DRN-2675585

The complaint

Mr C complains, on behalf of W, that Metro Bank PLC won't refund a disputed transaction made from their business account.

What happened

Mr C is the sole director of W.

Mr C explains that a transaction for the amount of £6,641.76 was made from W's account on the 24 July 2019 which wasn't authorised. This transaction was a faster payment made via the Metro mobile app.

Mr C explains that in July 2019 he gave an investor, I'll call A, access to W's online banking via the mobile app. But due to a disintegration in Mr C's relationship with A he became concerned about A having access to W's internet banking. For this reason Mr C explains that on the 19 July 2019 he visited his local Metro branch and asked for his online banking to be reset. Metro asked Mr C the reason for this reset but instead of advising he'd shared his online banking details with A, and assisted him to download the mobile app, he advised Metro that he was aware it's important to regularly update your security. On the 19 July 2019 Metro reset W's password and security number. However Mr C says that on the 24 July 2019 A accessed W's online banking and carried out an unauthorised transfer of £6,641.76.

Mr C complained on behalf of W to Metro. Metro investigated and decided not to refund the disputed transaction. They thought that Mr C had authorised the disputed transaction and he'd failed to comply with the terms and conditions of his business account by sharing his online banking details with A. Metro explained that although they'd reset W's password and security details on the 19 July 2019 this wouldn't reset access to the mobile app.

Mr C wasn't happy with Metro's response so complained to our service.

One of investigators looked into W's complaint and thought that although Mr C had authorised the transaction – through sharing his details with A – Metro should have asked Mr C more questions when he attended the branch on the 19 July 2019 and concluded that they also needed to reset W's mobile app. He said Metro should refund W the disputed transaction plus 8% interest.

Metro didn't accept our investigator's opinion, in summary they said:

- Mr C shared the online banking details for W with A and therefore he authorised the transaction.

- Mr C's failed to comply with the terms and conditions of the account specifically '*It is your sole responsibility to monitor and control access to and use of your account'.*

As Metro didn't agree the case was passed to me for a decision. I reviewed W's complaint and came to a different conclusion to our investigator. I issued my Provisional Decision on

the 23 February 2021 giving both parties until the 10 March 2021 to respond with any further comments.

Metro didn't respond to my Provisional Decision.

Mr C responded and in summary said:

- When he visited the branch there was a good relationship between him and A therefore he had no need to need to mention any security issues to Metro.
- Just because he didn't mention it doesn't mean Metro shouldn't have taken their responsibilities seriously.
- He acted responsibly in attempting to protect the security of W's account.
- The two branches he visited weren't aware that resetting online banking didn't also reset the mobile banking app. If the branch staff didn't know, how could he be expected to know?
- Even if he'd explained the full reasons for his actions, Metro still wouldn't have known that online and mobile banking security are two separate processes and been able to successfully secure W's account.

As Mr C didn't accept my Provisional Decision I've reconsidered all the evidence and Mr C's response.

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 I've not changed the outcome I reached in my Provisional Decision. And I'll explain why below.

In my Provisional Decision I said:

I'm satisfied from the bank's technical evidence that W's correct online banking details were used to make the disputed transaction. But the regulations relevant to this case say that is not, on its own, enough to enable Metro to hold him liable. So I also need to think about whether the evidence suggests that it's more likely than not that Mr C consented to the transaction being made.

I'll realise this will be very disappointing to Mr C, but I'm satisfied on balance he did authorise the transaction, I say this because:

I've seen evidence from Metro that the transaction on the 24 July 2019 was a faster payment processed via the mobile app using a payee set up in February 2019. Mr C's explained that he assisted A to download the mobile app and gain access to W's account. Although A wasn't listed on the business account, I'm satisfied giving him access to mobile banking is effectively clothing him with apparent authority. When looking at the Payment Service Regulations 2017 this means that any transaction carried out by A after this point would be seen by the bank as being carried out by the authorised account holder, namely Mr C.

