DRN-3829263

The complaint

Mrs C complains that Metro Bank PLC hasn't refunded her after she fell victim to a scam, where a fraudster impersonated her daughter on a messaging app.

What happened

Mrs C received a message on WhatsApp from an unsaved number. The message said, *"Hi mum, my phone is broken. This is the new number you can save. Are you home?".*

Mrs C immediately believed this message to be from her daughter. It was in fact a scammer. Mrs C has explained that she knew her daughter had been having problems with her phone and so the message was given legitimacy. Without prompting, the scammer went on to say that they'd dropped their phone, breaking it, hence the new one and new number.

The scammer went on to ask Mrs C to make a payment for her. They explained that their banking app was inaccessible because of the new phone and that it would take 48 hours for security checks to be completed.

Mrs C wanted to help but said she didn't have money in her account. She's explained how she felt overcome with panic and the need to help her daughter. She was worried that her daughter would get into trouble if she didn't make the payments that were due.

Mrs C suggested asking other family members for help, whom she mentioned by name. The scammer picked up on these names and asked Mrs C to request money for her. They said they were still completing installation and updates on the new phone and so were struggling to make calls.

Mrs C went on to contact two family members who agreed to send money to Mrs C, before she sent it on for her daughter, on the understanding it would be repaid within two days. Mrs C was able to get £800 together, although the scammer had asked for £1,250 to be sent. They said they'd contact the recipient to explain a partial payment was going to be made and that the balance would be paid in the next couple of days.

The scammer provided Mrs C with the account details the payment was to be sent to. The details included the names of an individual that Mrs C didn't know. She didn't ask what the payment was for or who the person was, only saying to who she thought was her daughter, "*This better not be dodgy*."

Once the money was sent, the scammer continued to message Mrs C in an informal, conversational way.

Mrs C genuinely spoke with her daughter later that day and the scam was revealed. She contacted Metro right away to report the scam.

Metro looked into what happened and considered whether it ought to reimburse Mrs C. It considered whether Mrs C was due a refund under the Lending Standard Board's Contingent Reimbursement Model (CRM) Code. The CRM Code, broadly speaking, states that a victim of a scam, like Mrs C, should be refunded unless it can be shown they failed to meet their requisite level of care, as set out in the Code.

Metro said that Mrs C had failed to meet that level of care because she'd ignored what the bank considered to be an effective warning, which it presented to her at the time she was

making the payment. It also said she'd not had a reasonable basis for believing she was speaking with her daughter, having not carried out any checks to make sure it was her. It declined to reimburse Mrs C's loss on those grounds.

Metro contacted the bank the money was sent to, but no funds were recoverable.

Mrs C was unhappy with Metro's answer and so brought the complaint to our service. One of our investigators looked at what had happened and found Metro had unfairly declined Mrs C a refund.

Our investigator considered the warning Metro said was most likely presented to Mrs C. He didn't believe it met the definition of an Effective Warning as set out in the CRM Code. The warning appeared as follows:

If you're sending money to someone you've never met or don't know, they might not be who they say they are.

Things to remember:

- *If you met them online, there's an even higher risk of them not being who they claim to be.*
- *Even if it's a friend or family member, check it's really them – one way to do this is to contact them in a different way than you usually do.*

Don't make this payment unless you know your money is going to the right place.

Call us if you have any questions.

That meant Metro couldn't rely on it as an exception to reimbursement. He noted that Metro couldn't evidence what warning it gave to Mrs C, but said that none of the warnings that were more likely than not to have been shown met the requirements of the CRM Code. He found the warnings weren't impactful or specific enough to bring to life the scam Mrs C fell victim to. He said the warnings also failed to set out the full consequences of proceeding.

The investigator also considered whether Mrs C held a reasonable basis of belief when she made the payment. His arguments can be summarised as:

- Mrs C was aware that her daughter was having problems with her phone and this matched what was said by the scammer;
- The scammer presented a plausible reason – tied to the replacement phone – as to why they couldn't make the payment themselves;
- The scammer explained the money was for a payment to someone else, and so the unknown payee name was explained;
- The tone of the messages was informal and conversational, with the scammer picking up on cues from Mrs C which made the chat seem more genuine;
- The scammer played on the emotional attachment between Mrs C and her daughter, exploiting the inherent trust between them. He said he could understand why Mrs C felt her daughter was in trouble and needed help getting out of it, so she was compelled to help.

Our investigator recommended a full refund based on the above. He awarded no compensatory interest as he could see the money had come from family members and would be paid back to them once refunded.

Metro responded to the investigator's view and didn't accept the outcome. The response contained no comment on the reasonable basis of belief element of the complaint; only the warnings were addressed. It said:

- the warning that was likely presented to Mrs C said, "*Even if it's a friend or family*

member, check it's really them – one way to do this is to contact them in a different way than you usually do."

- the heading of the warning cautions to '*stay safe from fraud'*. It said most people should understand the word 'fraud' and the consequences.
- Mrs C had said on a phone call that she'd *"probably not"* read the warnings presented to her, so it was unfair to place much weight on the contents of any warning.

