DRN-4221038

Complaint

Mr Y is unhappy that Metro Bank PLC didn't reimburse him after he fell victim to a scam.

Background

Mr Y's son has two accounts with banks other than Metro. In November 2021, his son received a phone call from someone who claimed to be an employee of the fraud team with one of those banks. Unfortunately, it subsequently transpired that this phone call hadn't come from a genuine employee of that bank, but from a scammer.

As I understand it, Mr Y was with his son at the time of the call. His son was told that there was a security breach that affected his phone and, by extension, the apps he had on that phone connected with his bank accounts. Mr Y's son was told that someone had attempted to use his details to lease a car in a different part of the country to the one Mr Y lived in.

To convince him that he was genuinely communicating with an employee of that bank, the scammers sent Mr Y's son a text message which appeared in an existing chain of messages he'd received from the bank. Neither Mr Y nor his son were aware that scammers could spoof the origins of text messages in this way.

There was a second phone call with someone posing as an employee of his son's other bank. This call took place to persuade Mr Y's son that the banks were cooperating as part of a wider fraud prevention initiative. This phone call was also made using a spoofed number. Mr Y and his son were encouraged to search for that number online to confirm the authenticity of the call.

His son was persuaded to transfer money from his accounts to a safe account. He was then asked whether there were regular payments from his account to any other. There were multiple payments between Mr Y's account with Metro and his son's. He was told that this meant Mr Y's account was also at risk and he needed to transfer his funds to a safe account too.

I understand Mr Y said that he wanted to call Metro directly to check if this was true. However, he was told that the consequences of doing so could be significant and that the investigation into this criminal activity might be jeopardised. The scammers persuaded him that he needed to make the transfers. His son helped him do so by taking control of his device and authorising the payments. Once he realised he'd fallen victim to a scam, Mr Y notified Metro.

Metro investigated but didn't agree to reimburse him. It considered his complaint under the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code. It wrote:

> *Unfortunately, we felt that you did not take reasonable steps to check if the payment was genuine. For example, you were not contacted directly, you didn't question how [the other bank] would have had information about your Metro Bank account, and you didn't contact Metro Bank until after. In addition, in this instance, we did not consider ourselves liable as we provided you with an effective warning as per the CRM code.*

Mr Y was unhappy with the response he received from Metro and so he referred his complaint to this service. It was looked at by an Investigator who didn't uphold it. She wasn't persuaded Mr Y had a reasonable basis for believing he was making the payments in connection with a genuine request. The scammers didn't know any of Mr Y's details, only those of his son. She didn't think it was clear why his account would be at risk even if his son's account had indeed been compromised.

Mr Y disagreed with the Investigator's opinion and so the complaint was passed to me to consider.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I issued a provisional decision on 1 June 2023. I wrote:

> *I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.*
>
> *The starting point here is that Mr Y authorised these payments, even though he did so because he'd been tricked by the scammers. The payments were made with his consent and so were authorised in accordance with Regulation 67 of the Payment Services Regulations 2017 (PSRs). Under those regulations, he is presumed liable for the payments at first instance.*
>
> *However, that isn't the end of the story. Metro Bank is a signatory to the CRM Code. This Code provides additional protection for the victims of authorised push payment ("APP") scams. I'm satisfied that the payments Mr Y made fall within the scope of the CRM Code. But despite offering additional protections, it includes provisions allowing a firm not to reimburse APP scam losses fully where it can establish that the customer failed to take sufficient care when making the payments. These are often referred to as the exceptions to reimbursement.*
>
> *Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that:*
>
> - *In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without having 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.*
>
> - *The Customer ignored an effective warning by failing to take appropriate steps in response to that warning.*
>
> **There are further exceptions outlined in the CRM Code that do not apply to this case.*
>
> *I've carefully considered the arguments made by Metro here, but I'm persuaded that Mr Y did have a reasonable basis for believing that the payments he was making were for legitimate purposes. In so doing, I've considered the characteristics of Mr Y as the customer.*

As I understand it, Mr Y and his son were in the same location when the initial call from the scammers was received. The scammers took several steps to persuade Mr Y's son that they were genuine employees of the banks he held accounts with. They inserted a confirmatory text message into an existing message chain he had with the first bank and then successfully spoofed the genuine number of the second bank when calling to confirm that they were part of an interbank anti-fraud collaboration. As I understand it, Mr Y's son was panicked by what he'd been told during these calls and it's likely this will have had an impact on how plausible the story was from Mr Y's perspective.

I've also considered the fact that Mr Y and his son were told that the Metro account was at risk because it made regular transfers to and from the son's account. This meant that it was vulnerable. While the explanation as to why the Metro account was at risk wouldn't have been a persuasive one to someone with some knowledge regarding mobile phone technology and the operations of bank accounts, Mr Y had very little knowledge on this subject. I think his conclusion that this explanation was plausible was a reasonable one, if I take into account his knowledge at the time he fell victim to the scam.

Mr Y was clearly minded to call Metro to check if what his son had been told applied to him. However, the scammers told him that to do so would jeopardise the investigation into the criminal activity. Having already been persuaded that it was likely these two calls were genuinely from his son's banks, I don't find it was unreasonable for him to have taken that request at face value.

Metro says that it displayed an effective warning as part of the payment process. However, Mr Y told us that he allowed his son to make the payments on his behalf. One of the consequences of Mr Y allowing his son to make the payments in this way is that he didn't have sight of any warnings displayed during the payment process.

The test here is set out above and must be applied to the customer. The term 'customer' is defined as having the same meaning as "payer" in the PSRs – in other words, "the person who holds the account and initiates, or consents to the initiation of, a payment order from that payment account …" That means there's no way of applying the test to Mr Y's son. Since Mr Y didn't see the warning that was displayed, he can't be said to have ignored it or that it ought to have impacted the reasonableness of his belief that this request to move his money was a genuine one.

I recommended that Metro Bank reimburse Mr Y's losses in full and add on 8% simple interest per annum. Metro Bank didn't respond to my provisional decision. Mr Y responded to say that he had nothing further to add.

As neither party has raised any new arguments or submitted additional evidence for me to consider, I don't see any reason to depart from the findings I have already outlined. I am therefore upholding Mr Y's complaint for the same reasons I outlined in the provisional decision.

Final decision

I uphold this complaint. If Mr Y accepts the decision, Metro Bank PLC should:

- Reimburse the money he lost to the scam; and

- Add to that sum 8% simple interest per annum calculated to run from the date it declined his claim under the CRM Code until the date the settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr Y to accept or reject my decision before 28 July 2023.

James Kimmitt
Ombudsman