be able to claim from us and they are as follows …

2. Loss where you have acted fraudulently or negligently.

my provisional decision

Having set out the relevant considerations in my provisional decision I made the following findings:

> *I think the above relevant considerations mean that, if the transactions Miss B disputes were unauthorised, it would be fair and reasonable for Metro to refund the full amount taken, unless, with intent or gross negligence, Miss B failed to comply with the terms and conditions of the account.*
>
> *I think there are some key questions that are relevant to my consideration about what is fair and reasonable in the circumstances:*
>
> 1. *Were the disputed transactions authorised by Miss B? and;*
> 2. *If they weren't, can Metro demonstrate that Miss B acted with gross negligence – particularly taking into account the terms and conditions of the relationship with Metro and the obligations set out in Regulation 57 of the PSR 2009?*
>
> *were the disputed transactions authorised by Miss B?*
>
> *Metro accepts that the payments in dispute left Miss B's account without her authority. But in the interests of completeness, I'll briefly set out why I also think the payments weren't authorised.*
>
> *As I've said above, the payer must have consented to a payment transaction taking place, before the bank is entitled to debit the account (PSR 55). 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. An account holder who is unaware a payment is being made, can't rightly be said to have given their consent to make a payment.*
>
> *There is no evidence that suggests Miss B knew a payment was being made from her account on 21 August 2017. On the contrary, Miss B believed that the fraudster was helping her stop a new payee that she hadn't set up, and secure her account from fraudulent payments.*
>
> *So my starting point is that I don't think Miss B should be held liable for the transactions unless it can be said that she failed with intent or gross negligence to*

comply with the terms and conditions of the account, and the obligations set out in the PSR 2009.

Can Metro demonstrate that Miss B acted with gross negligence?

The principal obligation relevant to this case is Miss B's obligation to take all reasonable steps to keep safe the "security features" of the account. The account terms and conditions explain what this means in practice. I think Miss B was under an obligation not to reveal her security details, including internet banking details and OTPs, to any other person.

There's no suggestion from Metro that Miss B has acted fraudulently or that she intentionally failed to comply with the terms and conditions of the account or with the other relevant obligations set out in regulation 57 of the PSR 2009. The reason why Metro declined to refund Miss B is because it says she acted "negligently" by sharing online security information and an OTP with the fraudster.

I note that term 8.4 states that the consumer is not able to claim back a loss where they have acted "negligently". But taking into account the PSR 2009, as noted above, I consider that the test ought to be whether the consumer acted with "gross negligence".

To begin with, I acknowledge that it's difficult to establish exactly what happened during Miss B's conversation with the fraudster on 21 August 2017. This is partly due to the time that passed between the call and the discovery of the fraud (almost a month), and also because Metro doesn't seem to have asked her during its investigation to describe what happened in any detail. This is unfortunate because if Metro had taken the opportunity to ask more about what the fraudster said to Miss B, and what passed between them, when the fraud was first discovered, I think it's possible Miss B would have been able to recall more, and a clearer picture about what happened might have emerged. Without that, I've had to decide what, on balance, I think is most likely to have happened.

I think it's possible the fraudster already had Miss B's login information – I'll return to why I think that later - or that, during the call, Miss B shared with the fraudster at least part of the security information needed to login to her online banking. I also think, despite her recollections, it's more likely than not Miss B shared with the fraudster the OTP that she received by text message from Metro while the fraudster was on the phone.

I understand that Miss B only recalls sharing information as part of what she thought was a "security verification process". And she has consistently said she doesn't think she shared the OTP. But there is simply no other explanation for how the fraudster got the OTP he needed to create a new payee. That OTP was prompted by the fraudster's online activity (creating a new payee), and sent to and received by Miss B's mobile phone. And I think it most likely she was convinced by the fraudster that sharing the OTP with him was necessary to identify her, or stop the fictitious fraudulent new payee and secure her account.

Given what I think Miss B most likely did, I think it would be fair to say that she failed to comply with the terms and conditions of her account. But simply failing to comply with the terms and conditions of the account does not make Miss B liable for the

unauthorised transactions. To be liable, Miss B would need to have failed in this way with gross negligence. And on the evidence I currently have before me, I don't think she did fail with gross negligence. I'll explain why.

It is widely accepted that scams such as the one experienced by Miss B are very sophisticated. And it's likely the fraudster used a range of persuasive techniques to trick, deceive and manipulate Miss B into doing what she did (this is called "social engineering"). The fraudster set up the scam by first 'spoofing' Metro's phone number and sending Miss B a text message suggesting there had been unauthorised activity (the setting up of a new payee) on her account. This text was quickly followed up by a phone call. I think it's likely that during the call the fraudster anticipated the OTP text message and made it part of the story he was weaving. So when a genuine text from Metro came through, joining the thread with the fraudster's previous text message from "Metro Bank", I don't think Miss B had any reason to think that the fraudster's text message wasn't genuine, or that the person she was speaking with wasn't from Metro.

She's told us that she had no suspicion she wasn't speaking with Metro staff. What the fraudster said and did would've been designed to closely replicate a genuine Metro call. I think that the convincing nature of the fraudster's call on 21 August 2017 explains why the fraud was only discovered by chance a month later, on 19 September. This speaks to the fact that Miss B trusted who she was talking to, and believed by the end of the call that her account was "under safeguard". I think many people in Miss B's position would have been similarly convinced they were speaking to a Metro member of staff, particularly because the text messages referred to by the fraudster appeared to, or did, come from Metro.

