FIRSTPOST.

ATM security breach hits 19 banks, 641 people; Rs 1.3 cr stolen: NPCI explains how it happened

by Oct 21, 2016

#A P Hota - MD & CEO NPCI #ATM cards #China #Debit cards #fraudulent withrdrawal #Hitachi Payments Services #MasterCard #NPCI #PCI Council #RuPay #SBI #security breach #USA #Visa

The country's largest every security breach has set off alarm bells for banks and customers alike with around 30 lakh debit cards issued in India by various banks, including the largest State Bank of India, coming under threat of potential financial fraud after reportedly the systems of Hitachi Payments Services were infested of a malware. According to media reports, Card network companies NPCI, Mastercard and Visa had informed various banks in India about a potential risk to some cards in India owing to a data breach.

] Representational image. Reuters

In a statement, A P Hota, MD and CEO, National Payments Corporation of India has sought to allay customer fears and said, “Necessary corrective actions already have been taken and hence othere is no reason for bank customers to panic. Advisory issued by NPCI to banks for re-cardification is more as a preventive exercise.”

The NPCI has also explained the issue that has wrought havoc in a few banks in the country:

1. The genesis of problem was receipt of complaints from few banks that their customer's cards were used fraudulently mainly in China and USA while customers were in India. Apprehending that this could be a case of card data compromise, all the ATMs / PoS terminals in India and three card networks - RuPay, Visa and MasterCard worked in a collaborative manner in the month of September 2016.

2. It was established through the analysis post such frauds were reported that there was a possible compromise at one of the payment switch provider's system. Based on the analysis, NPCI and other schemes identified the period of compromise and the possible card numbers which could have been compromised during that period.

3. Though there were no complaints from any of the RuPay cardholders, NPCI as a domestic utility for ATM payments has taken the lead role for proactive steps in discussing the matter with various banks and card networks.

4. The complaints of fraudulent withdrawal are limited to cards of 19 banks and 641 customers. The total amount involved is Rs. 1.3 crore as reported by various affected banks to NPCI. Cards of all these complainants are related to other card schemes. There is no RuPay cardholder who had lodged any complaint for such fraudulent usage.

5. All affected banks have been alerted by all card networks that a total card base of about 3.2 million could have been possibly compromised. Out of this 0.6 million are RuPay cards.

6. It was suspected that a compromise was at switch level which is PCI-DSS certified. Hence, subsequently PCI Council (the international body which sets standards on for PCI-DSS) was persuaded to conduct a forensic audit of the switch of one bank which is likely to be the point of compromise. The forensic study is in progress and NPCI is in touch with relevant stakeholders.

7. Based on the advisory issued by NPCI and other schemes, it is gathered that banks have advised their customers to change their debit card PIN. In situations where customers could not be contacted, the cards have been blocked and fresh cards are being issued by member banks.

8. NPCI is closely working with all stakeholders and once the forensic investigation is over and the root cause is identified, we will issue a further set of recommendations as precautionary measures to member banks.