Aadhaar Act, 2016: Enabling businesses by leveraging Aadhaar

- Do you have to reject customer applications for missing ID proofs?
- Do you want to get rid of those photocopies of customers' ID cards?
- Do you verify your customers' identity using Aadhaar-based authentication?
- Do you share your customers' identity information with third parties?

pwc

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, will be an enabler for your business. This act gives statutory backing for the unique Aadhaar number to be used as proof of identity for accessing services such as bank accounts and phone connections, or for disbursal of subsidies and government benefits.

The Aadhaar initiative was launched in 2009 to provide everyone in India with a unique identification number (UID). Aadhaar is world's largest biometric identification programme with over 100 crore registrants.

What Aadhaar Act means

Simplification of cumbersome and lengthy identification processes

Simplification of identification processes will save significant cost and time for service providers and enable them to serve more customers.

Onus for protection of customers' Aadhaar data

The Act lays down monetary penalties and imprisonment for service providers for unauthorised sharing of customers' identity information, failure to keep the records secure, failure to properly inform the customers about the use of their information, or failure to obtain their consent for authentication.

More customers due to ease in identity verification

With the Aadhaar-based authentication process, service providers will be able to acquire more customers, who would have otherwise not been enrolled due to lack of identification.

Reduced cost, time and errors in identity verification

Service providers can verify customers' details such as identity, address, photograph and age, without needing to maintain photocopies of their ID cards by validating directly from the UIDAI database. This electronic validation will reduce the chances of fake identification as well as reduce the usage of paper.

Direct benefit transfer (DBT) to a resident's bank account

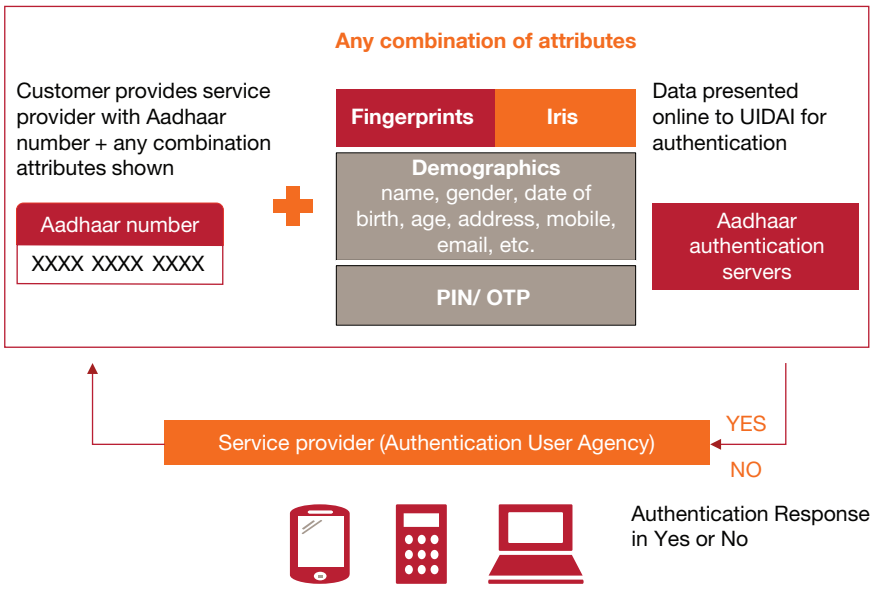
A major benefit of Aadhaar authentication is the facilitation of DBTs or payment of subsidies to the resident's bank account.

Verification for telephone services, bank transactions, attendance etc.

Aadhaar may also be used to verify a customer's identification for telephone services; bank transactions; travel; courier/e-commerce deliveries; Aadhaar-enabled payment systems; government attendance; controlled/ restricted access; and more.

The system also helps in maintaining the privacy of customers by getting rid of paper-based photocopies of customer IDs, which may be easy to lose.

How Aadhaar Authentication works



- The authority will not share the core biometric information of the resident, such as fingerprint or iris scan, with the service provider.
- Both the service provider requesting authentication and the UIDAI are forbidden from sharing the residents' or customers' identity information or the record of authentication with anyone, save for specified exceptions.

What it needs

The service provider must be registered as an Authentication User Agency (AUA) or a sub-AUA according to the UIDAI policy.

It needs to have in place the required infrastructure, including devices to capture customers' identity information and network connectivity to send and receive information from UIDAI. It also must have adequate safeguards in place for protection of customers' identity information and data:

Privacy policy to be implemented and followed across the company	**Data Security** to be maintained through adequate controls	**Consent form** from user to use personally identifiable information
Third-party audits and reviews to ensure compliance with the law	**Stakeholder awareness** about the provisions of the law	**Customer grievance mechanism** to deal with aadhaar related queries

Provisions

- **8(2) A requesting entity shall—**
  - (a) unless otherwise provided in this Act, obtain the consent of an individual before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations; and
  - (b) ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication.
- **8(3): A requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identity information for authentication, the following details with respect to authentication, namely:—**
  - (a) the nature of information that may be shared upon authentication;
  - (b) the uses to which the information received during authentication may be put by the requesting entity; and
  - (c) alternatives to submission of identity information to the requesting entity.
- **29(1): No core biometric information, collected or created under this Act, shall be—**
  - (a) shared with anyone for any reason whatsoever; or
  - (b) used for any purpose other than generation of Aadhaar numbers and authentication under this Act.
- **29(2): The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations.**
- **29(3): No identity information available with a requesting entity shall be—**
  - (a) used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or
  - (b) disclosed further, except with the prior consent of the individual to whom such information relates.
- **29(4): No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.**
- **57: Nothing contained in this Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or any body corporate or person, pursuant to any law, for the time being in force, or any contract to this effect provided that the use of Aadhaar number under this section shall be subject to the procedure and obligations under section 8 and Chapter VI of the Aadhaar Act.**

The authority has recently notified the regulations under the Aadhaar Act covering areas of Sharing of Information, Data Security, Authentication, Enrolment and Update, Transaction of Business at Meetings of the Authority.

Penalty and punishment

Sections 40, 41 and 42 of the act deal with penalties and punishment for offending entities.

Whoever, being a requesting entity, uses the identity information of an individual in contravention of sub-section (3) of section 8, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Whoever, being an enrolling agency or a requesting entity, fails to comply with the requirements of sub-section (2) of section 3 or sub-section (3) of section 8, shall be punishable with imprisonment which may extend to one year or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Section 43(1) states that Where an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to any punishment provided in this Act if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

How PwC can help

As a multidisciplinary practice, PwC is well placed to help businesses make the most of the new avenues opened up by this law, while navigating through the complexities of the penal provisions. The PwC team encompasses resources with diverse experience and on the ground expertise in all major aspects to address different requirements.

Current state assessment	• Assess the current information security posture • Identify and recommend necessary modifications in compliance with the Aadhaar Act and Regulations
Draft/review privacy policy	• Create/review the privacy policy for compliance to the Aadhaar Act, 2016
Create resident consent form	• Assist in creating consent forms for residents to ensure transparency of the privacy and security practices and compliance to the act
Audit and review	• Facilitate security assessment and periodic review • Evaluate and suggest continual improvement of the process
Awareness campaign	• Run awareness campaigns to meet the compliance requirements of the act

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

Contacts

Neel Ratan
Leader
Government and Public Sector, PwC India
neel.ratan@in.pwc.com

Sivarama Krishnan
Leader
Cyber Security
sivarama.krishnan@in.pwc.com

Rahul Aggarwal
Director
Cyber Security
rahul2.aggarwal@in.pwc.com

pwc.in

SUS/July2016