complaint

Mr F complains that Metro Bank plc closed his accounts at short notice and applied a CIFAS marker against his name. CIFAS is the UK's fraud alert service.

background

In early November 2017 Mr F opened two accounts with Metro Bank. The bank's records indicate that he reported a lost card on 13 November and changed the mobile phone linked to the account on 20 November. A replacement card was issued on 22 November. Shortly after that, three new payees were set up on one of the accounts and small payments made to them.

On 28 November a payment of £10,000 was made to the other account and then different sums were transferred between the two accounts and to the payees that had been set up previously. Mr F then called Metro Bank to change his mobile phone back to that which had originally been registered.

On 30 November Metro Bank identified that the payment of £10,000 had been fraudulent; that is, the holder of the account from which it was made hadn't given authority for it. Metro Bank wrote to Mr F to say it was closing the accounts. It recorded a CIFAS marker against Mr F's name.

Some time later, in October 2018, Mr F contacted Metro Bank asking for bank statements. When he received them he said he didn't recognise the activity on the accounts and asked that the CIFAS marker be removed.

Mr F explained that he'd lost his card between 22 and 25 November 2017. He also said that he used an internet café for online banking; he kept a note of his online banking details which he'd put in the bin at the internet café. He also explained that he'd asked for a SWIFT code and IBAN when he'd opened the accounts, as he was expecting a payment from a friend overseas. Unfortunately, however, that friend had died before they could make the payment.

When Mr F referred his complaint to this service, one of our investigators considered it. She identified a number of inconsistencies in Mr F's version of events. Specifically:

- Mr F said he'd lost his card between 22 and 25 November. The bank's records show however that he'd reported a lost card on 13 November and that a replacement had been issued on 22 November. But in any event, the card wasn't used for any of the transactions that are relevant here.

- Mr F said he'd written down his online log-in details and left them in a public bin. Even if that were true, Mr F's mobile phone would have been needed to set up a new payee and make payments from his accounts. The log-in details wouldn't have been enough on their own.

- Mr F had changed the mobile phone number linked to the account on 20 November. The new payee codes were sent to the new number. The number was changed back on 28 November. Mr F said that the original phone was being repaired between these dates; however, the bank's records indicated that he had used the original number in that time.

The investigator thought it unlikely that someone had managed to get hold of Mr F's online banking details from the bin at the internet café and also managed to get access to his replacement phone to which the access codes were sent.

The investigator also noted that the SWIFT code for the account was quoted when the fraudulent payment was made. She wasn't persuaded that Mr F had requested that so a friend could make a payment to him. She noted too that Mr F had logged onto his accounts on 28, 29 and 30 November 2017 but later said he knew nothing about the activity on the account. She concluded that Mr F was more than likely involved in the payments and that Metro Bank hadn't treated him unfairly by acting in the way it did.

Mr F didn't accept the investigator's findings and asked that an ombudsman review the case.

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, however, I've reached the same overall conclusions as the investigator did, and for broadly the same reasons.

As the investigator identified, CIFAS members (which includes Metro Bank) should only record information of the type involved here if there are reasonable grounds to believe that a financial crime has been committed or attempted and that the evidence is such that the member could confidently report the conduct of the subject (here, Mr F) to the police. It's not enough that Metro Bank merely suspected wrongdoing on the part of Mr F.

In this case, our investigator thought that the evidence was sufficient to meet that standard. I agree with that assessment. Quite apart from the fraudulent payment, there were a number of unusual developments in the few weeks that Mr F's accounts were open – the loss of a card; the expected payment from overseas which never materialised; the temporary change of phone numbers; and the disposal in a public place of log-in details. And, as the investigator also noted, Mr F already had an account with a different provider.

Mr F provided very little supporting evidence of his version of events. For example, he said he had a medical condition that meant he couldn't remember his online banking details and so had to write them down; that he was expecting funds from abroad, but that his friend died before they could be sent; and that his original phone was being repaired.

Overall, though, I think it most unlikely that someone was able to use Mr F's newly-opened accounts to receive stolen funds and then to transfer them away, unless he was involved. His explanations about how that happened without his involvement are, in my view, not credible. In the circumstances, I'm satisfied that Metro Bank has treated him fairly.

my final decision

My final decision is that I don't require Metro Bank plc to take any further steps to resolve Mr F's complaint. Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 9 February 2020.

Michael Ingram
ombudsman