In these circumstances I don't think Miss B acted unreasonably by responding to the fraudster's requests for information. I think it possible the fraudster simulated a "security verification process" to gather what he needed for online login (although, as I've said, I think it's also possible the fraudster already had Miss B's login information). I think the fraudster also asked her for the OTP. In short, I think the fraudster was convincing and tricked Miss B into sharing these security details. And I don't think Miss B's actions fell so far below what a reasonable person would do in these circumstances as to amount to gross negligence.

I've said it's possible that the fraudster already had Miss B's login information. I say this because it seems unlikely Miss B gave the fraudster her 12 digit customer number during the call on 21 August 2017. She said at the point the fraud was discovered, that this is not something she knows "by heart", and the fact that she couldn't give it to the fraudster seems to have prompted him to say that Miss B would be sent a new one. It also looks likely from the online banking audit that someone logged into Miss B's account from an IP address similar to the one used by the fraudster the evening before the fraud, and that someone logged into the account shortly before the text message and follow up call from the fraudster. This suggests that the fraudster had all that was needed to login and only called Miss B so that he could trick her into divulging the OTP to set up a payee.

If the fraudster did already have Miss B's login details, where he obtained this information is something that I cannot know with any certainty. There are a number of possibilities, the most likely being that, at some point before the 21 August 2017 Miss B's details were 'phished' from her. Fraudsters 'phish' sensitive details by

posing as a trusted entity and convincing consumers to enter their details into fake websites, or respond to fake emails or texts. We know that this happens, and I have seen examples of phishing websites that look strikingly similar to the Metro website. Miss B hasn't told us about any incidents likely to be the point of compromise for her information. But if she did respond to a phishing attempt, I don't think that automatically amounts to gross negligence on Miss B's part. Phishing attempts can be so convincing that the reasonable consumer would not have any appreciation they were dealing with a fake.

Metro has drawn my attention to the security warnings it displays on its website. It's highlighted the warning it gives about 'Passcodes and alerts'. This reads:

"To keep you safe we'll send a unique code to the mobile you've registered with us:

- *To confirm when you set up a new payee using internet banking*
- *For setting up your security information*

We'll never ask for this code at any other time and you should never share it with us or anyone else if it's not for the reasons above …"

From what I understand of the screenshots Metro has provided, to read this warning a consumer would need to go to the Metro website, click on 'Personal', click on 'Ways to bank', click on 'Banking securely', and scroll down or expand the information under the 'Passcodes and alerts' tab. It's not a warning that a consumer would see regularly or at the point of login, and it's not a warning that Miss B would have seen when she was on the phone to the fraudster.

The other warning Metro has highlighted is the 'Communications' warning which includes information about the "sneaky ways" fraudsters steal personal information and says:

*"Don't respond to suspicious calls, texts or emails. If you think something's gone wrong, come in store and tell us or call us on 03** ** ** *00 … If you get a suspicious phone call, make sure the line is clear before you call us."*

I appreciate that increasing public awareness of fraud is a big challenge for businesses. And it's good practice to display warnings about scams, and undertake other awareness raising initiatives, with consumer protection in mind. Increased levels of consumer awareness may, in some cases, help to prevent frauds like this from succeeding. And it's reasonable for Metro to expect that account holders, including Miss B, will engage with its efforts to raise awareness. But Miss B didn't have any reason to think the call she received on 21 August 2017 was suspicious because of the accompanying 'spoofed' and genuine texts. And not remembering the warning about OTPs, which she may or may not have read in the past, when she was under the influence of a sophisticated scam does not, in my view, mean that Miss B acted with gross negligence.

Metro Bank's account monitoring

Miss B has also complained that Metro Bank's account monitoring systems didn't spot and prevent the transfers. She's said it should have because she wasn't in the habit of making payments using online banking, and hadn't before transferred such a

*large sum of money. Having looked back over the online audit I can see that Miss B did make the odd online transfer – on 16 January 2017 she sent £300 to an account ending **011, and on 28 March 2017 she sent £1,000 to an account in her own name ending **441 – so I don't think an online transfer in and of itself should have triggered any extra checks by Metro.*

I also don't think there was anything about the way Miss B's account was logged in to on 21 August 2017 that should've alerted Metro to what was going on; the correct login details were used and the OTP sent to Miss B's registered mobile was entered correctly. It might well be then that there was nothing to make Metro suspicious about this payment. But as I already think this complaint should be upheld for the reasons set out above, I don't think I need to make a finding on this point.

responses to my provisional findings

In response to my provisional findings both parties accepted my decision. And Metro Bank agreed to compensate Miss B in accordance with my findings.

my findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. I remain of the view that this complaint should be upheld for the reasons set out in my provisional decision, which I have reproduced above, and which now form part of my final decision. In short, I don't think it would be fair and reasonable to say that Miss B authorised the transactions. And I don't think, in all the circumstances, that she failed with intent or gross negligence to comply with her obligations as a payment service user.

fair compensation

For the reasons given, I don't think it was fair or reasonable for Metro Bank to refuse to refund to Miss B the amount stolen from her account. To fairly compensate Miss B, I direct Metro Bank PLC to:

1. Credit Miss B's account with £1738.74;

2. refund any fees or charges that Miss B may have incurred on her account that directly resulted from the withdrawal of the disputed payments;

3. pay interest on the amount at 1. at the rate the money would have attracted if it had not been withdrawn, from the date of the withdrawals to the date of the settlement.

If Metro deducts tax from the interest element of this award, it should provide Miss B with the appropriate tax deduction certificate.

my final decision

Cases such as this are a good example of the kind of finely balanced decisions I have to make in circumstances where I can't know for sure everything that has occurred – decisions that I must make on the balance of evidence, fairly and reasonably. But, for all the reasons I've set out above, I think it's fair and reasonable to tell Metro Bank PLC to reimburse Miss B's loss.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 12 April 2019.

Beth Wilcox
ombudsman