DRN-4381890

The complaint

Miss M complains that Barclays Bank UK PLC is holding her liable for the money she lost to a scam.

What happened

The details of this complaint are well known to both parties. So rather than repeat them all again here, I'll briefly summarise the key points.

In August 2021, Miss M was on holiday abroad when she received a call from a number that appeared to be Barclays. She had a bad connection, so they arranged to call her back later that afternoon. Unfortunately, it seems this was a scammer who impersonated Barclays and 'spoofed' its number.

Miss M says she was told that transactions were happening on her card from a UK location. She checked her app and told the scammer she couldn't see any unexpected transactions. They said that was because their fraud systems pick up attempted payments before they show on the account.

Miss M says, in addition to the number spoofing, the caller knew details about her such as her mother's maiden name. She says they also told her they would pay her £250 for staying on the line. And at one point, she saw what appeared to be £75 credited into her account.

Thinking she was speaking to her bank, Miss M admits providing codes to the scammer – including 'PINsentry' codes, which would have allowed them access to her account. They told her there was a virus on her app, so they needed to transfer her funds to check whether it was working – but said they would pay the money back into her savings. It seems Miss M therefore provided the scammer with OTP codes to authorise payments out of her account.

Miss M says the scammers, posing as the bank, told her they would call her back the next day. But she didn't receive a further call from them. She then spoke to her mum and realised she had been scammed. She called Barclays to report this and found out £72,990 had been transferred out of her account, partly funded by a £23,000 loan. I understand the timeline for this is as follows:

Date	Time	Event	Amount	Main source
27/08/2021	16.38.57	Bank transfer to 'Mr M'	£24,990	Savings
27/08/2021	16.54.52	Bank transfer to 'Company One'	£24,000	Savings
27/08/2021	*17.03.37*	*Loan application*	*£23,000*	*n/a*
28/08/2021	09.32.01	Bank transfer to Company One	£10,000	Loan
28/08/2021	09.46.26	Bank transfer to 'Company Two'	£14,000	Loan and savings

Unhappy that Barclays was holding her liable for the payments and the loan, Miss M complained. But it didn't agree to refund her or to write off the loan. It did offer her £75 compensation – which it later increased by £100 (so £175 in total) - for service failings while considering her fraud claim. Miss M didn't agree so referred the matter to our service.

Our investigator didn't uphold the complaint. She thought the case should be considered in line with the Lending Standards Board's Contingent Reimbursement Model (CRM) code – which requires firms to reimburse customers who fall victim to authorised push payment (APP) scams unless they can show an exception applies under the code. But she thought an exception did apply, as she didn't think Miss M had a reasonable basis for believing the person she was speaking to was legitimate.

Miss M appealed the investigator's view, so the case was referred for a final decision. Since then, I have received further information – which I have shared with Barclays – regarding the accounts the funds went sent to. The recipient bank confirmed the account names these show as being sent to (one appeared to share Miss M's surname, and the other two appeared to be businesses local to her home address) were false. It has since closed the accounts due to fraud concerns.

I also requested further information from Barclays, such as further audit information relating to the loan application, and a clearer explanation of the account use at the time of the scam, in June 2023. I subsequently escalated my request. Barclays didn't responded.

In accordance with the rules set out in the 'DISP' section of the Financial Conduct Authority handbook, specifically DISP Rule 3.5.9(3) and DISP Rule 3.5.14(1), I proceeded to issue a provisional decision based on the information I held in September 2023 – taking into account Barclays's failure to provide the information I requested.

