DRN-3372319

The complaint

Mr F is unhappy that Monzo Bank Ltd won't refund transactions that were made when he fell victim to a 'safe account' bank impersonation scam.

What happened

In August 2020, Mr F received a text message purporting to be from Monzo. It said there was a £1,200 transaction to a retailer being attempted on his account. It appeared in the thread of genuine messages Mr F had previously received from the bank. The text message gave Mr F a phone number to call.

Mr F says that he rang the number and spoke to someone for about 20 minutes. He thinks that he confirmed his name and his email address during the conversation but ended the call because it didn't seem right. Mr F said the situation didn't add up because at the time he didn't have any money in his Monzo account.

Within minutes, Mr F received a phone call. His phone records show that the incoming call appeared to come from a genuine Monzo phone number. Mr F has told us that the caller went through security processes with him, knew what his last genuine transaction was and said that there had been an attempt to change details on Mr F's account so they were ringing to confirm whether those changes were requested by him or not. Mr F explains he was convinced he was speaking to the genuine bank because the phone number matched the number on the back of his card. He adds that this caller sounded very knowledgeable and professional.

The caller convinced Mr F that all of his bank accounts were unsafe and that he needed to move his money into his Monzo account because it could be secured. Mr F followed the caller's instructions and transferred £2,400 from his other bank into his Monzo account. Mr F has provided a copy of his bank statement to this service which confirms this is what he did.

Unfortunately, Mr F was speaking to a fraudster that was impersonating Monzo. During this call, Mr F gave the fraudster his personal security information, including access to a Monzo 'magic link' email and his PIN number.

The fraudsters told Mr F that he needed to reinstall his app to be able to reconfirm his identity and complete the account resetting procedure. This distracted Mr F. Using the 'magic link' and PIN number, the fraudsters added a new device to Mr F's profile and made a transaction of £1,000 without Mr F's knowledge or agreement.

Mr F explains that when he reinstalled the app and saw that a payment of £1,000 had left his account, he panicked. The fraudster reassured him that the funds could be recovered if they acted quickly to trace the payment. Mr F says he was told he needed to quickly make another payment so they could work together to try and trap the culprit.

Mr F explains that the fraudster talked him through the steps to follow to make a payment of £1,400. Mr F says that he wanted to make a much lower payment, but the fraudster told him that a payment of £1 would not be enough to trigger the bank's fraud detection systems.

Mr F recalls that the fraudster told him to move past any pop-up messages that asked him if he was on the phone as they were meant for other kinds of situations. Mr F explains that the fraudster told him exactly what was going to pop up just before it happened. Mr F recalls the fraudster also told him to set the payment purpose as something else, stressing that the situation was very time sensitive as there was only a limited window for the bank to trace the payment. After Mr F made the payment, the call ended abruptly.

Mr F immediately called Monzo and asked to be reconnected to the person he was speaking to. During this call, Mr F discovered he'd been the victim of a scam and had lost money. Monzo took steps to secure Mr F's account and tried to recover the funds that had been sent. It looked into Mr F's scam claim but said it was unable to refund the money he'd lost.

Mr F wanted to appeal and made a complaint. He said he was following instructions from people who he believed to be the bank and the payment he made was in panic after seeing the unauthorised payment go out.

Monzo issued its final response. It said Mr F was not covered by fraud protection regulations and could not be refunded. It said he had placed his account at risk and had not taken reasonable measures to keep it safe.

Mr F disagreed and referred his complaint to this service. Our Investigator looked into the matter and broadly recommended that it should be upheld. He didn't think Monzo had done enough to protect Mr F and pointed out that the Lending Standards Board's Contingent Reimbursement Model (the CRM Code), which Monzo has agreed to adhere to, applied.

Monzo replied to say the principles of the CRM Code only applied to the payment Mr F made himself. It considered both payments in turn and said that it felt Mr F had been grossly negligent by sharing very sensitive information. It pointed out there was a clear warning to not forward on the 'magic link' email and that it is common knowledge that a PIN should never be shared, even with a bank. When considering the second payment, it didn't think the bank had failed in its duty under the CRM Code. It said it was not convincing that a bank would use a customer's funds to trap a fraudster and pointed out that Mr F also had reservations about the payment because he'd initially asked to send £1 and not a large sum.

