complaint

Mr C, represented by Ms R, complains that Metro Bank Plc filed a Credit Industry Fraud Avoidance System (CIFAS) marker against his name. He says that he had nothing to do with fraudulent activity on his account, and that the marker is preventing him from getting another bank account. He wants Metro Bank to remove the CIFAS marker.

background

Mr C attended a branch of Metro Bank on 17 November and opened a bank account. He was accompanied by a friend who he'd met through online gaming. Mr C said he'd got talking to the friend about not having a bank account, and the friend had offered to meet and go with him to open one. Mr C said he'd not previously met the friend in person, but he'd been chatting to him online for about six months. He described the friend as someone he "*didn't know properly*".

In branch Mr C was issued with a debit card and security details and self-selected a PIN. He also downloaded the Metro Bank mobile banking app on to his phone (Device A). Later that day he withdrew the £10 he'd opened the account with from a cash machine.

The debit card was used to make a contactless payment to a transport provider on 21 November. Mr C initially said that wasn't him, and that he'd lost his card not long after opening the account – probably on 20 November. He reported his card lost and was issued with a new one on 2 December. Both cards had the same primary account number (PAN – the long card number).

On 2 December a payment of almost £500 was received into Mr C's account from another bank, I'll call D. Within minutes of the payment being received £250 was withdrawn from a cash machine. The rest of the money was sent to an existing payee using the mobile banking app on another mobile phone (Device B). That payee had been added to Mr C's account a few days earlier through the mobile banking app on Device B.

Metro Bank have explained that to register a new device for mobile banking someone would've needed Mr C's 12-digit customer number, his internet banking ID and password, and a one-time pass code (an OTP) sent to Mr C's registered mobile phone number. To add the new payee another OTP would've been needed along with several digits from the PAN on Mr C's card.

The following day Metro Bank received notification from bank D, who said their customer hadn't authorised the payment to Mr C's account. As a consequence, Metro Bank gave Mr C seven days' notice that they would be closing his account and filed the CIFAS marker.

Below I have set out a timeline of the significant activity related to Mr C's account.

Date Time	Activity
17/11/2018 12:17	Account opened – welcome email sent to Mr C including 12-digit customer number needed for both mobile and online banking. Debit card issued and PIN self-selected in branch by Mr C.
12:25	Mobile app registered on Device A.
13:26	Fingerprint validation added to Device A.
15:20 – 19:43	Mobile app accessed on Device A four times using both PIN and fingerprint validation.

21/11/2018	Debit card used to make a contactless payment to a transport provider.
21:46	Mobile app accessed on Device A using fingerprint validation.
27/11/2018 17:37	Mobile app accessed on Device A using fingerprint validation.
17:58	Mobile app registered on Device B.
19:57	Mobile app accessed on Device B using PIN validation. New payee added to account.
29/11/2018 22:01	Mobile app registered on Device C.
30/11/2018 15:23	Fingerprint validation added to Device C.
02/12/2018 13:51	Mr C reported his first debit card lost and was issued a new one.
14:19	Mobile app accessed on Device C using fingerprint validation.
15:53	Mobile app accessed on Device B using PIN validation.
15:58	£493 credited Mr C's account.
15:59	Mobile app accessed on Device B using PIN validation.
16:01	£250 withdrawn from cash machine with debit card and PIN.
16:04	Mobile app accessed on Device B using PIN validation.
16:05	£240 faster payment made to payee added on 27/11/2018
16:06	Mobile app accessed on Device C using fingerprint validation.
16:10	Mobile app accessed on Device B using PIN validation.
03/12/2018 15:13	Bank D contacted Metro Bank to inform them that their customer had been the victim of fraud.
14/12/2018	Mr C received a letter from Metro Bank advising him that his account would be closed, and he reported his second card lost.

What Mr C told us

Mr C has explained that when he was opening his bank account in branch, he was asked by the member of staff to write the numbers and passwords he would like to use as his PIN, mobile banking logins and online banking logins on a piece of paper in full view of his friend. He's said he was offered no privacy. The member of staff then asked Mr C to set up mobile banking in front of his friend. He said he later let the friend use his mobile phone (Device A) for social media.

Mr C said that after he'd lost the first debit card, he took the same friend back to branch to get a new card on 2 December. Mr C suggested that it was his friend who had added the new payee to the account via the mobile banking app, and also taken his debit card to make the cash withdrawal.