I explained I was minded to uphold the complaint and direct Barclays to refund some, but not all, of Miss M's loss for the following reasons:

> *Authorisation*
>
> *There were a couple of calls made to Barclays as part of the process to authorise these payments. It seems these calls weren't made by Miss M, but by someone impersonating her. However, Miss M admits that, during the scam call, she shared codes with the scammer. And it also seems she was aware, and understood, that payments were being made. It's just that she thought she was acting on the instructions of her bank, who would refund her afterwards.*
>
> *Miss M has also provided a screenshot of a text exchange from Barclays, asking her to reply 'Y' if she made the payment to Mr M, or 'N' if it was fraud. She replied Y. Which further suggests she was aware of, and agreed to, the payments.*
>
> *While Miss M may not have completed all the steps to make the payments, I do think she was aware that payments were being taken – and was completing some steps to allow that to happen, or to grant the person she was speaking to authority to make the payments. I therefore consider the payments on 27 August 2021 to be authorised.*
>
> *But based on the available evidence, I also think Miss M was the victim of an APP scam. There has been consistent testimony from her throughout about having been tricked, and she's shown us records of the calls she received from the spoofed Barclays number.*

While I understand why Barclays was initially concerned about the payment destinations, I think the information from the recipient bank offers more reassurance that the recipients weren't actually linked to Miss M. I've pointed this out to Barclays – and it hasn't responded to raise anything further regarding this. So, as things stand, I think the payments rightly fall under the scope of the CRM code.

However, Miss M maintains she didn't receive the call back she was expecting the following day. And, having listened to the call Barclays received in relation to the £10,000 payment, I don't think it was made by Miss M. Nor – so far as I've been made aware – was it made from Miss M's number. It's also not clear to me what location the call was made from.

A code was sent to Miss M's phone during this call – which the scammer provided to Barclays for security. It's not clear to me how the scammer got hold of this code. Miss M is adamant she didn't share any security information or download anything to allow access to her devices. And she's also consistently maintained that she didn't speak to the scammers on this date. So, unlike the payments on the first day, it doesn't fit that she was handing them over to the scammer with the intention of allowing payments to be made.

While I don't know how the scammer got hold of this code, bearing in mind the lack of clear information I have about the devices used, I'm minded to conclude these payments weren't authorised by Miss M.

During the call there is mention of "unusual software" being detected on a device being used to access the account – seemingly via online banking rather than mobile banking. But this raises concern about unauthorised access to the account. Although Miss M doesn't recall downloading anything to grant access to any device, it's possible she may have been tricked into doing so inadvertently. Or that the scammer was able to use the codes she shared to set up online banking on another device which they had control of.

Without knowing exactly how the scammer got hold of the code, and in the absence of further evidence which I requested from Barclays to help clarify this point (and other points), I'm not persuaded Miss M likely shared it for the purpose of authorising a payment. And I haven't seen any indication that a further code was sent for the payment to Company Two.

I also don't think, in the circumstances, Miss M acted with gross negligence in failing to keep her security details safe. As anything she did share, was shared with who she thought was her bank. While (as I'll expand on below) I do think there was some negligence on Miss M's part, I'm not persuaded it amounts to gross negligence. This is also in the context of her being put under pressure, with the scammer using social engineering to influence her actions during the call the previous day. And again, I'd reiterate that I haven't received information which I've requested from Barclays, in order to consider the circumstances of the payment further.

I'm therefore minded to conclude the payments on 28 August 2021 were unauthorised, and that Barclays is liable for them.

<u>CRM code</u>

As our investigator explained, the starting position under the code is that banks should refund victims of APP scams unless an exception applies. She thought the relevant exception that applied here was:

- *The customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.*

Having carefully considered this point, I agree with the investigator that this exception does apply. I appreciate that the scam involved some sophisticated techniques, such as spoofing and social engineering. But Miss M has also told us she was suspicious of the call. And that is further supported by the records she has sent us, showing she was taking screenshots of the calls whilst still speaking to the scammers.

Despite this, she repeatedly shared codes with the caller – which were sent with warnings about the importance of not sharing codes, and provided specific details for at least one of the payments. She also appears to have missed that she was sent a text from Barclays saying that a loan had been applied for, and to get in touch if this wasn't her.

