DRN-4577615

The complaint

Mrs H, on behalf of Company N, is unhappy Metro Bank PLC ("Metro"), won't refund the money she lost whereby she sent money to an account held at Metro that she considers was as a result of an authorised push payment ("APP") scam.

What happened

The details and facts of this case are well-known to both parties, so I don't need to repeat them at length here.

In summary, Mrs H thought she was paying a legitimate company (whom I'll call "Company I") who would assist in providing services to raise capital for Company N through investors. Mrs H was also introduced to the director of Company I through a 'Local Director' at Metro.

Mrs H made a payment of £5,000 on 18 November 2022 and then a further payment of £20,000 on 21 November 2022. Both payments were made from Company N's bank account (held at another provider) to an account held at Metro.

Mrs H had concerns when no invoices for the initial payments were received, despite multiple requests, nor a 'term sheet' outlining the next steps of how the proposed capital will be raised through potential investors and the timeframe for it to be carried out. Mrs H became increasingly concerned when the director of Company I sought more information about Company N and its product. Mrs H concluded that Company I was only after its product and never intended to raise capital for Company N. She sought a refund from Company I, which it seemingly was willing to agree to, but it never carried this out and continued providing excuses until contact stopped in March 2023.

Company I was to be struck off 'Companies House' with a two-month formal notice given in the First Gazette in February 2023. Mrs H contacted Companies House in March 2023 to contest the strike off, given she was owed outstanding monies.

It was around this time Mrs H also contacted a professional representative who complained to Metro, where the receiving bank account was held.

Metro is signed up to the Lending Standards Board's voluntary Contingent Reimbursement Model (the "CRM Code").

The CRM Code was implemented to reduce the occurrence of APP scams. It sets out what is expected of the 'Sending Firm' when payments are made, which includes a consideration of whether a customer met their requisite level of care when making the payment. And it also sets out the obligations for the 'Receiving Firm' to prevent, detect and respond to the receipt of funds from APP scams in order to prevent accounts from being opened, or used, to launder the proceeds of APP scams. Where there is a failing by either the Sending Firm or Receiving Firm, they may be required to reimburse the customer. And the customer may also be required to share some responsibility for the loss.

From my understanding, Mrs H hasn't raised a complaint about Company N's bank – as the Sending Firm, as she considers Metro as the Receiving Firm should be liable for the loss.

Mrs H says Metro, as the Receiving Firm, should refund the loss as she considers one of its accounts was opened and used fraudulently and the recommendation to use Company I came from a 'Local Director' at Metro.

Metro, in its submissions to this service didn't agree that it was liable for the loss Mrs H incurred. In summary, it said that the funds Mrs H had paid into the account were utilised by the account holder prior to it being informed of Mrs H's concerns, so it was unable to return any funds. It also explained that it had complied with regulatory requirements when opening and managing the account. It accepted that Company N was introduced to Company I through one of its Local Directors – but said no promises or guarantees were made by the Local Director, and it was just an introduction as its Local Directors and Business Managers attend and also host networking events to help the community and businesses expand their networks.

One of our Investigators looked into things and didn't recommend that Metro do anything further. Overall, he was satisfied Metro had met the standards required of it under the CRM Code and wasn't responsible for Mrs H's losses as it couldn't reasonably have done more to prevent the loss. He was also satisfied it had responded appropriately to the notification of fraud it received.

Mrs H disagreed and asked for an ombudsman to review her 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.

First, to clarify, this decision focuses solely on the actions of Metro – as the Receiving Firm of the account to which Mrs H made the payments. Under the CRM Code Mrs H is also entitled to raise a complaint about Company N's bank as the Sending Firm.

Both parties in this case agree that Mrs H and Company N fell victim to an APP scam, so I don't need to make a finding of fact on that point here. Instead, I have looked to see whether Metro met its obligations in its capacity as a Receiving Firm and whether it could have reasonably prevented Mrs H's loss.

I'm sorry to disappoint Mrs H but I'm not upholding her complaint about Metro. I don't believe Metro has acted unfairly or unreasonably in its answering of the complaint. I'm satisfied Metro has demonstrated that it has met its requirements under the CRM Code and therefore isn't liable to reimburse the losses. I'll explain why.

Among other things, regulated firms receiving payments like Metro, are required to conduct their 'business with due skill, care and diligence' (FCA Principle for Businesses 2) and to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements.

Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship).

And, more generally given the increase in sophisticated fraud and scams in recent years, as a matter of good industry practice at the time, I think firms should reasonably have had measures in place to detect suspicious transactions or activities that might indicate fraud or financial abuse (something also recognised by the Banking Standards Institute's October 2017 'Protecting Customers from Financial harm as a result of fraud or financial abuse – Code of Practice').

And I'm satisfied that this good practice requirement meant not just looking out for situations where a customer might be the victim of fraud, but also situations where the customer might be the perpetrator of fraud or a money mule.

Also relevant in this case, as mentioned earlier, is the CRM Code that Metro has signed up to.