Mr C said that when he arrived home on 2 December, he realised he'd lost the second card as well. But he was too embarrassed to tell anyone and couldn't block it because his mother had taken his mobile phone away. He's also said he wasn't overly concerned because he thought he'd lost it within the house.

During conversations with our investigator Mr C's representative, Ms R, offered another explanation for how his banking and security details could have been compromised by a third party. She said that he'd taken the new account welcome pack and the piece of paper with various security information on it to a fast food restaurant and taken a picture of his food

which he then posted to a social media website. The security information was accidentally visible in the picture. When this was pointed out to Mr C by one of his friends, he deleted the picture. Ms R said that before the picture was deleted someone could have made a record of the security details.

Mr C initially agreed this was possibly how his banking information had been compromised. More recently, however, Mr C has said he thinks it's likely it was the friend who went with him to open the bank account who carried out the fraud. He's said:

- His friend would have seen his 12-digit customer number on the day he opened the bank account as it was "in clear view for him";
- He wrote down his potential PIN for his card and mobile banking app, and a password, on a sticky note while he was opening the account;
- As he was unaware of the dangers of fraud, he used the same sequence of four digits as the PIN for unlocking his phone, for accessing his mobile banking app and for using his card;
- He used the same password for accessing his bank account as he used for his gaming account;
- He'd given his gaming account password to his friend in the past as he'd met him through online gaming;
- His friend had access to his mobile phone and knew his PIN;
- He allowed his friend to use his mobile phone on 27 November for social media and listening to music;
- He thinks his friend signed into mobile banking on another phone and set up the new payee on 27 November – receiving and deleting the OTPs from Mr C's phone before giving it back to Mr C;
- He recalls telling his friend on 2 December that he'd lost his card, and the friend asking to come along when he collected a new one;
- On the way home on 2 December his friend asked to use his phone again;
- His card was missing when he got home on 2 December – he's not sure how his friend managed to take it; and
- He didn't report his card missing because he didn't think anyone could do anything as he had no money in the account, and he felt embarrassed.

Mr C has also told us that he only knows the friend's name. He doesn't know where he lives or what school or college he went to at the time. He said he didn't report this friend to the police as he had no information on them, and even found he was blocked from finding their gaming account again.

What Metro Bank said

Metro Bank have explained that Mr C would have been asked to select a PIN in branch on the day that he opened his account. But he would not have been encouraged to write it down. They said the debit card is printed in branch and customers are taken to a PIN entry machine to choose their own PIN. They've also said that the 12-digit customer number is included in the welcome email customers receive once their account is successfully opened, not handed to the customer in branch.

Metro Bank say it's unlikely a third party became aware of all the information necessary to carry out these transactions without Mr C's knowledge and involvement.

Our investigator's view and Metro Bank's response

Our investigator upheld Mr C's complaint. He said it was possible Mr C's friend, who'd accompanied him on the day he opened the account, had seen his PIN and card details. He also said it was possible the same friend had set up the new payee. Overall, he didn't think Metro Bank had explored the possibility that someone had taken Mr C's card and security details to use them without his knowledge. He didn't think Metro Bank had enough evidence to satisfy the criteria for filing a CIFAS marker, so he said it should be withdrawn.

Metro Bank said they were satisfied by the account activity that they'd met the requirements of CIFAS and that they didn't need to make further enquires of Mr C before taking the decision to file the marker. They asked for the complaint to be passed to an ombudsman for a decision.

my provisional decision

I issued a provisional decision on 1 May 2020. I said I wasn't minded to uphold Mr C's complaint. I explained:

"*Metro Bank applied the CIFAS marker because bank D said their customer didn't authorise the payment made to Mr C's account. So I've looked at whether it was fair of Metro Bank to apply the marker, based on the evidence and what the rules say about applying such markers.*

When a business is a member of CIFAS it can record a marker against an individual customer when that customer has used their account fraudulently (a 'misuse of facility' marker). This type of marker will stay on record for six years and will usually make it difficult for a customer to take out new financial products.

If a business decides to file a marker it must have evidence and meet CIFAS's standard of proof. To meet the standard of proof the business must have: reasonable grounds to believe that a fraud or financial crime has been committed or attempted; and clear, relevant and rigorous evidence such that the business could confidently report the conduct of the customer to the police. The conduct of the customer must also meet the criteria of the type of marker (in this case, the criteria for the 'misuse of facility' marker), and the business must usually have rejected, withdrawn or terminated a financial product on the basis of fraud. This means that a business shouldn't apply the marker on the basis of its suspicions only.