The circumstances of her being told she would be paid if she stayed on the line also sound unusual. While I appreciate Miss M says she appeared to have received a payment during the call, the amount she says this showed didn't match the amount she says she was told she would be paid. And it doesn't sound particularly credible that a bank would be offering her money to stay on the line.

Taking this altogether, I don't think Miss M did have a reasonable basis for believing the caller. While that means I don't think Barclays is obliged to refund her in full, I've also thought about Barclay' obligations under the code.

In response to the first payment, Barclays did identify a risk; it stopped the payment pending a conversation with Miss M. But it seems the scammer was able to pre-empt this by calling Barclays. And it verified the caller by sending a code to her registered device, which the scammer was able to provide. In the context of what Miss M has told us, I understand this was likely due to her sharing the code with the caller. The caller was also able to correctly answer a security question relating to Miss M's personal details.

The scammer was therefore able to provide assurances over the phone about the payment, such that Barclays was happy to proceed once Miss M responded to its text asking her to confirm the payment.

In the circumstances, I can't see what else Barclays ought reasonably to have done that would have had a material bearing on her loss. It wasn't put in a position where it could have taken reasonable steps to deliver an effective warning that Miss M would have seen.

Miss M shared the code she was sent, meaning the scammer was able to speak to Barclays about the payments. Furthermore, she shared PINsentry codes which (from what we've been told) allowed the scammer access to make the payments on Miss M's behalf under false pretences. So Barclays wasn't in a position to deliver an effective warning to her which Miss M she could have acted on.

I appreciate this will be disappointing for Miss M. But in the circumstances, I'm not persuaded it would be fair and reasonable to expect Barclays to refund her for these payments, in line with its expectations under the CRM code.

The loan

Miss M maintains that she didn't apply for this loan. Barclays says it was applied for using her IP address from a genuine device. But it hasn't responded to my request for clear evidence of this.

As things stand, taking account of Barclays' failure to provide the information I've asked for, I consider it likely the loan was unauthorised. Miss M has consistently denied applying for it. As she shared PINsentry codes, we also have a plausible explanation for how someone else had access to her online banking and make the application – without having her permission to do so.

In line with what I've explained above, I'm also satisfied the funds were moved on from the account without Miss M's authorisation.

In the circumstances, I therefore don't think Miss M should be held liable for the terms of the loan contract, as I don't believe she consented to them. And as I don't think she knowingly passed on the funds, I don't consider it fair for Barclays to pursue her for the capital either. That is another reason why I wouldn't consider it fair for Barclays to hold her liable for the payments made on 28 August 2021 – as they were predominantly funded by the loan.

Compensation

Barclays has offered a total of £175 compensation for how it handled Miss M's fraud claim. Bearing in mind the main cause of Miss M's upset is the actions of the scammer, I'm satisfied that fairly reflects the distress and inconvenience caused by Barclays' service failings. Such as the time taken to respond, and the lack of clarity it gave initially about whether the loan had been drawn down.

I invited both parties to submit any further comments or evidence in response. Barclays responded to accept my provisional decision, but Miss M didn't agree. In summary, she said that – while she understands that the more codes shared, the less reasonable the basis for belief – it was reasonable to share the first code, for the payment of £24,990.

Miss M also said there was a failing by Barclays, as it didn't proactively reach out and instead allowed the scammer to call in. And she doesn't think that was sufficient. Particularly bearing in mind that the number called from wouldn't have been her genuine number.

I had also asked Miss M to clarify a few points, bearing in mind Barclays had the opportunity to provide further information following my provisional decision (although it has opted not to). She confirmed the following: so far as she can recall, she didn't any suspicious calls or texts etc. prior to the scam call; she didn't receive a call on the morning of 28 August 2021; she mainly uses her Barclays app on her phone to access the account, and while she has access on her laptop she rarely uses it; she saw the £75 compensation payment on her app; and there was no use of remote access on her phone.

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.

Having done so, including considering Miss M's response, I've come to the same outcome as I did in my provisional decision – and largely for the same reasons, which are set out above and form part of my final decision. So I'll focus here on responding to the further points Miss M has raised.

