Tesco Bank fraud: key questions answered

Suspicious transactions spotted on around 40,000 accounts have seen online payments frozen. So what next?

Tesco Bank: but it was the wrong people making the withdrawals. Photograph: Paul Ellis/AFP/Getty Images

Hilary Osborne

Monday 7 November 2016 11.41 GMTLast modified on Monday 7 November 2016 22.00 GMT

Current account customers at Tesco Bank have had online payments frozen after tens of thousands of accounts were attacked by fraudsters.

How many people were affected?

The bank said suspicious transactions had been spotted on around 40,000 accounts, and that money was taken from around 20,000 customers. Many account holders reported losing hundreds of pounds, with one customer telling the Guardian that more than £2,400 had been taken. Tesco Bank will not say how much money is involved in total.

So what happened?

The bank says it fell victim to online criminal activity. Tesco spotted suspicious activity on accounts on Saturday evening and texted customers who had been affected. Several people have reported that their accounts show transactions made overseas, such as in Spain and Brazil. A criminal investigation has been launched.

How was its security breached?

Tesco has not given any details, but technology specialists have speculated on what might have happened. Cliff Moyce, global head of financial services at technology firm DataArt, said the chance of the problem being cause by a "remote technical hack" was less than 50%. "Far more likely is the (in)action of a human actor, or weak process/management controls when information is shared between providers," he said.

Moyce said Tesco would need to investigate the possibility of an “economic hack” in which an offshore employee is offered a large sum of money in return for a tranche of customer data. “But incompetence rather than ill intent from an employee or subcontractor remains the more likely factor to be correlated with the malintent of the criminals,” he said.

Ed Macnair, chief executive of cloud security company CensorNet, agreed that a remote attack was unlikely. “People are the weakest link for most organisations, and I would not be at all surprised if that’s the case here,” he said. “It’s pretty hard to remotely hack into a network without some sort of assistance – which is often provided accidentally. People tend to do stupid things, like reusing passwords or clicking on random links, giving hackers the access they need.”

Moyce suggests that the hack was timed for the weekend when banks have reduced staff and the response time will have been slower than during the week. “Automated fraud detection systems appear to have worked well, but a lack of people at desks will not have helped,” he said.

What happens now?

An investigation by the National Crime Agency is under way. For customers, the bank says it plans to return to normal service as soon as possible. It has said that all direct debits and bill payments will go through as usual, and people can still withdraw cash and use their debit cards. Customers should also still be able to log in to online banking and check their accounts.

But there will be some disruption – those affected can still use their debit cards, but will be sent new ones within seven to 10 days.

Will customers be compensated?

Tesco Bank has told customers that it will refund accounts as soon as possible, hopefully on Monday, and cover any financial loss that they have suffered as a result of the fraud. For some customers who have paid penalties to other organisations, perhaps because of missed payments, this may mean providing proof to Tesco of those losses.

What should customers do?

As well as keeping an eye on their account, the chief executive of Get Safe Online, Tony Neate, said they should change their passwords immediately.

“We’d also strongly advise people to change the security question they get when forgetting their passwords, as these answers may have been compromised as a result of this breach,” he said. “We would also suggest that Tesco customers look at any other online accounts they currently have to make sure that no suspicious activity has been taking place – particularly if

you have used the same login details, which is something you should never do."

Although not directly linked to their Tesco Bank account, Neate said cyber criminals may have been able to gain access to personal information which could potentially help them unlock other online accounts.

Will customers stick around?

Tesco Bank offers a competitive current account: it is paying 3% interest on balances of up to £3,000. This may be enough to keep and attract some people. Previously, RBS managed to keep hold of customers after IT problems that went on for weeks.

Others may decide to go elsewhere. On Twitter some said they would be off. One customer said this was not the first time it had happened, and that it was "Time to move to a secure bank".

How secure are other banks?

Two years ago the Bank of England warned that banks were not taking the threat of cyber-attacks seriously enough, and experts have warned that they could fall victim to different types of fraud. But so far there have been no other attacks on the scale of that reported by Tesco.

In January, HSBC customers were locked out of online banking after the company was targeted in a "denial of service" attack. This brought down the website, but there were no reports of any losses to customers following the attack.

Macnair said banks could take some precautions. "The safest thing for organisations to do is simply restrict access to anything employees don't need in order to do their day-to-day jobs," he said. "That will at least confine any damage and prevent hackers roaming the network unchecked."

Original article — https://www.theguardian.com/money/2016/nov/07/tesco-bank-fraud-key-questions-answered-suspicious-transactions-40000-accounts