Having reviewed Mr C's account of events and the evidence Metro Bank have provided, I'm currently satisfied that Metro Bank have sufficient evidence for the CIFAS marker to be recorded on his file. I say this for the following reasons:

- *Metro Bank have provided evidence to show the payment to Mr C's account on 2 December was reported by bank D as fraudulent;*
- *I think it's unusual for someone to open their first bank account in the company of someone they've never met and only know through online contact;*
- *I find it unlikely the friend who was present during the account opening process observed and remembered Mr C's account number, sort-code, 12 digit customer number, debit card PIN, mobile banking passcode and other security details – I think it's more likely that if a third party was involved here, Mr C gave them that information;*

- *I also find it unlikely the friend got hold of the first debit card between 17 – 20 November (they'd have needed it for the PAN to set up the new payee) without Mr C's knowledge;*
- *Whilst it's possible that the friend remembered enough information to download the mobile banking app on to a second device, and had the first debit card in his possession, I see no reason why that friend would have waited 10 days before registering the app on Device B;*
- *I note that the mobile banking app was registered on Device B within 30 minutes of Mr C accessing the app using his fingerprint on Device A;*
- *Mr C didn't access the app on Device A again after the app had been registered on Device B, suggesting he was aware it had been registered on Device B;*
- *Mr C did not report his first debit card lost or stolen until 2 December;*
- *It seems to me an unlikely coincidence that the fraudulent funds were credited to Mr C's account on the same day he collected his second debit card in branch;*
- *I don't think it's likely Mr C would have taken the same friend, someone who he barely knew and hadn't met face to face before 17 November, to collect his second debit card on 2 December unless the intention was to give it to him;*
- *I don't find it plausible that the friend acquired the second debit card without Mr C knowing; and*
- *Mr C didn't report his second debit card lost until he received notification of Metro Bank's decision to close his account – this suggests to me that he knew who had it.*

Overall, I don't think it's plausible that a third-party fraudster achieved what happened here without Mr C's knowing involvement.

Taking everything into account, I find that Metro Bank have met the burden of proof required by CIFAS to file the marker. So, I'm not going to ask them to remove it."

responses to my provisional findings

Mr C didn't agree with my provisional findings. He made the following points:

- He took the friend with him to open his first bank account because that person was one of his only friends;
- The friend wouldn't have needed to remember all the security information, as they could easily have taken a picture with their mobile phone of what was laid out on the table;
- The friend would've been able to access the welcome email containing his 12-digit customer number on Mr C's phone;
- He did not lose his first debit card shortly after opening the bank account – he lost the first card the day before he reported it a lost;
- There's a possibility he accidentally made the contactless payment to a transport provider on 21 November;
- He didn't think it was important to say before, but after he opened the bank account he saw the friend nearly every day and the friend had access to Mr C's phone whenever he wanted;
- He saw the friend on 27 November and logged on to online banking "to show him that the card was used on [public transport]" – that's the reason he accessed the app using his fingerprint on Device A, 30 minutes before the mobile banking app was registered on Device B;

- The reason he didn't access the app on Device A again after the app had been registered on Device B, was that he had exams during this period and his mother would "*regularly take his phone*";
- He took the friend with him to collect his second debit card as he didn't want to go alone;
- The friend could've taken the second debit card from his pocket while they were on the train back home;
- He didn't report the second debit card "stolen" because his mother took his phone that day and didn't give it back to him until a while after his exams had finished; and
- He was naïve and used by a person he "*once called a friend*".

I asked Mr C about why he'd changed his story about when he'd lost the first debit card. He said he thought it would help his case if he said he'd lost his card shortly after opening the account, but he actually remembered having it in his wallet after 20 November 2018 until he noticed it was missing on 1 December. He added that his friend had been persistent about meeting up on 30 November too.

With regard to why he had allowed the friend to use his mobile phone freely, Mr C said he let this happen because sometimes the friend's mother took his phone, and also the friend's phone was 'slow'. He thought if he said no the friend would leave. He also didn't think the friend would be able to do anything with his banking app. He didn't realise the friend had figured out that his phone PIN and mobile banking passcode were the same.

Metro Bank had no comments on my provisional decision.

my findings

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, although I know that Mr C will be deeply disappointed by the outcome, I do not uphold his complaint.