The relevant considerations for Receiving Firms under the CRM Code sets out the following:

> *"CRM Code: Payment Journey – Receiving Firm*
>
> *SF2 Receiving Firms should take reasonable steps to prevent accounts from being used to launder the proceeds of APP scams. This should include procedures to prevent, detect and respond to the receipt of funds from APP scams. Where the receiving Firm identifies funds where there are concerns that they may be the proceeds of an APP scam, it should freeze the funds and respond in a timely manner.*
>
> *Prevention*
> *SF2(1) Firms must take reasonable steps to prevent accounts being opened for criminal purposes.*
>
> *Detection*
> *SF2(3) Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds.*
>
> *Response*
> *SF2(4) Following notification of concerns about an account or funds at a receiving Firm, the receiving Firm should:*
>
> *(a) respond in accordance with the procedures set out in the Best Practice Standards.*
>
> *SF2(5) On identifying funds where there are concerns that they may be the proceeds of an APP scam, Firms must take reasonable steps to freeze the funds and, when appropriate, should repatriate them to the Customer's Firm. Where appropriate, this should be done in accordance with the procedures set out in the Best Practice Standards."*

In considering all of the above, and to determine if Metro met the standards required of it under the CRM Code, I have looked at whether Metro opened the receiving account correctly, whether there was anything in the way the account was being used that should have given Metro any cause for concern and finally; once notified did it act appropriately and in a timely manner. And if I consider there were failings in relation to any of the above, I have to consider whether Metro's acts or omissions fairly resulted in Mrs H's loss.

I would like to point out to Mrs H at this point, that while Metro has provided our service with information about the receiving bank account – it has done so in confidence. This is to allow us to discharge our investigatory functions and Metro has provided that which is necessary for the determination of this complaint. Due to data protection laws our service can't share any information about the beneficiary, the receiving bank account or any investigation and action Metro subsequently took. However, I would like to assure Mrs H, I have thoroughly reviewed and considered all the information provided before reaching my decision.

Prevention - The account opening process

To help decide whether or not a bank failed to prevent the loss of an APP victim when opening the beneficiary account, we would generally ask to see evidence that; it correctly followed its account opening procedures; carried out checks to verify the identity of the named account holder; and did its due diligence when opening the account.

I appreciate Mrs H has said she doesn't think Metro has followed correct procedures as an account was opened and was subsequently used fraudulently. But in the circumstances of this complaint, I'm satisfied that Metro carried out checks to verify the identity of the named business account / account holder and did its due diligence when opening the beneficiary account. There wasn't anything at the time that I think reasonably could've alerted Metro that the account it was opening would potentially be used fraudulently later on. So I'm satisfied Metro has taken reasonable steps to prevent the accounts being opened for criminal purposes and it didn't miss an opportunity to prevent Mrs H's loss when opening the account.

Detection - Account activity

The primary duty of a bank is to follow their customer's instructions and make payments as directed in line with the mandate – which is usually set out in the terms and conditions of the account. The CRM Code sets out that Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds. This ties in with long standing regulatory and legal obligations Banks and Building Societies have to monitor their business relationships and to be alert to other risks - such as fraud, which would include giving consideration to unusual and out of character transactions.

I've looked at the account history for the beneficiary account and I can't say there was any account activity that I think would reasonably have stood out to Metro as suspicious or significantly outside of what might be expected for an account of that type. I'm also satisfied there was no notification of fraud on the account prior to the payments Mrs H made into the account, nor any other red flags where it could reasonably be argued that Metro might have had sufficient grounds to suspect any potential fraud and refuse execution of their customer's payment instructions.

So, from what I've seen, I'm satisfied Metro has demonstrated that it has taken reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds. I also don't think Metro ought reasonably to have had concerns where I would have expected it to have intervened, so I can't fairly say that it could have prevented Mrs H's loss in this way either.

Response to notification of fraud

The Best Practice Standards set out that a Receiving Firm must take appropriate action, in a speedy manner, upon notification of APP fraud and notify the Sending Firm if any funds remain for recovery. Here, Metro was informed of what happened some months after the payments were made (through the representatives Mrs H had instructed to act on her behalf). I'm satisfied Metro took the necessary actions required of it and did so in a timely manner. Metro has confirmed no funds remained in the account that could be recovered as they had already been moved on / withdrawn from the account.

So, taking the above into consideration I'm satisfied, following Metro receiving a notification of APP fraud, it responded in accordance with the procedures set out in the Best Practice Standards. And I don't think I can fairly say Metro didn't do enough to respond to the alleged APP fraud.

Finally I note that Mrs H was introduced to Company I through a Local Director within Metro. Metro has explained that it has Local Directors and Regional Retail / Business managers regularly attend and/or host networking events with the aim to help the local community and businesses with expanding their networks. While I empathise with Mrs H at the unfortunate circumstances that followed – I can't fairly say that at the time of the introduction, Metro or the Local Director, would have had any concerns about Company I or that the director of Company I may not act in Company N's best interests subsequently.

Overall, I'm satisfied that Metro met the standards required of it under the CRM Code. I also don't think Metro could've done anything more as the Receiving Firm to have prevented the loss of Company N's money. And it responded appropriately once notified of the alleged fraud. So, it follows that I don't think they are liable to reimburse any of the loss under the CRM Code or otherwise.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H, on behalf of Company N, to accept or reject my decision before 22 March 2024.

Matthew Horner
Ombudsman