DRN-3688075

The complaint

Mr B complains that Metro Bank PLC won't reimburse him for the money he lost when he fell victim to an 'authorised push payment' ("APP") safe account scam.

What happened

The details of this case have been clearly set out by our Investigator. As such, the facts are well-known to both parties, so I don't need to repeat them at length here. I'll recap the key points and focus on giving reasons for my decision.

In December 2021, Mr B lost his debit card and noticed some transactions on his account that he didn't make, which he reported to Metro. A couple of days later, Mr B received a text message, from what appeared to be Metro, asking if he'd attempted a transaction. As Mr B hadn't attempted the transaction, he replied 'N' to the message.

Shortly after this, Mr B received a call from somebody claiming to be from Metro, saying that his account had been compromised. The incoming call seemed to come from Metro's genuine telephone number. The caller told Mr B that his accounts were at risk and he needed to move his money to a 'new account' to protect it.

Mr B said that initially alarm bells were ringing. But he's said the caller was able to provide personal information about him, including his mother's maiden name, details of transactions on his account and his address, which he thought only his bank would know.

Mr B has said the call lasted for over an hour and a half. He added that, to begin with, the caller told him that they would start the 'new' account set up process, but that he could go into a Metro branch to complete it. But that then the caller changed this, saying that trojans could get his money at any point, so he had to move it straight away.

Mr B was instructed to transfer funds from his Metro account to a friend's account, to get the money out of the account straight away. The caller told Mr B from there it could then be sent, by his friend, to another of Mr B's accounts and then onto his 'new' Metro account. Believing everything to be genuine, Mr B went ahead and made four payments, totalling £9,800, to a friend's account. A breakdown of the payments he made is listed below;

16 December 2021	£2,500
16 December 2021	£2,500
16 December 2021	£2,500
16 December 2021	£2,300

Mr B's friend then sent the money back to him, via an account Mr B held with another provider, and from there the money was sent to the 'new' account, that the caller had provided details for. But unknown to Mr B at the time, he had been speaking to a fraudster and had sent his money to an account they controlled. Mr B has said £9,700 was lost to the fraudster.

Mr B realised he'd been scammed when, after the payment had been sent to the account details provided by the fraudster, the line went dead and he lost contact. Mr B contacted Metro to report what had happened. Metro investigated Mr B's fraud claim and considered its obligations to provide him with a refund. Metro is a signatory of the Lending Standards Board's (LSB) Contingent Reimbursement Model (CRM) Code which requires firms to reimburse customers who have been the victims of APP scams like this one in all but a limited number of circumstances.

Metro issued its final response on 7 January 2022, not upholding Mr B's complaint. In summary it didn't think it was liable given the circumstances of what happened, this was because Mr B had sent the money to a friend's account and so Metro said the payments were legitimate. It added that in this instance, it didn't think the payments fell under the CRM code.

Unhappy with Metro's response, Mr B then brought his complaint to our service and one of our Investigator's looked into things. It was our Investigator's view that the complaint should be upheld. In summary our Investigator thought the payments were covered by the CRM code. She didn't think Metro had established that it shouldn't reimburse Mr B under the CRM code. Our investigator also thought Metro ought to have identified that the payments Mr B made were unusual and suspicious and, coupled with Mr B raising a fraud on his debit card just a couple of days before, Metro ought to have made further enquiries, before allowing the payments to be made. Our investigator recommended Metro should refund Mr B the money he lost, along with interest.

Metro didn't agree with our Investigator's view. As an agreement couldn't be reached the complaint has now been passed to me for a 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.

Metro is a signatory of the CRM Code, which requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr B has fallen victim to, in all but a limited number of circumstances.

I note that Metro has argued that the CRM code doesn't apply, as Mr B had made the payments to a friend. But I don't agree, the funds that were ultimately lost to the fraudster belonged to him – they just passed through his friend's account on the way to the fraudster. This is a tactic used by fraudsters to make it harder for banks to identify a scam risk, and to make it more difficult for banks to trace and recover their victim's funds. I think that Metro, with its industry knowledge of fraud, ought to be aware of this.

In any event, the LSB has confirmed that the CRM Code includes cases, such as this one, where a victim was tricked into sending money to a fraudster's account via a family member or friend's account and the funds are now lost.