It later added that as Mr F worked in cybersecurity at the time of the scam, he should have understood that forwarding on the 'magic link' email would give whoever it was sent to account access. It felt Mr F understood this but wilfully ignored it at the time of the scam.

As no agreement could be reached, the complaint was referred to me.

My provisional decision

On 20 May 2022, I issued my provisional decision to both parties. In it, I explained why I was minded to uphold the complaint and say that Monzo must refund the money Mr F lost along with interest.

My reasons are provided in italics below:

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

In deciding what's fair and reasonable in all the circumstances of a complaint, 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 be good industry practice at the time.

Payment one – an unauthorised payment of £1,000

Both parties accept that Mr F did not make the £1,000 payment and that he did not give the fraudsters any permission to make payments on his behalf. This means that as a starting point, in line with the Payment Service Regulations 2017 (PSRs), Mr F isn't liable for a payment he didn't authorise, unless he failed with gross negligence or intent to comply with the terms of the account or keep his personalised security details safe.

From the circumstances as they have been described, I don't think Mr F failed with intent to comply with his terms and conditions or keep his details safe. I am persuaded he genuinely believed there was a problem with his banking and that he needed to protect his money.

So I've gone on to consider whether Mr F failed with gross negligence. In other words, whether he was significantly careless; whether he acted so far below what a reasonable person would've done; or seriously disregarded an obvious risk. Establishing gross negligence requires me to consider all the circumstances of what happened. A finding can't be made that Mr F seriously disregarded an obvious risk by sharing the information he did without exploring why he proceeded.

I think it is important to consider the environment created by the fraudsters. Mr F has explained that the phone call came from what he thought was the bank's genuine phone number. Number spoofing is a very powerful technique used by fraudsters which quickly establishes trust and confidence. I can see how the number spoofing persuaded Mr F that he had been mistaken in doubting the call earlier that day. Added to this, the caller knew information about Mr F's genuine transactions and Mr F's recollections of the call suggest that it closely mirrored genuine bank procedures, all of which would have acted to further persuade him that he was speaking with the real bank.

I do not consider that Monzo has placed appropriate weight on the environment that the fraudsters had created. I am persuaded it was not unreasonable for Mr F to trust the information he was being told, especially considering the difficulty he faced thinking clearly under the kind of worry and emotional pressure the scam placed him under. He genuinely thought his money was at risk and that he needed to take action to keep it safe. He thought he was following the instructions of an organisation that he knew and trusted. The prevalence of impersonation scams strongly suggests that lots of other people would have done exactly the same thing as Mr F if they had been in his shoes.

Monzo has highlighted the security features that Mr F shared which enabled the fraudsters to access his account to make this payment, including Mr F's PIN and the 'magic link' email that was forwarded on to the fraudsters which gave them access to login from another device. Whilst I recognise Monzo's concerns that Mr F has been negligent, having considered everything, I am not persuaded that the available evidence is enough to show that Mr F seriously disregarded an obvious risk.

Mr F recalls he was told his PIN was required to make security changes and resets to his account. I asked him what he could remember about how exactly this happened. Mr F told me that he did not say the number out loud at any point but keyed it into his phone's keypad, as the fraudster instructed him to do. Mr F explains that he thought following the steps he was being told was the right thing to do and would enable the bank to check on his account. He pointed out that his other bank uses a security code process and he thought this was a similar verification step. This does not sound like an unreasonable assessment by Mr F. I am persuaded that in the situation the fraudsters had masterfully created, Mr F was not anticipating that a fraudster could detect the number sequence from the keypad tones. I don't think Mr F's unwitting actions in entering his PIN in the manner and circumstances that he has described go so far that they could be considered as significantly careless.

