

The complaint

Miss K is unhappy that Monzo Bank Ltd are holding her liable for a transaction she says she didn't make.

What happened

On 15 July 2021, Miss K says she received a call from someone claiming to be from Monzo. She says the phone number matched Monzo's number, and the caller knew some of her personal details such as her name and date of birth.

Miss K explained that the caller told her that someone was trying to access her account and was persuading her to open her banking app to verify something. She said she wasn't happy to do so as she was aware Monzo wouldn't call her. She also said that the caller was trying to keep her on the phone and since she wasn't comfortable, she ended the call.

Shortly after, a payment of £234.97 left Miss K's account and she contacted Monzo to report it as unauthorised. It was a contactless payment made via Apple Pay using a secondary device to that of Miss K's trusted device.

Miss K confirmed that she still had her card in her possession and no one else had access to her card, phone or Personal Identification Number (PIN). She told Monzo her phone is protected with Face ID. She also hadn't recently clicked on any text messages or emails asking her to enter any of her information nor did she download any apps on her phone at the caller's instruction. She said she didn't give the caller any information, didn't open her banking app or authorise anything. She explained that if she had approved anything on her banking app, it was done so accidentally.

Monzo said they were unable to refund Miss K as the payment was made using an Apple Pay token on a secondary device which only she could've authorised. Unhappy with this, Miss K referred her complaint to our service.

Monzo told our service they believe Miss K may have been a victim of a scam, but she hadn't provided all the necessary information to help them investigate. They say Miss K was active on her banking app while the transaction was approved, and she knows how the banking app works. They believe it would've been clear to Miss K that she was approving a card for Apple Pay so it's reasonable to assume she knew what she was doing.

Our investigator said she didn't think Miss K had authorised the payment. She asked Monzo to refund her and add 8% simple interest to this amount. Monzo disagreed and asked for an ombudsman to make 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.

Under the relevant regulations, Monzo can hold Miss K liable for the disputed transaction if the evidence suggests it's more likely than not that she made or authorised it herself.

The disputed payment of £234.97 was authenticated using Apple Pay. Monzo have provided technical evidence which shows that the payment tools issued to Miss K approved the Apple Pay token to be added to the secondary device – which was then used to make the disputed payment shortly after.

But this alone isn't enough for Monzo to hold Miss K liable for the disputed transaction. I also need to be satisfied that based on the evidence, it's likely that Miss K herself made, or otherwise authorised the transactions.

Miss K has maintained that she didn't go into her banking app at the scammer's request to verify anything. This explanation conflicts with the technical evidence as the audit report shows that Miss K had accessed her banking app several times during the scam call and that she approved the Apple Pay token by entering her card's Personal Identification Number (PIN). Miss K has clarified when questioned further that if she approved anything on the banking app, it was done so accidentally.

This is a finely balanced case, and I can't say with completely certainty as to what exactly happened. So, I need to make a decision based on what I think is most likely.

Monzo believe Miss K has been a victim of a scam. I agree this is one possibility. But on balance, I find Miss K's explanation that she might've accidentally approved the Apple Pay token plausible and most likely, given that she's also said that she recognised the call was a scam quite early on. It follows, I don't think Miss K authorised the disputed transaction.

In order for Miss K to have consented to the disputed transaction, I need to be satisfied that she:

- Disclosed her long card number, expiry date and three-digit security code; and
- Approved the Apple Pay token to be added using her banking app.

I appreciate there's some inconsistencies in Miss K's testimony, but I've not seen any evidence to suggest that she disclosed all the card details required for the scammer to add the Apple Pay token to their device.

I don't think it's improbable and nor can I rule out the possibility that Miss K's card details may have been compromised somehow without her involvement. For example, through data linked to transactions she authorised leading up to the scam call.

While the evidence shows that Miss K approved the Apple Pay token on her banking app, she has explained that if she did so, it was likely by accident. Monzo feel that it's very unlikely for Miss K to have completed the process accidentally as she would've had to tap to continue and then input her PIN.

I've looked at the screenshots Monzo have provided which shows the process Miss K would've followed to approve the Apple Pay token. I don't think it's clear from the screenshots that Miss K would've been aware that she was approving for her card to be set up on a secondary Apple device.

I'm persuaded it's plausible for Miss K to have approved the Apple Pay token by 'accident' and that she didn't knowingly approve the Apple Pay token, particularly given that we know

this happened towards the end of the spoof call when Miss K was distracted due to the scammer trying to keep her on the phone, and she was frequently checking her banking app during this time.

Based on what I've seen, I don't think there's enough evidence to show that Miss K, or someone with her permission, completed both the steps required to have consented to the Apple Pay token being added to a secondary device – meaning the disputed transaction wasn't authorised.

I also don't think Miss K failed with intent or that she was grossly negligent. Since Miss K approved the Apple Pay token, she allowed the disputed transaction to take place. However, I don't think Miss K intentionally approved the Apple Pay token and she did so without realising that the safety of her account would be compromised. So, Miss K didn't fail with intent.

The standard for gross negligence is whether Miss K was significantly careless – did she act so far below what a reasonable person would've done or seriously disregarded an obvious risk.

Monzo say they can't assess whether Miss K was grossly negligent without her revealing the full details surrounding the spoof call. I agree it'd be simpler if Miss K was able to provide further information, but this isn't a clear-cut case.

I don't believe Miss K is deliberately holding back details. Monzo have accepted the call she received was likely from a scammer, but they've not appropriately considered the range of emotions that the recipient of one of these calls goes through. Even though Miss K twigged that something was amiss during the call, it wasn't like that right from the off, otherwise she would've immediately hung up. The caller must have resonated with her to some extent so I can understand why she wasn't thinking clearly in the moment within a stressful environment.

So, I don't think that the actions Miss K took under the circumstances of this complaint – approving the Apple Pay token accidentally and unintentionally, when the notification on the banking app wasn't clear that she was agreeing for her card details to be added to a secondary device not belonging to her, while she likely was unaware that her card details were already compromised – amounts to gross negligence.

Miss K took the actions I'd expect as soon as she became aware of the disputed transaction. She immediately froze her card and contacted Monzo to dispute the transaction which prevented any further unauthorised transactions – which is consistent with her testimony that she didn't authorise the transaction.

Monzo feel Miss K has attempted to hide information from them about a text message they sent to her on 15 July 2021. This, along with the lack of explanation from Miss K about the spoof call, has raised their suspicions. They say they haven't been able to complete a full investigation due to Miss K's dishonesty which they believe is an exception for reimbursement under the Contingent Reimbursement Model (CRM) code.

I can't say for certain about what happened to the text message Monzo sent Miss K. But I can't see a plausible explanation for why Miss K would withhold this information as it doesn't undermine her case as she's presented it. I think it's most likely that Miss K didn't receive the text message as she reacted to Monzo's notification about the disputed transaction debiting her account immediately.

In any event, I should clarify that the CRM code only applies to authorised push payments such as faster payments. The CRM code doesn't cover pull payments such as contactless payment transactions, so the exceptions of the code can't fairly be applied in this case.

All things considered, I don't think it's fair and reasonable for Monzo to hold Miss K liable for the disputed transaction and to put things right, they should:

- Refund Miss K £234.97;
- Add 8% simple interest* per annum from the date of the payment to the date of settlement.

*HM Revenue & Customs requires Monzo to deduct tax from this interest. Monzo must give Miss K a certificate showing how much tax they've taken off, if she asks for one.

My final decision

For the reasons given above, I uphold this complaint and require Monzo Bank Ltd to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss K to accept or reject my decision before 4 January 2023.

Ash Weedon
Ombudsman