For all the reasons set out in my provisional decision, which I have summarised above, I still think it's more likely than not Mr C was knowingly involved in what happened.

Mr C remains adamant that he never gave any banking security information or his debit cards to a third party. He says the friend acquired all that was necessary to withdraw the fraudulent funds without his knowledge or involvement. But I don't find Mr C's version of events credible.

There have been some significant inconsistencies in what Mr C has said. In response to my provisional decision he's said the card payment to a transport provider on 21 November *was* probably him because he didn't lose that card until the day before he reported it lost. But in his first letter to Metro Bank after their decision to close his account, he'd said:

"*The issue started when I lost my card on the 20th November ... After blocking the card on the 23rd November, I checked my account balance and discovered my card was used to make a transaction to* [a transport provider] *with an amount of £5.50. I never made this transaction as I am a teen with free transport …*"

He's now explained that that wasn't the truth. However, if Mr C did, as he now says, have the first debit card in his possession until 1 December, I think that makes it even more likely he was involved in the adding of the new payee on 27 November.

Mr C's version of events is that at 17.37 on 27 November he logged on to his account via the mobile app to show the friend that the card had been used on public transport. Mr C says the friend must have then, 21 minutes later, downloaded and registered the app on Device B.

To do this the friend would've needed Mr C's 12-digit customer number, his internet banking ID and password, and an OTP sent to Mr C's registered mobile phone number. That would have required a lot of activity with Mr C's phone that I think he'd have noticed – the friend would have need to search Mr C's emails for the welcome email containing the 12-digit customer number and receive and delete an OTP.

Later, to add the new payee, the friend would have needed to access the mobile app, obtain another OTP from Mr C's phone and several digits from the PAN on Mr C's card. As Mr C now says he still had this card on that date, the friend would have needed to take and replace the card without Mr C noticing. I don't think that's likely.

Another inconsistency in Mr C's story is that he originally told us his details had been compromised when he posted a picture of his food to social media with his banking details in the background. It wasn't until later that Ms R submitted a letter explaining another way that the transactions could have taken place. That letter set out how the friend had been present at the opening of the account and could have gained enough information at that time to later access the account. It also said the friend had used Mr C's phone on occasion for a "*short while*".

Mr C has since said that the friend had free access to his phone. But I think it would be unusual to give a person you barely know such access, just as I remain of the view that opening your first bank account in the company of a virtual stranger is an unusual thing to do.

In my provisional decision I said the fact Mr C didn't access the app on Device A again after the app had been registered on Device B, suggested he was aware it had been registered on Device B. Mr C says that's not the case. He's explained that he didn't open the app on his phone again because his mother would "*regularly take his phone*".

But Mr C did have his phone at times after 27 November. It's unlikely to have been in his mother's control on 29 November when the phone would have received an OTP as part of the process for registering the mobile app on Device C. He also had it on 2 December when he went to collect his new card.

If Mr C had been unaware of the existence of the app on Devices B and C, I think he'd have accessed it on Device A at some point after 27 November if only to check the security of his account when he realised he'd lost the first debit card. Before 27 November the audit shows he accessed the mobile banking app on Device A at least once a day and, on one day, 14 times. I don't think going from that level of access on Device A to nothing can be explained by the phone being taken away by his mother more often. I still think Mr C stopped using the app on Device A because he knew about Device B.

Finally, I remain of the view that it's unlikely Mr C would have taken the same friend, someone who he barely knew and hadn't met face to face before 17 November, to collect his second debit card on 2 December unless the intention was to give it to him. I also find it unlikely that the friend acquired the second debit card without Mr C's knowledge so quickly

after they collected it. And I'm not convinced by Mr C's reasons for not reporting it lost until 14 December.

So overall, I think Mr C's was involved in the fraud here. I think it's more likely than not he accepted the fraudulent money into his account and either withdrew and moved that money on himself, or he provide a third party with his bank details so that they could complete the transactions. It's of course possible that Mr C was persuaded to do this by a third party, rather than the instigator of what happened. I've asked Mr C was targeted and convinced by others to become a 'money mule', but he says not.

Taking everything into account, I find that Metro Bank have met the burden of proof required by CIFAS to file the marker. So, I'm not going to ask them to remove it."

my final decision

My final decision is that I do not uphold Mr C's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 1 August 2020.

Beth Wilcox
ombudsman