I'm satisfied that Mr B's complaint falls within the scope of the CRM Code. With this in mind and having considered things carefully, I'm satisfied that, adhering to the CRM Code, Metro should have refunded Mr B the money he lost. I'm not persuaded any of the permitted exceptions to reimbursement apply in the circumstances of these payments. I'll explain why.

Did Metro present Mr B with an effective warning?

The CRM Code requires a firm, where it identifies an APP scam risk in the payment journey, to take reasonable steps to provide the customer with effective warnings. This should include appropriate actions for customers to protect themselves from APP scams. The CRM Code requires firms to consider payments instructed against normal transactional data and customer behaviour.

Metro has acknowledged that it didn't provide Mr B with a warning during the payment journey. It said Mr B's payments were sent to an existing beneficiary, that had been set up on his account in 2018, at which time effective warnings were not in place. It added that Mr B had also made payments to his friend prior to the payments that ultimately ended up with fraudsters.

I appreciate what the bank has said about the payment going to a known payee. But having looked at Mr B's account statement, I can see that the payments made weren't typical of how the account usually run. In the months leading up to the scam I can see that, more typically, the account was used for much lower value card purchases, direct debits, cash withdrawals and 'account to account' transfers. The payments which ended up with the fraudster, were made in quick succession, immediately followed a large transfer into the account from Mr B's savings account and cleared almost the entirety of the balance, which can point to fraudulent activity. So, I think there was enough going on here to fairly and reasonably have expected Metro to have provided Mr B with an effective warning, despite the payment destination.

The bank acknowledges that it didn't provide Mr B with an effective warning, so I'm not persuaded that it can rely on this exception to reimbursement.

Did Mr B make the payments with a reasonable basis for belief?

Overall, I'm satisfied that Mr B had a reasonable basis for belief in this case;

- When Mr B received the call from the fraudster, he had already become aware that he had fallen victim to a fraud on his debit card and was therefore already on alert that his details were compromised. I can understand why, in the moment, this led Mr B to be more susceptible to believing his accounts could be at risk.

- Mr B checked the phone number he was being called from while on the phone to the fraudster and saw it was a genuine Metro number. I think it's important not to underestimate the impact this would have had on Mr B's decision making going forwards, given this reassurance he was genuinely speaking to his bank. Mr B wasn't advised throughout this scam that fraudsters can spoof genuine phone numbers.

- The fraudsters were able to provide a number of pieces of personal information to Mr B, that I think he fairly and reasonably only thought would have been known to his bank. Including his memorable password and details of transactions that had taken place on his account.

- I've considered, in the circumstances of this case, the fact the fraudster has created an environment where Mr B thought he had to act quickly to protect his accounts from an attack. With the benefit of hindsight and the removal of the pressured environment, it's easier to identify elements where Mr B may have had an opportunity to ask further questions. But 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.

Considering everything, the fraud was sophisticated and overall, I'm not persuaded that Metro has shown Mr B didn't have a reasonable basis for believing he was making genuine payments, or that he ignored an effective warning. I therefore consider Metro should provide a full refund to Mr B of his losses.

Could Metro have done anything else to prevent the scam?

For reason's explained earlier, I think the payments Mr B was making were unusual and suspicious, when compared to how he typically ran his account. This, coupled with Mr B having contacted Metro shortly before regarding another fraud matter, leads me to conclude that there was enough going on that Metro ought to have had concerns that Mr B may have been at risk of financial harm. Considering this, I think it ought to have intervened at the point Mr B transferred nearly £10,000 from his savings account and made the first payment, for £2,500.

Had Metro intervened at this point, as I think it ought to have done, I think it would have made the difference and I think the fraud would have come to light. I say this as Mr B hadn't been coached by the fraudster on what to say if his bank had of intervened, as can often be the case with scams, so I think he would have answered any questions Metro put to him freely. And given the concerns Mr B has said he had himself, when he very first received the call, I think the scam would have quickly come to light and the loss would have been prevented.

For clarity, my findings that a further intervention from Metro is more likely than not to have prevented the payments being made, has a limited impact on the outcome of this complaint, given I've decided Mr B should've been reimbursed under the provisions of the CRM Code. The impact relates to the interest payable only.

Putting things right

For the reasons explained above, Metro Bank PLC should now;

- Refund Mr B the money he lost, being £9,700.

- Pay interest on this amount, at the savings account rate, from the date the payments were made, to the date of settlement.

My final decision

My final decision is that I uphold this complaint against Metro Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 7 March 2023.

Stephen Wise
Ombudsman