DRN-3468269

The complaint

Mr B brings this complaint on behalf of A – a limited company. Mr B is unhappy that Metro Bank Plc ("Metro Bank") hasn't reimbursed all of the money he transferred to a scammer.

What happened

Mr B was contacted by a scammer pretending to be from his internet provider. They told Mr B his IP address was being hacked and directed him to view information online that evidenced the attempts the hacker had made to access his network. They said any apps or websites he used online were at risk including his bank account and he needed to move his money to a safe account.

The scammer instructed him to download applications to his phone, one of which allowed the scammer to 'mirror' his phone screen and see his information. The scammer instructed him to start moving money from his business bank account to safe accounts that had been set up with another bank. They told him he needed to move the money to several different accounts under code names. Within 30 minutes Mr B made the following transfers, each to different beneficiaries:

28 November 2020 11.28 am	£2,500
28 November 2020 11.33 am	£2,500
28 November 2020 11.47 am	£1,242.09 (unsuccessful)
28 November 2020 11.52 am	£2,500
28 November 2020 11.58 am	£2,500
28 November 2020 12.00 pm	£1,100.09
Total	£11,100.09

Metro Bank hasn't explained why the third payment was unsuccessful, but from what I've seen it didn't contact Mr B about this or prevent him from making further payments from the account.

I issued a provisional decision earlier this year upholding the complaint in part. I felt the 50% Metro Bank had already refunded to Mr B was reasonable, but I thought it needed to pay additional interest on this amount.

Mr B responded and said he felt Metro Bank ought to have done more to stop the payments being made. He felt the other high value transactions on his accounts weren't normal activity on his account, they were one off payments made for specific purchases. And whilst he thought he maybe should've been more vigilant he explained how the panic he felt when he made the payments and the fact that he was caught off guard effected his judgment.

Metro Bank responded to the decision and confirmed it had no further comments for me to consider.

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 have considered both parties' responses to my provisional decision. Having done so, my decision remains the same. For completeness, I have set my provisional decision out below and addressed the parties' arguments within it to form my final decision.

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.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

However, where the consumer made the 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.

When thinking about what is fair and reasonable in this case, I've considered whether Metro Bank should have reimbursed A in line with the provisions of the CRM Code it has agreed to adhere to and whether it ought to have done more to protect A from the possibility of financial harm from fraud.

There's no dispute here that Mr B was tricked into making the payment. He thought he was moving money to protect it. But this isn't enough, in and of itself, for A to receive a refund of the money under the CRM Code. The Code places a level of care on Mr B too.

THE CRM CODE

Metro Bank has signed up to, and 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 Metro Bank 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

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

Metro Bank has accepted it didn't provide Mr B with any warnings in this case. And, I think from the second payment Mr B made to scammers it was obliged to do this. I say this

because when he made the second payment of the same amount within a short space of time Metro Bank ought to have recognised unusual activity that might've been indicative of a scam. As it failed to meet its requisite level of care under the CRM code, it's reimbursed A for 50% of its loss.

It's now for me to decide whether I think Mr B had a reasonable basis for believing what he was told by the scammers when he made the payments he did and therefore met his requisite level of care.

Did Mr B have a reasonable basis for belief?

Having considered what Mr B has told us about his interaction with the scammers very carefully, overall, I'm not persuaded he did have a reasonable basis for believing what he was told. I understand that the nature of scams like this one are that scammers skilfully apply pressure to their victims and create a sense of urgency. But, I also think there were several points where Mr B reasonably ought to have questioned what he was being told. I say this because:

- The scammers told Mr B they were calling from his internet provider and they could see his bank accounts were at risk. But it's not clear how an internet provider would have access to A's bank accounts and banking security information. And it's not clear why he didn't question why he would be hearing his bank account was at risk from someone who wasn't calling from his bank.
- The scammers asked Mr B to move A's money to safe accounts it had set up under code names. But it's not clear why he believed his internet provider had the capability of setting up 'safe accounts' given it isn't a bank and doesn't offer any banking facilities.
- Mr B had said the scammer knew a specific number from his router. When questioned further by our service he's said they knew the product number on his router rather than one of the numbers unique to him. It's not clear if he checked this during his call with the scammer. It doesn't appear the scammer had any other personal information about him that offered reassurance they were who they said they were and it doesn't appear Mr B asked for any reassurances or tried to check. And although I understand they said they were calling from his internet provider and they knew who this was, it doesn't seem it would be difficult for someone to guess Mr B might've been a customer of one of the UKs largest providers.
- The evidence the scammers used to convince Mr B A's accounts were at risk appears to have been directing him to external websites. They also told him to download software that allowed them to view and access his computer, seemingly without any plausible explanation as to why he needed to do this. Although I do understand he was worried and felt under pressure, I think he reasonably ought to have attempted to verify what he was being told before he started to make the payments he did.

I do understand that scammers use tactics to panic and confuse their victims. And although I have taken this into account here, I still think Mr B reasonably ought to have questioned some of what he was being told before proceeding to make the payments he did.

Overall I don't think Mr B did have a reasonable basis for believing what he was told by the scammers.

Could Metro Bank have done anything to have prevented the scam?

Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I think Metro Bank should fairly and reasonably:

- Have been monitoring its accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.

- 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). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.

- 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.

I've thought about the transactions in this case and whether I think they ought to have prompted further intervention from Metro Bank.

This account wasn't Mr B's personal account, it was one he used for business purposes. In the six months leading up to his payments to the scammer I can see he made a payment of £5,000 in June 2020 and a payment of £14,000 in October 2020. The payments Mr B made to scammers were much lower than these amounts so wouldn't reasonably have seemed significantly unusual as I think they fit within the general use of A's account. And whilst Mr B has pointed out the specifics of what these payments are for, they were still payments he legitimately made from A's account and created a pattern of behaviour.

That said, Mr B transferred over £11,000 out of A's account to five new payees within half an hour. And whilst I accept that when running a business account it is likely the case new payees will be added, I think this many transactions of identical amounts to this many payees in such a short space of time ought to have raised concerns with Metro Bank as I think it's indicative of a scam. Particularly as these transactions totalled almost the entire account balance.

By the time Mr B made the third payment to scammers I think Metro Bank reasonably ought to have stopped the payment and intervened by asking Mr B for further verification. I say this because it was the third payment of £2,500 within around 20 minutes with one failed transaction of over £1,000 in the middle.

I think Metro Bank reasonably ought to have asked Mr B probing questions about the payment including what it was for an who it was to before it was sent. I haven't seen any reason Mr B wouldn't have been honest about what he was doing – moving the money to a safe account. Afterall, he didn't suspect anyone at the bank as he'd been told by the scammers a hacker was the problem. So I think the scam would've been uncovered straight away by Metro Bank staff, who I'd reasonably expect to be trained to recognise and be on the look out for common scams like this one.

Had Metro Bank intervened Mr B wouldn't likely have made the last three payments to the scammers. So I think it needs to pay additional interest on these three payments as outlined below.

Putting things right

- As Metro Bank has already reimbursed A for 50% of its loss I don't think it needs to reimburse A for anything more.

- However, as I think it ought to have intervened when the third payment was made and likely would have been able to prevent the payments being made from this point, it should pay interest at the simple rate of 8% per year on this amount from the date of payments (28 November 2020) to the date of settlement.

Based on the account statements available it seems that the money was paid to scammers from A's business account and likely would've remained there for general use had the money not left the account which is why 8% is the appropriate rate of interest in this case.

My final decision

I uphold this complaint in part. Metro Bank Plc needs to pay A the redress outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask A to accept or reject my decision before 6 June 2022.

Faye Brownhill
Ombudsman