Our investigator's view wasn't changed by what the bank had said. He went on to have a further conversation with Mrs C about her personal circumstances. Mrs C explained several health conditions, along with major life events, which our investigator felt meant she exhibited some significant vulnerabilities, in the context of the scam she fell victim to.

I won't go into excessive detail here as to do so would be unnecessary. But some key points are:

- Mrs C's husband had left the marital home without notice three months earlier which had caused a great deal of upset and anxiety;
- Mrs C has a chronic condition which is a source of stress and anxiety for her. She also takes medication which can exacerbate her anxiety and bring on confusion.

Mrs C has explained how the combination of life events and different medications often leave her in an anxious state and unable to make the right decisions. She's explained she often experiences confusion and forgetfulness. At the time of the scam, when she thought her daughter needed money quickly, she's explained how she was solely consumed with helping her and could focus on nothing else.

With this additional information in mind our investigator wrote to the bank to explain he felt a further section of the CRM Code was applicable in Mrs C's case. This section specifically talks about the protection of vulnerable customers. The relevant part of the Code says:

R2 (3)A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered. This should be assessed on a case-by-case basis. In these circumstances, the Customer should be reimbursed notwithstanding the provisions in R2(1), and whether or not the Firm had previously identified the Customer as vulnerable. Factors to consider include:

(a) All Customers can be vulnerable to APP scams and vulnerability is dynamic. The reasons for dynamics of vulnerability may include: the personal circumstances of the Customer; the timing and nature of the APP scam itself; the capacity the Customer had to protect themselves; and the impact of the APP scam on that Customer.

On this basis our investigator said Metro ought to refund Mrs C, regardless of its thoughts on the warnings presented and Mrs C's reasonable basis of belief. Metro responded but only to say it hadn't been aware of Mrs C's vulnerabilities before the scam, and the details hadn't been revealed through its investigation. The investigator pointed out that Metro needn't have been aware of the vulnerabilities in advance in order for a refund to be due under the Code, but he received no further response. And so the case has been passed to me for a final decision.

What I've decided – and why

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

Metro is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM) Code which requires firms to reimburse customers who have been the victims of APP

scams like this in all but a limited number of circumstances. Metro says one or more of those exceptions applies in this case.

It says Mrs C ignored what it considers to be an effective warning. It also contends that she didn't have a reasonable basis for believing she was speaking with her daughter. Metro says Mrs C ought to have done more to make sure it was her daughter she was talking to.

It's for me to determine whether those exceptions to reimbursement can be fairly applied in the circumstances of this case.

Did Mrs C ignore an effective warning?

The first thing to note here is that Metro can't evidence what warning Mrs C would have been shown. The Code requires banks like Metro to keep robust evidence about any claim decisions made under the Code. As it is unable to evidence what warning Mrs C might have been presented with, I'm not persuaded it can fairly rely on the effective warning exception to reimbursement.

It's also true that the warnings Metro believes Mrs C most likely saw do not meet the standards set out in the Code. I, like the investigator, find the warning doesn't bring to life the scam Mrs C was falling victim to.

Banks like Metro ought to be very much aware of how scams like this tend to unfold. Contact will often come unprompted from a new number, with a 'hi mum/dad' introduction. Scammers often try to impersonate a parent's child in this way, and WhatsApp is a common means of doing so. But none of that detail is brought to life.

I don't find that the suggested steps to prevent such a scam go far enough either. These aren't really linked to the detail of how the scam works. And it would seem to be more impactful to spell out specifics, such as actually calling someone if a new phone number has been supplied. It's not for me to tell Metro how its warnings should appear. But it is clear to me that the warnings it has provided aren't specific or impactful enough to meet the requirements of the Code.

I know Metro has also said that the heading of the warning – '*stay safe from fraud' – ought* to have been enough to inform a customer about the consequences of proceeding with a payment. I disagree. The Code requires Metro to clearly express what the consequences would be; that the money would likely be lost and irrecoverable. Metro contests that customers would understand that inherently, but again I disagree. Many people believe that they are protected by their bank, should they fall victim to fraud or a scam. Or that their bank will be able to claw back funds sent as a result of a scam. Metro ought to be aware that neither of those points are necessarily true, and often aren't the case at all.

Metro has also argued that given Mrs C said she probably didn't read the warning at the time it's more likely than not she'd have not taken heed of any warning, no matter the wording. Whilst I can see the point Metro is making here, I don't believe the argument carries weight. Had the warning been more specific and impactful, by properly addressing the scam and how to prevent it, there's a good chance it would have altered Mrs C's actions.

Even if a warning with different content and wording wouldn't have made a difference, it doesn't automatically follow that Mrs C failed to meet her requisite level of care under the Code. Metro would still have to consider whether Mrs C ignored an effective warning and, if so, whether it was reasonable for her to do so in all the circumstances of the case. A consideration of her reasonable basis of belief would also still be necessary. If neither exception were to apply, then it doesn't matter whether Metro could have prevented the scam (through a warning) or not and Mrs C would still be due a refund under the Code.