First, I've considered Miss M's argument for why she feels she had a reasonable basis of belief when making the first payment. But, in line with the considerations of the CRM code, I'm not persuaded she did.

As set out in the table above, the first payment went through at 16.38. Miss M has provided search results from her phone showing she looked up the number, in connection to it being a scam, at 16.39 and 16.40. To me, that suggests she did have concerns at the time of the first payment – which matches what she has told us about being suspicious of the call. She was also taking screenshots throughout the call, which again suggests to me she had concerns.

Miss M had already received several messages and codes by this point. The first, which appears to have been sent at 16.26, explained that Miss M would receive a text to confirm a payment made via online banking. It warned that, if she had been called and asked to transfer money to a secure of secure account, to stop as this was a scam. Yet she responded to the message, sent separately, to confirm she had requested it.

Following this, Miss M was sent a message saying she had called, and Barclays had provided a one time passcode, contained in the message, which she had requested. It said to contact Barclays if she hadn't requested it (which she hadn't). She then seemingly shared the code with the scammer. This is seemingly in addition to what she has told us about sharing PINsentry codes.

This was all done in the course of making the first payment. In the circumstances, including the timings and sharing of codes set out above, but also the wider points I set out in my provisional decision, I'm not satisfied Miss M had a reasonable basis for believing the caller was legitimate. For example, I'm not persuaded the explanation that she needed to send these funds to test the app due to a virus, but would later be refunded, sounded plausible.

I think Miss M had cause to take further steps to confirm the caller before handing over the codes. Which were compounded by what happened later on, when she received the text about the loan that was taken out. I therefore consider that Barclays has fairly applied the exception under the CRM code due to Miss M not having a reasonable basis for belief.

I have also reconsidered whether Barclays did enough in light of Miss M's rebuttal. And I am mindful that one of the queries I asked Barclays, which it didn't respond to, was about the phone the impersonation calls were received from.

However, there are many legitimate reasons why someone might contact their bank from a different number to the one they have registered with their bank. Given the details the scammer knew about Miss M – including that she was abroad – I don't think this in itself gave Barclays much cause for concern.

Furthermore, as explained in my provisional decision, Barclays didn't just rely on an incoming call from what may have shown as a different/unrecognised number. It sent Miss M a text to her registered device during the call, which the scammer provided to Barclays. This was in addition to Miss M responding to a text to confirm the payment, and security questions it asked to verify who it was speaking.

I therefore don't think Barclays was put in a position where it should reasonably have taken further steps to effectively warn Miss M about the scam risk. And this was due to her responding to messages to verify the payment, as well as sharing codes with the scammer – which, as I've explained, I'm not satisfied she did with a reasonable basis for believing the caller. In those circumstances, I therefore don't consider it fair to direct Barclays to reimburse her under the terms of the CRM code.

I appreciate this will be disappointing for Miss M. But, when looking at Barclays liability here, I'm not persuaded it's fair to direct it to refund her for the authorised payments. However, as explained in my provisional decision, I don't think she should fairly be held liable for the loan or the subsequent unauthorised payments.

My final decision

For the reasons given above, my final decision is that I uphold this complaint. To put things right, I direct Barclays Bank UK PLC to:

- Remove any information reported to the credit reference agencies about the loan taken out in Miss M's name, and stop pursuing her for this debt.
- My understanding is that Miss M hasn't made any payments towards the loan. But if she has, those should be refunded, plus 8% simple interest per year from the date of payment to the date of settlement.
- Refund her £1,000 for the unauthorised payments funded from her own money rather than the loan. As I understand these originated from her savings account, Barclays should pay the savings account interest rate on this amount, from the date of payment to the date of settlement.

Barclays Bank UK PLC must pay this compensation within 28 days of the date on which we tell it Miss M accepts my decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 2 November 2023.

Rachel Loughlin
Ombudsman