THE HINDU BusinessLine

Banks claim their systems are robust, can deter cyber attack

Our Bureau

Point out that security breach took place in the network of another bank

Mumbai, October 20:

Top banks on Thursday said they have robust mechanisms to deal with any cyber attack. This follows a breach of the ATM platforms of some banks, which may have affected as many as 3.2 million customers.

"...the possible breach of information of debit cards has taken place in the ATM network of another bank. As a precautionary measure, the PINs of debit cards used at the ATMs of that bank have been changed," said an ICICI Bank spokesperson. "Further, we are using our real-time fraud monitoring systems to identify and proactively stop any misuse of the cards which may have been impacted by the alleged breach in that bank."

Axis Bank, in a statement, said the breach has "occurred in the case of customers who have used certain non-Axis Bank ATMs. Over the last few weeks, Axis Bank has proactively reached out to the affected customers and advised them to change their debit card PINs." The bank added that it had a state-of-the-art monitoring division working 24X7.

ATM service providers also said their systems could withstand such attacks. Himanshu Pujara, MD, India, Euronet Services, said: "No ATM managed by Euronet has been affected by any sort of malware attack that would have led to debit cards being blocked. The ATMs you are talking about belong to a competitor of Euronet that manages the ATMs of the particular bank."

On the possibility of a spillover of cyberattacks on to financial markets, India's largest bourse, NSE, said: "NSE monitors such possibilities round the clock. Our firewalls and cyber security measures prevent possible penetrations."

"LODR (SEBI's Listing Obligations and Disclosure Requirements) gives operational freedom to the boards of listed entities to decide 'materiality' of an event which needs to be reported to the exchange. We understand that listed entities have policies on what are material to be reported, when to report and how much to report. The exchange will disseminate whatever is reported. If the same sources suggest that the cyber attack is of high magnitude, the exchange may also *suo motu* seek clarification if the listed entity does not report"

(This article was published on October 20, 2016)

MORE FROM BUSINESS LINE

Coming soon to your wallet: ₹2,000 notes

How US elections impact Indian stock markets

Mukesh Ambani has no fresh investment plans