The PIN in isolation would not have been enough to enable a fraudster to move money from Mr F's account. They needed to use those details in conjunction with the 'magic link'. Mr F recalls that the fraudster told him that an email had been sent to him and that he needed to forward it on. He says the fraudster told him not to open the email and to delete it afterwards. Mr F explains that he forwarded the email on believing he was on the phone to Monzo and that he did not read it at the time. He's said he was on his phone app, checking his emails and talking on the phone all at the same time. He's explained that whilst this was happening, the fraudster was telling him about invalid attempts to access his account. Mr F has explained that he was feeling stressed and that he wanted to try and protect his account as quickly as possible.

From what I have seen, I am not currently persuaded that Mr F was significantly careless when forwarding on the 'magic link' email either. He has described an environment where it is very difficult to think clearly and to rationally absorb and process information. He'd been cleverly manipulated into thinking he was doing the right things to keep his money safe and that he needed to act quickly. I understand Mr F's actions provided the tools the fraudster needed to access his account. But in the circumstances, I'm satisfied the possibility of this happening hadn't crossed his mind, given his belief he was talking to his bank. He did not know that a fraudster would use that information to access his account from another device.

For the reasons I have explained, I don't think Mr F's actions fell so far below what a reasonable person would've done that they amount to gross negligence. I am currently minded to say that Mr F isn't liable for the unauthorised transaction of £1,000.

I will now go on to consider the second payment.

Payment two – an authorised payment of £1,400

Under the Payment Services Regulations 2017, the startling position is that Mr F is liable for payments that he has authorised.

As Mr F was the victim of an authorised push payment (APP) scam, my considerations don't end with the PSRs. When a consumer makes a payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

I am also mindful that when Mr F made this payment, Monzo should fairly and reasonably also have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). And in some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

The CRM Code

Monzo has agreed to adhere to the provisions of the Lending Standards Board Contingent Reimbursement Model (the CRM Code) which requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances.

It is for Monzo to establish that a customer failed to meet a requisite level of care under one or more of the listed exceptions set out in the CRM Code.

Those exceptions are:

- *The customer ignored an effective warning in relation to the payment being made.*
- *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.*
- *The customer has been grossly negligent*

There are further exceptions within the CRM Code, but they do not apply in this case

Monzo has argued that Mr F has been grossly negligent. It says that he did not take reasonable measures to keep his account safe and that he has an enhanced awareness of this sort of scam because he is employed in cybersecurity.

It says that the second payment was made on the basis of setting a trap to catch the fraudster, which it didn't feel was a convincing explanation. It felt Mr F had reservations about the situation by initially wanting to pay £1.

It adds that it provided Mr F with 'high friction' warnings at the time that he was making the payment.

But I don't think Monzo has been able to establish that it may choose to not fully reimburse the payment Mr F made under the terms of the CRM Code. I'm not persuaded any of the listed exceptions to reimbursement under the provisions of the CRM Code apply in the circumstances of this case.

Did Mr F ignore an effective warning?

The CRM Code says that when a firm identifies an APP scam risk in a payment journey, it should take reasonable steps to provide the customer with effective warnings, including actions for the customer to take to protect themselves from APP scams.

Having looked at Mr F's account statements and how his account usually ran, I think there were significant risk factors with the payment he was making. Mr F used the account infrequently and kept a low balance, often reducing it to zero. To move money in and then almost immediately pay it out again did stand out, especially given the funds were going to a payee that had only been created that day. It's unclear why a consumer would send multiple genuine payments to the same payee in quick succession when they could have sent the funds at the same time in one lump sum. I'm also mindful that there was a suspicious pattern of spending potentially emerging as the first payment had been initiated using a new device

that had only been added that day, but the second payment was being initiated minutes later from Mr F's usual device.

Having looked carefully at the circumstances here, I think Monzo was required to give an effective warning during the payment journey.

Under the provisions of the CRM Code, an effective warning must have (as a minimum) been understandable, clear, timely, impactful and specific. Beyond these minimum requirements, an effective warning must provide information that gives customers a better chance to protect themselves against being defrauded – otherwise it could not have been an 'effective warning'.

