## complaint

P, a company, complains that it's been a victim of fraud, resulting in a fraudulent credit being received on to its account and a fraudster then removing those funds.

P is unhappy about how TSB Bank plc has responded to these circumstances.

P's complaint is referred here by its director, Mr E.

## background

P's account received a credit of £20,000 on 13 December 2015. On the same day, two sums of £10,000 were transferred to two external accounts by use of internet banking. The original credit was subsequently confirmed as fraudulent and TSB recorded information about the activity with CIFAS; that there'd been 'misuse of facility – fraudulent faster payment transaction'.

Mr E says that he, and therefore P, wasn't responsible for this activity on the account. But the internet banking payments were made to new payees and were able to be set up by use of the debit card and card reader. And the bank's internet event records show that two text alerts were sent to Mr E's correct and current mobile number on 13 December about new payees being set up.

The internet banking event records also show that the card and a card reader was used to access P's account online on 18 and 19 November 2015 – prior to the funds crediting the account.

Mr E told our adjudicator that around the end of November 2015, he'd received a few calls from what appeared now to be someone purporting to be from TSB. And during these calls, he was asked to confirm his internet password, personal identification number ("PIN") and two characters of his memorable word. He says he called TSB to ask why it called him and was told it was probably to confirm his internet banking set up; and so it was required to ask some security details from him.

Mr E also disputes receiving any texts and said if he had have done so, he'd have called TSB to question the payments. At one stage, Mr E thought his phone may have been in for repair so he didn't see the texts; but he later confirmed that wasn't the case.

And he says he never received his card reader or had accessed online banking since internet access was rectified, after problems with it. He has confirmed the debit card was always on him and the PIN was safe, although he has since said he never received a card.

Mr E says the account was dormant prior to these transactions and maintains the card was possibly cloned and internet banking log in details compromised through the earlier calls he had in November 2015.

But the adjudicator wasn't persuaded the payments hadn't been properly authorised on behalf of P. She didn't think it was adequately shown that the security on the account was compromised and an unknown third party was able to access P's account online.

Mr E had admitted that the account wasn't used and there were specifically no card transactions on the account. She said that cards can't be cloned over the telephone, usually,

the magnetic strip being cloned when a fraudster has accessed the card. Yet, the card wasn't used at a cash machine or for retailer transactions. And Mr E had kept the card on him as well. So she didn't think the card had been cloned.

And she was satisfied that a card reader was sent to P. And even if this wasn't received, a card reader doesn't hold any individual personal information. Any card reader can be used and as Mr E had held a personal account since 2010, with the same user ID, she couldn't rule out that a card reader issued at another time was the one that was used.

The adjudicator considered that a fraudster would have been taking undue risk, even if they'd been able to make the payments, in that they wouldn't have been successful if the alert had been received by Mr E. No attempts were made to change the registered mobile number to divert the alerts elsewhere.

And the bank's internet banking event records also showed that Mr E was sent three text alerts on 21 December 2015 showing the transactions for the past week and letting him know the balance on P's account was overdrawn. These were recorded as sent to Mr E's correct mobile number. The adjudicator found it most likely that if Mr E received these texts, he would have questioned the transactions if he hadn't authorised them. Yet Mr E didn't complain to TSB until 5 May 2016.

In conclusion, the adjudicator didn't think it likely that P's account was accessed by an unknown third party or that Mr E didn't authorise the payments from the P's account, which were made from funds fraudulently received. So she didn't consider she could recommend that TSB remove the information recorded with CIFAS, about Mr E as a director of P.

P has asked that the complaint be reviewed. It hasn't presented new evidence but has made reference to various web pages which contain articles about various fraud, scam and account security issues.

**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, I agree with the findings and conclusions as the adjudicator.

I can't now know with certainty what happened in relation to the credit to the account and the transfers. And where evidence is incomplete, inconclusive, or contradictory, I have to reach a decision on the balance of probabilities; that is, what I consider is most likely to have happened, given the evidence that is available and the wider surrounding circumstances.

Taking into account all the evidence available, I don't think P has provided a plausible explanation of how the account activity in dispute took place without Mr E authorising it. And, I've not seen anything in the web pages that Mr E has sent links to which persuades me that Mr E was, more likely than not, not responsible for that activity.

P has also referred to Data Protection legislation in his reply to the adjudicator but I'm not aware that this has a bearing on what I consider to be the fair and reasonable outcome to this complaint.

I light of what I've said, I don't require the bank to take any action in settlement of this complaint by P, this includes that it doesn't need to pay compensation or alter the CIFAS mark that's been made against P's director, Mr E.

**my final decision**

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask P to accept or reject my decision before 11 July 2016.

Ray Neighbour
**ombudsman**