

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 882
TO BE ANSWERED ON 09-02-2018

AUTHENTICATION FAILURES FOR AADHAAR IDENTITY VERIFICATION

882. SHRI HUSAIN DALWAI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) the details of authentication failures for identity verification through Aadhaar since 2015, State-wise, month-wise and Scheme-wise;
- (b) whether such data is maintained by UIDAI, if not, the reasons therefor;
- (c) the reasons for authentication failures;
- (d) whether authentication failure can lead to benefits associated with Aadhaar card being denied;
- (e) if so, the details of complaints of denial of benefits received in last one year, State-wise, month-wise and Scheme-wise; and
- (f) the remedy available in case of authentication failure?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a) and (b): Unique Identification Authority of India (UIDAI) does not maintain details of authentication failures for identity verification through Aadhaar State-wise, month-wise and scheme-wise. There is no such requirement as per the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

(c): The reasons for authentication failure may be poor network connectivity, biometric mismatch, demographic mismatch, invalid OTP value, incorrect Aadhaar number, etc.

(d), (e) and (f): No resident can be denied benefits on the basis of Authentication failure. The details in respect of denial of benefits, if any, would be available with concerned Ministries/ Departments which are using Aadhaar authentication in their respective schemes.

DBT Mission, Cabinet Secretariat vide their letter dated 19.12.2017 has issued guidelines on exception handling for use of Aadhaar in benefit schemes of Government, which inter-alia stipulates the following mechanism in respect of cases where Aadhaar authentication fails:

- i. Departments and Bank Branches may make provisions for IRIS scanners along with fingerprint scanners, wherever feasible.
- ii. In cases of failure due to lack of connectivity, offline authentication system such as QR code based coupons, Mobile based One Time Password (OTP) or Time-based One Time Password (TOTP) may be explored.

In all cases where online authentication is not feasible, the benefit/ service may be provided on the basis of possession of Aadhaar, after duly recording the transaction in register, to be reviewed and audited periodically.