I've looked carefully at Monzo's 'high friction' warning screens that it says would have been shown to Mr F at the time he was making the payment to decide whether he ignored an effective warning. Mr F does recall this part of the payment process but explains he was coached by the fraudster into quickly moving past the information and to select the payment purpose "something else". It is not uncommon for a fraudster to persuade a victim to choose an alternative reason for payment deliberately to circumvent the bank's fraud detection system.

This means that Mr F did not see the warning most relevant to his circumstances – as he was directed to choose a different payment reason by the fraudsters. This is unfortunate in the context of preventing the scam, but I'm only able to assess the effectiveness of the information Mr F did see.

The information that was presented to Mr F at the top of the "something else" warning prompted him to consider whether a deal seemed too good to be true or not. This would not have resonated with him in the moment as it did not apply to the particular scam he was falling victim to.

Monzo has pointed out further down the "something else" warning it says that the name and phone number of legitimate companies can be 'spoofed' or faked. I can see why the bank considers that this relates, in part, to the scam Mr F fell victim to. It's clear from Mr F's submissions that he steadfastly believed he was talking to the bank because the fraudster had been able to replicate the bank's genuine phone number.

But the information in the warning does not really bring to life what safe account scams look like. It doesn't explain that fraudsters pose as banks and other genuine companies and apply pressure to convince their victims that the funds in their account are at risk if they don't move them to a safe account with urgency. Nor does it talk about the prevalence of this type of scam or explain how sophisticated the scams can be – it doesn't for example, explain that fraudsters often know personal information about their victims and use this as a tactic to convince them that they are genuine. Finally, the warning doesn't explain the potential consequences of continuing with an irrevocable payment.

Overall, I'm not satisfied that a reasonable person in Mr F's position would have appreciated the scam risk from the information Monzo gave. Mr F has told us he was convinced he was talking to his bank, and as a result followed every instruction the fraudster gave him. I think it's understandable in the circumstances that Mr M followed the instructions he was given and therefore moved past the warnings as the fraudster managed his journey through the payment. Customers tend to follow instructions from their bank, even more so when it comes to fraud.

It follows that I'm not satisfied that it can reasonably be said that the requirements of the effective warning exception under the CRM Code were met in the individual circumstances of this complaint. I am not persuaded the warning Monzo gave was impactful or specific enough for me to say that Mr F ignored an effective warning.

Did Mr F make the payment without a reasonable basis of belief?

It's not clear if Monzo is arguing that Mr F lacked a reasonable basis for believing he was making genuine transactions. In any case, I've considered whether Mr F held a reasonable basis for belief in making the payment, taking into account whether he actually did believe what he was told and whether that belief, taking into account his characteristics, was reasonable.

Having done so, I don't think it was unreasonable for Mr F to believe he was genuinely speaking to Monzo.

Mr F has said that the fraudster's telephone manner and the way it mimicked the bank's own procedures and processes was compelling. He has pointed out that the fraudster knew details about his banking, such as his last genuine transaction. He has also repeatedly highlighted the bank's genuine telephone number had been replicated, which absolutely convinced him that this was genuine contact from the real bank.

I'm also mindful that Mr F was being coached by the fraudster who knew step by step the actions he needed to take, which gave the caller credibility as they were able to describe the upcoming payment screens in a natural and knowledgeable way. I've also taken into account that Mr F was being put under time pressure to make a payment and the fraudster had given him a plausible reason to make a larger payment than he was comfortable with.

I accept that there were some factors here that ought to have caused Mr F pause for thought – such as why he was being told to select a different reason for the payment and why he was making payments to an account in a different name to his own, but it's really important to remember that this didn't happen in the cold light of day. I'm mindful that the convincing nature of these scams can often have a negative effect on a person's thought process and make them take steps that, in the cold light of day they might not otherwise take.

From what Mr F has said, I am not persuaded that his actions were as a result of carelessness or indifference to what was happening, but rather deference to an expert that he believed was trying to assist him. In following their instructions (which in hindsight were clearly designed to divert his attention away from warnings and concerns) he appears to have believed he was simply carrying out instructions in the most expedient way possible.