But it's important for me to consider Mr C's main argument here – namely that on the 19 July 2019 he visited a Metro branch and whilst carrying out another banking transaction asked for W's password and security code to be reset. I've considered what happened here in detail and it appears that both Metro and Mr C agree on the main events – unfortunately Metro haven't been able to provide notes for the branch visit. Essentially Mr C says that he

informed the member of staff he'd like to reset W's security details. The member of staff asked Mr C was there a particular reason for resetting his password and security code. And Mr C explained that he was aware it's important to regularly update your passwords.

Crucially, although he was asked why he wanted to reset his details Mr C didn't mention his concern about A. I'm satisfied if he had done so at that point it's highly unlikely A would have been able to carry out the transaction – and I need to take this into consideration. Mr C thought from this point onwards he'd protected access to his account, and internet banking, from A – but unfortunately A still had access via the mobile app. Our investigator explored this further with Metro – who provided evidence of their security reset if a customer asks for their online banking to be reset. There's no mention here of resetting the mobile app. I've seen the registration process for the mobile app – and it's clear here that the password and security code is needed – but once this has been set up Metro have explained this is no longer required. And all A needed to access the app was a four digit PIN code he'd previously set up or his fingerprint.

What I need to consider here is whether Mr C did enough to end the apparent authority he clothed A with. And I realise that Mr C will find this disappointing, but I don't think he did. I agree with his argument that Metro are the experts, and they should be aware that you wouldn't require the password and security code to access a registered mobile app. But, both parties now agree that Mr C was specifically asked why he wanted to reset his security credentials and instead of advising he was concerned about A he explained that he thought this would be best practice. I've thought about Metro's response here and their usual practice, and I don't think it's reasonable to expect them to consider resetting or blocking access to any previously downloaded apps. I say this because I wouldn't expect Metro to see a possible risk here. Mr C didn't tell the bank that he had concerns about A accessing his online banking or more importantly that he'd assisted A in downloading the mobile app. If he had done so then I'd have expected Metro to act on this.

For the reasons I've explained above, I'm satisfied that by giving A access to W's mobile app Mr C effectively gave A authority to make authorised transactions. And although Mr C attempted to end this authority on the 19 July 2019 his actions were not sufficient to terminate this.

Mr C responded with a number of additional points to my Provisional Decision, which I've considered below. I've not considered these individually, as I'm satisfied that Mr C's main points are he wasn't aware A was a risk to W when he visited the branch and how can he be expected to know that resetting his online banking wouldn't also reset the online banking app if the Metro staff weren't aware.

I understand what Mr C's trying to say here – but unfortunately once he gave A access to his online banking, and assisted him in downloading the mobile app, he was giving A the authority to transact on behalf of W. Whether he knew about a potential risk from A when he visited the Metro branch and reset his security doesn't impact on this. The key question – which I addressed in my Provisional Decision – is whether Mr C did enough to terminate this authority. Mr C argues that by visiting his local Metro branch and asking the staff member to reset his security details this was enough – and how could he possibly know that the mobile banking app wouldn't also be reset, and A would still have access. I realise this will disappoint Mr C but whether he knew the mobile app wouldn't be reset doesn't impact on my conclusions. Mr C gave A access to W's online banking and from that point on, until he informed Metro that he'd allowed A to download a mobile app or carried out sufficient actions which prevented A gaining access, A acted with his authority. I'm not satisfied it's Metro's responsibility to guess what Mr C was trying to achieve when he visited the branch that day. Or to take all reasonable steps, including resetting access to any mobile banking apps, to

prevent A gaining access when they weren't aware Mr C had shared his online banking details with him and allowed A to download the mobile banking app.

I realise this will disappoint Mr C but I'm satisfied that the disputed transaction was authorised by W. And it follows Metro are entitled to hold W liable.

My final decision

My final decision is I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask W to accept or reject my decision before 9 April 2021.

Jeff Burch
Ombudsman