Did Mrs C have a reasonable basis for believing the purpose of the payment and person she was talking to were legitimate?

It's important to remember when dealing with scams like this, and in fact any scams, that customers are generally not in a state of alert when it comes to detecting and preventing fraud. People don't expect to be scammed in their day to day life. And I think it's easy for the banking industry to become almost 'hyper-sensitive' to scams, where the expectation is that all details of any interaction ought to be questioned by a customer. Particularly when reviewing a case of fraud in hindsight.

But that isn't a realistic view of how individuals go about their lives and the expectation is set too high.

Unless there is something within an interaction that clearly seems out of place or unusual, people will often not detect that something might be wrong. Scams like this succeed because fraudsters are adept at exploiting human nature and behaviours.

Mrs C's case is a prime example of such exploitation. She was contacted on a new number by who she believed was her daughter. It was purely by chance that Mrs C knew her daughter's phone had been playing up, meaning legitimacy was immediately lent to the messages received.

What followed, whilst not detailed, appeared to be a normal conversation about needing to borrow some money fairly urgently. This kind of scam is designed to prey on a parent's natural inclination to help and defend their child. And so, it's fair to say, the rationale or circumstances may not be questioned as much as they otherwise might be. The fraudster is playing on an emotional response, that the parent is unlikely to be particularly aware of at the time.

Where there isn't anything within the messages that appears off or unusual, I find it's fair to say that Mrs C held a reasonable basis of belief that she was dealing with, and helping out, her daughter.

I can see from the chain of messages that the fraudster quickly and cleverly picks up on cues from Mrs C, notably around the names of family members and seeking help from them too.

The messages show the scammer added legitimacy to the request for payment by giving a reasonable explanation as to why the payments couldn't be made by Mrs C's daughter. It was explained that the banking apps weren't yet accessible on the new phone. I consider that's not an unreasonable explanation for Mrs C to have accepted.

I can't see that Metro has considered these points in its investigation. Indeed, it failed to comment on any of the detail after our investigator issued his opinion. And so it's given no further defence on the reasonable basis of belief argument.

Mrs C has explained how she panicked at the time and was just thinking about helping her daughter. And it's clear from what happened, in terms of sourcing the funds, that Mrs C was somewhat frantically trying to help. She quickly suggested other family members that might have been able to assist, and even contacted them herself in order to gather at least some of the money that had been requested.

Metro's position prior to the investigator's view looks to have largely been based on an assumption that Mrs C ought to have been immediately wary about contact from a new phone number, and ought to have been questioning the detail immediately. But I don't consider that to be a fair and reasonable position to take, in light of the circumstances of the case and the nature of the scam.

Was Mrs C vulnerable to this type of APP scam at the time?

Unfortunately, I don't know what Metro's view of Mrs C's vulnerabilities are. It's chosen not to comment on them despite our investigator setting them – and the impact of them – out in correspondence with the bank. All Metro has said is that it was unaware of Mrs C's

vulnerabilities and that she hadn't informed it of anything before the scam took place or whilst it was investigating (including several conversations on the phone).

I find this to be a disappointing response from Metro, for a few reasons. For one, Metro ought to know that upfront knowledge of any vulnerability is not an exception to reimbursement under R2(3) of the Code. Once details of vulnerabilities have been presented, they should be considered and assessed. Metro hasn't done that here, even after the involvement of – and prompting from – this Service.

It's also clear that Metro didn't seek to question Mrs C on her personal circumstances, or to investigate any potential vulnerabilities, at the time she reported the scam. I wouldn't expect a customer to divulge their personal and medical history to their bank unprompted. Often an individual will wish to remain private and won't understand the significance of providing such detail. It's for Metro to sensitively enquire about a customer's personal circumstances in order to draw out important details that might impact their claim.

Given what Mrs C has said about her anxiety and the state of panic she found herself when she received the request from her daughter, and the lack of input from Metro, I do think it would be fair to say reimbursement under R2(3) applies. And so even if there had been a finding that Mrs C ignored an effective warning, or that she didn't have a reasonable basis of belief, a refund would still be due.

Putting things right

Metro should now refund the £800 lost to the scam. Like our investigator, I make no award of interest on the amount as the principle sum was provided by family members on the understanding it would be repaid.

I make an award of £200 compensation for distress and inconvenience on the following grounds, which I've covered in my findings above:

- Metro Bank's failure to properly engage with this service in respect of responding to the investigator's findings;

- Metro Bank not adhering to the principles of the Code. This is evident both at the time the scam claim was being investigated by Metro, and when the complaint came to this service;

- Any complaint will naturally take time to resolve. It's not the case that compensation ought to be paid just because a business didn't resolve the complaint itself, and that it was brought to our service. But the two above points have meant the resolution of this case has been unnecessarily protracted. This would likely cause anyone unnecessary upset, but Mrs C suffers from anxiety, and has other health conditions, which have meant having the scam hanging over her for so long has been particularly distressing.

My final decision

I uphold this complaint against Metro Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs C to accept or reject my decision before 4 April 2023.

Ben Murray
Ombudsman