Monzo has suggested that Mr F's employment in cybersecurity would impact his knowledge and awareness of this type of scam, but Monzo's internal notes suggest that it did not ask Mr F to explain more about his job role and what it entails. I have done so, and he has explained that he is involved in internal computer network security assessments. I am not persuaded that Mr F's employment has given him knowledge sufficient to say that he ought to have realised he was speaking to a fraudster or that he was falling victim to a safe account scam.

Has Mr F been grossly negligent?

As I have explained earlier in this provisional decision, a finding of gross negligence would require a very significant degree of carelessness on Mr F's part. I am not persuaded his actions or inaction in this case goes far enough to meet that very high bar.

I've already gone into considerable detail to explain why I don't think Mr F's actions show a lack of care that goes significantly beyond what a reasonable person would have done in the same situation. I don't think he disregarded or acted with indifference towards the risk of his bank account being compromised and money being stolen. He genuinely believed he was speaking with his bank and that he had to follow its instructions in order to protect his money. It's because of this that Mr F didn't digest the surrounding detail on the magic link email – he simply followed the instructions of whom he believed to be his bank. And as I've already explained, in the circumstances, I don't think Mr F's belief was unreasonable. I think in similar circumstances a reasonable person would have acted in the same way Mr F did here.

Should Monzo have intervened to stop the payments?

Though I can see that Mr F didn't use his Monzo account like a current account, I'm still of the view that there was enough activity on the account in the six months prior to the scam for Monzo to recognise that the disputed payments were sufficiently unusual and out of character that it ought to have intervened and questioned them in order to try and protect him from financial harm from fraud.

Had it asked Mr F about the activity, I've seen nothing to suggest he would not have told Monzo what was happening, that it would have quickly recognised that he was falling victim to a scam and that the loss would have been prevented. The effect of this finding is limited, given I'm upholding the complaint, but it does mean that Monzo should pay interest on the second payment from the date of loss rather than the date it declined the claim under the CRM Code.

Mr F has provided evidence to show the money he transferred to Monzo came from his current account held at another bank. So I think 8% simple interest per year from the date the payment was made to the date of settlement would be appropriate redress here, less any tax lawfully deductible.

Responses to my provisional decision

Mr F responded to my provisional decision and said there were no final points that he wanted to make.

Monzo responded and did not agree with the proposed outcome. It said Mr F's act of forwarding on an email from his bank which he didn't open was a negligent act, regardless of who was telling him to do this and he should have at least reviewed the email before forwarding it onto the scammer.

It noted that whilst the phone number had been spoofed, this didn't outweigh the other concerns Mr F ought to have had for being suspicious about the calls he received. It said he moved his money from a non-compromised account into his Monzo account to facilitate the scam. It felt Mr F had strong evidence that the caller was the fraudster and no longer had any reasonable basis for belief the caller was who they said they were when the first payment left his account. It said it wasn't reasonable for Mr F to move the money into his Monzo account, give his bank details to a caller, see a £1,000 payment leave his account and then trust that caller and send money to that same account.

The bank emphasised it is required to provide warnings that are as specific as they can reasonably make them, based on the information available at the time of payment. It felt it was unfair to look in hindsight at the warnings and it was not possible for any bank to have a monitoring system that prevents every possible scam transaction. It pointed out that it needed to strike a balance between protecting customers whilst not being overly disruptive

in adding unnecessary friction to legitimate payment requests.

It said that transactions weren't significant in the wider scheme of payments that the bank sees on a regular basis and were not concerning enough to be blocked and investigated further. It said it would be disruptive to thousands of legitimate customer payment requests to expect the bank to pick up and intervene prior to processing payments like this.

As both parties have responded, I shall now reconsider the complaint.

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.

I've taken account of all that was on file before my provisional decision as well as the arguments put forwards since.

