DRN-2903541

The complaint

Mr J is seeking to recover £20,200 from Metro Bank PLC ("Metro"), which was stolen from his bank account as a result of a third-party scam.

Metro says it is not liable for the loss because Mr J unwittingly authorised the payment and once notified of the fraud, it had acted as quickly as it could to try and recover the money from the payee bank. Only £4.85 remained and this was recovered, returned to Metro and subsequently credited to Mr J's account on 5 June 2019.

An investigator looked into the complaint and considered it should be upheld. Metro provided its response, disagreeing, and asked for an ombudsman's decision.

As the matter hasn't been resolved, it's been passed to me to decide.

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.

Upon reading all the available evidence and arguments, I have concluded that the fair and reasonable outcome, in all the circumstances, would be to uphold this complaint. I'll explain why.

It is common ground that Mr J 'authorised' the scam payment of £20,200. Mr J had been liaising with his solicitor in regard to making a payment, which was for a deposit, for the purchase of a property. Unbeknown to Mr J, a fraudster had intercepted the email correspondence. And this resulted in Mr J paying the amount via online banking on 9 May 2019 to the details provided by the fraudster, as opposed to his genuine solicitor.

I accept that this was an 'authorised payment' even though Mr J was the victim of a sophisticated scam. Mr J made the payment via online banking. So, although he did not intend the money to go to the scammers, under the Payment Services Regulations 2017, and the terms and conditions of his account, Mr J is presumed liable for the loss in the first instance.

However, 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 consider Metro should fairly and reasonably:

- Have been monitoring 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.

- Have 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.

- 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.

- For branch transactions, those steps may include following the Banking Protocol where appropriate.

In this case, Mr J's payment did flag on Metro's systems and it was held. Metro sent Mr J a text asking him to call in to verify that he had authorised the payment. There was subsequently a call between Mr J and Metro on 20 May 2019.

In other words, Metro had been triggered by unusual or uncharacteristic activity or by the amount of the payment so much so that it held the payment and wanted to speak with Mr J, before it processed it. So accordingly, it's just a question of whether Metro did *enough* in all the circumstances.

Having listened to the call between the adviser and Mr J, I don't think enough was done. I'll explain why.

The adviser, after verifying he was speaking to Mr J says:

> *"…this is [the payment] being held for security reasons, we just wanted to ensure that it was you that initiated the payment. This payment is something that you recognise making, just to confirm – is that correct sir."*

The call was short in its duration, and the adviser only checked to see if Mr J had made the payment, to which Mr J replied he had – as he was unaware that he had been the victim of an email intercept scam. In total, around 15 seconds was spent talking about the payment.

Banks such as Metro have actual or constructive knowledge of all the main scams, such as email intercept scams which Mr J was unknowingly falling victim to. So, as the payment had 'flagged' on Metro's security systems it could and should have done more. Had it asked Mr J about the payment, what is was for and how he received the details; Mr J would have said that it was a deposit for a property and that he was paying his solicitor and had obtained the account details through email and most of the correspondence had been through email.

The adviser should have then been on alert that Mr J could possibly be at risk of financial harm – given its knowledge of these types of scams and the prevalence of email intercept scams, which can often involve transfers of large sums which are intended for conveyancing purposes, as was the case here. The adviser could have brought to life very simply what an email intercept scam would look and feel like. And to ensure that Mr J wasn't at risk of financial harm, to contact his solicitor on a verified number and not through any telephone numbers provided on emails as those numbers could well be directing Mr J back to the fraudster.

Put simply, had the type of scam Mr J was at potential risk of, been explained to him, given the value and importance of the payment to Mr J, I believe he would have made contact with his solicitor and it would have come to light that the account details he had been provided with weren't correct and had been changed. In short, the scam would have been prevented and Mr J would not have lost £20,200.

I have also considered whether Mr J should bear some responsibility by way of contributory negligence and have taken into account Metro's comments on this aspect. However, it is clear that up to and including the time of authorising the payment, Mr J genuinely believed that he had been liaising with his solicitor. While the email addresses were slightly different – they weren't so different that Mr J, being unaware of this type of scam, had any cause for concern. The fraudulent email address contained the name of the solicitors' firm.

I am satisfied there was no contributory negligence on this occasion. Mr J was simply the unwitting and blameless victim of a clever fraudster.

In the circumstances I am satisfied Metro should fairly and reasonably reimburse Mr J for the loss he suffered, without any reduction, together with interest to compensate him for being deprived of the money he lost.

My final decision

For the above reasons, I have decided it is fair and reasonable to uphold this complaint about Metro Bank PLC – and I therefore require Metro Bank PLC to:

- Pay Mr J £20,200 less any sums already refunded (£4.85) within 28 days of receiving notification of his acceptance of my final decision; plus

- Pay simple interest on this amount, from the date of the loss to the date of the settlement. The interest rate should be 8% a year. †

† HM Revenue & Customs requires Metro Bank PLC to take off tax from this interest. Metro Bank PLC must give Mr J a certificate showing how much tax it's taken off if he asks for one.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr J to accept or reject my decision before 28 July 2021.
Matthew Horner
Ombudsman