

GOVERNMENT OF INDIA
MINISTRY OF FINANCE
LOK SABHA
UNSTARRED QUESTION NO-†728
ANSWERED ON- 12/12/2022

ATM FRAUD CASES

†728. DR. MANOJ RAJORIA
SHRIMATI RANJEETA KOLI
SHRI UDAY PRATAP SINGH
SHRI RAHUL KASWAN
SHRI SUMEDHANAND SARASWATI
SHRI BALAK NATH

Will the Minister of FINANCE be pleased to state:-

- (a) whether the Government has taken cognizance of the increasing number of ATM fraud cases by way of cloning ATM cards, tracking its PIN & OTP and other methods in the country;
- (b) if so, the details thereof including the number of complaints received in this regard during each of the last two years, State and bank-wise including Alwar, Sikar, Karauli-Dholpur, Bharatpur districts in Rajasthan;
- (c) whether the Government has taken any concrete steps to stop cyber-fraud; and
- (d) if so, the details thereof?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(DR. BHAGWAT KARAD)

(a) to (d): As per Reserve Bank of India (RBI) data on frauds reported by Scheduled Commercial Banks (SCBs) under the category “Card/Internet- ATM/Debit Cards”, the amount involved in such frauds, based on the year of occurrence, has declined from Rs. 116 crore in the financial year 2019-20 to Rs. 76 crore in the financial year 2020-21 {year-on-year (Y-o-Y) decline of 34.5%} and to Rs. 68 crore in the financial year 2021-22 (Y-o-Y decline of 10.5%).

The National Crime Records Bureau (NCRB) collects data for crime in India from States and Union Territories, and publishes the same periodically. NCRB has informed that the bank-wise details regarding complaints received under the category “ATM frauds” is not maintained by it. However, state-wise details of complaints registered under the category “ATM frauds” is at **Annex-1** and complaints registered in Alwar, Bharatpur, Dholpur, Sikar, Karauli, districts in Rajasthan are at **Annex-2**.

Comprehensive steps taken in order to strengthen security of digital transactions and to stop cyber-frauds include, *inter alia*, the following:

- (i) RBI has issued a comprehensive circular in June’ 2016 on Cyber Security Framework in Banks. As per this circular, banks were advised to put in place a board-approved cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.

- (ii) RBI has issued Guidelines dated 31.12.2019 on Cyber Security Controls for third party ATM Switch Application Service Providers (ASPs).
- (iii) RBI has issued Master Direction on Digital Payment Security Controls on 18.2.2021. As per this direction, banks have been advised to put in place necessary controls to protect the confidentiality and integrity of customer data, and processes associated with the digital product/services offered by them.
- (iv) Ministry of Home Affairs has launched a National Cyber Crime Reporting Portal to enable public to report incidents pertaining to all types of cybercrimes.
- (v) The Indian Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics and Information Technology issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies, and is working in coordination with service providers, regulators and LEAs to track and disable phishing websites and facilitate investigation of fraudulent activities.
- (vi) The Indian Cyber Crime Coordination Centre (I4C), working under the Ministry of Home Affairs has operationalised Financial Cyber Fraud Reporting and Management System module, for immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters.
- (vii) A toll-free number has also been operationalised to get assistance in lodging online complaints regarding cybercrimes.

In addition to this, a number of steps have been taken to enhance security of digital payment transactions, including those of card transactions, online transactions *etc.*, and to reduce online banking frauds which include, *inter alia*, the following –

- (i) enabling all ATMs for processing EMV chip and PIN cards;
- (ii) mandating PIN entry for all ATM transactions;
- (iii) conversion of magnetic strip card to EMV chip and PIN cards;
- (iv) restricting international usage by default and enablement of the same only after specific mandate from the customer;
- (v) certification of merchant terminals;
- (vi) Capping the value/mode of transactions/beneficiaries;
- (vii) mandating enablement of online alerts for all transactions;
- (viii) setting daily limits; and
- (ix) issuing alerts upon addition of beneficiaries.

In addition, several other initiatives have also been taken to spread awareness on prevention of cyber-crimes. These initiatives include, dissemination of messages on cyber-crime through short message service (SMS), radio campaigns, publicity on prevention of cyber-crime and cyber safety tips through social media accounts of the Indian Cybercrime Coordination Centre (I4C), conducting of electronic-banking awareness and training (e-BAAT) programmes by RBI *etc.*

Lok Sabha Unstarred question no. 728, regarding “ATM FRAUD CASES”

Details of State/UT-wise Cases Registered, under ATM Fraud for Cyber Crimes during 2020-2021

State/UT	2020	2021
Andhra Pradesh	54	62
Arunachal Pradesh	0	0
Assam	10	5
Bihar	642	775
Chhattisgarh	2	5
Goa	0	0
Gujarat	63	28
Haryana	0	0
Himachal Pradesh	0	0
Jharkhand	21	25
Karnataka	0	0
Kerala	3	2
Madhya Pradesh	10	12
Maharashtra	324	104
Manipur	0	0
Meghalaya	0	0
Mizoram	0	0
Nagaland	0	0
Odisha	362	217
Punjab	2	1
Rajasthan	117	76
Sikkim	0	0
Tamil Nadu	1	16
Telangana	315	443
Tripura	0	0
Uttar Pradesh	203	93
Uttarakhand	0	0
West Bengal	31	34
A&N Islands	0	0
Chandigarh	0	0
D&N Haveli and Daman & Diu	0	0
Delhi	0	0
Jammu & Kashmir	0	1
Ladakh	0	0
Lakshadweep	0	0
Puducherry	0	0

Source: NCRB

Lok Sabha Unstarred question no. 728, regarding “ATM FRAUD CASES”

Number of Cases Registered under ATM Fraud in the mentioned districts of Rajasthan during 2020 and 2021

District	2020	2021
Alwar	23	39
Bharatpur	0	0
Bhilwara	0	0
Dholpur	0	0
Karauli	0	0
Sikar	61	25

Source: NCRB