Having done so, I remain of the view that Monzo should refund the unauthorised payment of £1,000. Monzo has responded to say that Mr F's actions when forwarding on the email were negligent. But negligence isn't enough for me to fairly say that Monzo can hold Mr F responsible for this payment. For the reasons I've already explained in my provisional decision (which is included above to form part of this final decision), I don't think Mr F seriously disregarded an obvious risk when he, on balance, unwittingly shared sufficient details to allow the fraudster to transfer £1,000 out of his account. This means I do not consider that Mr F failed with gross negligence. It can be difficult for consumers to think clearly and rationally under the kind of worry and emotional pressure Mr F found himself under at the hands of the fraudster. I think a lot of people would have been fooled into doing the same or something similar in the heat of the moment. It follows that I don't think Mr F's actions when sharing the details that ultimately enabled a fraudster to access his account and make a payment fell so far below what a reasonable person would have done that they amount to gross negligence.

I also remain of the view that Monzo should refund the later payment of £1,400 that was authorised by Mr F. Whilst I acknowledge Monzo's position that Mr F ought to have found the situation suspicious, I remain of the opinion that Monzo has not given sufficient weight to the environment that the fraudsters created when assessing Mr F's actions. I am still persuaded it was difficult for Mr F to think clearly in the heat of the moment and I'm mindful the panic he has described feeling when he saw £1,000 had left his account was not an unreasonable reaction to the situation. I am persuaded that it did heighten the stress he was feeling. Fraudsters are masterful at creating urgent situations. From what I have seen, Mr F genuinely believed his money was at risk and his motivation when making the second payment was to try and protect it. I am not persuaded that Mr F missed or ignored any red flags that should have been obvious to him at that time. It can be easy, in the cold light of day, to critically reflect on exactly how events could have happened. It is likely that Mr F has also replayed the events of that day over and over again in his mind given how significant the loss of the money has been to him.

I am not expecting Monzo to be able to prevent every possible scam type as it unfolds.
I agree with the bank that it is not possible to prevent every scam, and also appreciate that it needs to strike a balance in order to not unduly delay legitimate payment instructions. But in this instance, Monzo should have identified an APP scam risk because of the significant changes to the way the account typically ran.

The CRM Code that Monzo has agreed to adhere to says that where firms identify APP scam risks, they should provide effective warnings to their customers. I have already assessed the information Mr F was presented with in my provisional decision and for the reasons I have previously explained, I not satisfied that it can reasonably be said that the requirements of the effective warning exception under the CRM Code were met in the individual circumstances of this complaint. I am not persuaded the warning Monzo gave was impactful or specific enough for me to say that Mr F ignored an effective warning. This means Monzo did not meet the obligations it has agreed to adhere to under the CRM Code.

Monzo has said that the payment Mr F was making was unremarkable in character and that it wasn't significant enough to warrant further intervention and challenge at the time it was being made. I can appreciate that a payment of £1,400 in and of itself isn't a remarkable amount of money for a customer to be spending at any given time. But transaction value alone isn't the only factor that the bank should take into account when deciding whether it ought to intervene in a payment. Monzo should be on the lookout for unusual transactions or other signs that might indicate that its customers were at risk of fraud, amongst other things. I think the activity that day was significantly out of character for the way Mr F's account typically ran. There were other risk factors evident, such as the creation of a new payee, a payment being instigated from a new device and money being moved in and then immediately moved on, which contrasted considerably to the way Mr F's typically ran. Taking those factors in conjunction with transactions that represented a departure from the type of spending Mr F typically did, I am persuaded the account activity ought to have triggered Monzo's fraud alert systems.

Putting things right

To put things right, Monzo should now:

- Reimburse Mr F for the £1,000 unauthorised payment
- Pay 8% simple interest per year on the sum from the date the payment debited Mr F's account until the date of settlement
- Reimburse Mr F for the £1,400 payment he made
- Pay 8% simple interest per year on the sum from the date the payment debited Mr F's account until the date of settlement

My final decision

My final decision is that I uphold Mr F's complaint about Monzo Bank Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 14 July 2022.

Claire Marsh
Ombudsman