INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

INFOLEX
NEWSALERT

OCTOBER 2018

THE AADHAAR JUDGMENT AND RECENT POLICY CHANGES:

WHAT DOES IT MEAN FOR FIN-TECH COMPANIES?

1. INTRODUCTION

At the end of September, the Supreme Court of India, in *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.* (the **"Aadhaar Case**"),[1] upheld the validity of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "**Aadhaar Act**") while striking out parts of the Aadhaar Act which permitted private companies and other body corporates to use the Aadhaar number of an individual for establishing the identity of an individual for any purpose.

The effect of this judgement is that companies are no longer permitted to use the authentication and e-KYC facilities authorized under the Aadhaar (Authentication) Regulations, 2016, (the **"Authentication Regulations**") which had become a preferred method for authenticating and establishing identity details of individuals, when transacting in a paperless format.

The judgement of the Supreme Court is likely to have a disproportionate effect on fin-tech companies, which have largely based their business models around the possibility of using e-KYC facilities for identity authentication.

This news alert looks at the implications of the Aadhaar Case and other recent policy measures or proposals and analyzes their collective effect on the ease of doing business for the *fin-tech* industry.

2. ANALYSIS

2.1 Aadhaar Case and e-KYC

The Master Direction – Know Your Customer (KYC) Direction, 2016[2] (the "**KYC Master Direction**") issued by the Reserve Bank of India (the "**RBI**") required entities regulated by the RBI to undertake a customer identification process, while undertaking transactions with their customers.

For an individual eligible to enroll and receive an Aadhaar number, the KYC Master Directions required the mandatory submission of Aadhaar details and required the regulated entity to undertake KYC authentication based on Aadhaar data for account-based relationships. It is to be noted that the KYC Master Direction stated that it was subject to the final judgement of the Supreme Court in the Aadhaar Case.

To a certain extent, the customer identification process is carried out using the *one time password* ("**OTP**") based e-KYC, which is a feature permitted by the Aadhaar Act and recognized by the KYC Master Directions. Many fin-tech companies, having mostly online operations with limited offline presence were reliant on this OTP based e-KYC for complying with the customer identification process requirement.

[1] *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.*, available at <https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf>.

[2] Available at < https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10292> (Last updated on July 12, 2018).

Section 57 of the Aadhaar Act was the enabling provision, allowing private companies to use Aadhaar numbers to establish the identity of individuals for any purpose, pursuant to a contract. The Authentication Regulations further allowed an entity (*authorized under the Authentication Regulations to use e-KYC authentication* facility) to share the e-KYC data of the Aadhaar number holder with other entities for a specified purpose, subject to the consent of the individual concerned. This was relevant for those fin-tech companies, which were offering a number of *different* services through *group companies* without each of the group companies having to undertake the KYC process.

The Supreme Court partially struck down Section 57 of the Aadhaar Act as violating the fundamental right to privacy of individuals to the extent it allowed any company or any person to use Aadhaar numbers to establish the identity of individuals for *any purpose* pursuant to a contract.

It was noted that any restriction on privacy is required to be backed by law and be *proportional* to the objective sought to be achieved by the restriction. The use of words '*any purpose*' was read down as '*a purpose backed by law*'. Further, allowing any body corporate (*including private companies*) to use Aadhaar data, especially on the basis of a contract with such body corporate or person, was seen as *disproportional* since it enables commercial exploitation of an individual's information by private entities.

As noted earlier, the KYC Master Direction states that the submission of Aadhaar details and Aadhaar-based authentication was *contingent* on the views of the Supreme Court on the validity of using an individual's Aadhaar number and other identification details. In light of those parts of Section 57 of Aadhaar Act, which enabled private entities to use Aadhaar numbers for authentication being struck down, further clarity is required on the manner of undertaking customer identification

In this context, the recent amendments to the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (the "**PMLA Rules**") required the *mandatory* linking of Aadhaar with customer bank accounts. The Supreme Court has struck down these amendments as being unconstitutional. To the extent an individual was eligible to be enrolled for an Aadhaar number, the verification required under the PMLA Rules was required to be undertaken by the authentication mechanism under the Authentication Regulations.

Given the Supreme Court ruling, more clarity is required on the manner of verifying the identity of customers. Nevertheless, with the Aadhaar Case disallowing the use of Aadhaar based authentication of individuals by private companies, using OTP based e-KYC ceases to be an option for these fin-tech companies. This effectively removes the possibility of a non face-to-face customer identification process, which will substantially increase the time and cost of enlisting customers.

2.2 Payment Systems – Data Localization

Turning to other recent policy developments, in April 2018, the RBI came out with a notification[3], which mandated all payment system providers to store all data relating to payment systems operated by them in a system located in India. This data localization requirement applies even to full end-to-end transaction details and information collected, carried or processed as part of the message or payment instruction.

System providers were required to comply with the data localization requirement by October 5, 2018 and are required to report compliance to the RBI by October 15, 2018. An audit is also required to be conducted by CERT-IN empaneled auditors and the Systems Audit Report duly approved by the board of the system provider is required to be submitted to the RBI by December 31, 2018.

[3] Available at <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0>.

The data localization requirement results in significant costs for the payment system providers, who do not have local infrastructure for data storage.

2.3 Prepaid Payment Instruments – Interoperability

In October 2017, the RBI issued Master Directions on *Prepaid Payment Instruments*[4], specifying the requirements for operating *e-wallets* that facilitate the purchase of goods and services against the value stored on such instruments.

Among other requirements, the issuers of *prepaid payment instruments* were required to enable the interoperability of *wallets* amongst themselves, through a *United Payments Interface* (a "**UPI**").

Further, interoperability was also required to be enabled between *wallets* and *bank accounts* through a UPI, pursuant to the operational guidelines to be issued by the RBI. The interoperability guidelines are expected to be issued soon by the RBI and could potentially impact the fin-tech space.

The operational guidelines will likely require changes to the underlying technology framework and may also impact their competitive advantage. Enabling interoperability may require a degree of standardization in the technology used, which may limit the ability of fin-tech companies to innovate with their platform to create a competitive advantage.

2.4 Personal Data Protection Bill, 2018

Pursuant to the report of the B.N. Srikrishna Committee which was set up to suggest data privacy legislation in India, the Personal Data Protection Bill, 2018[5] (the "**Bill**") has been proposed to govern the processing of personal data of Indian residents by entities in India and overseas.

The Bill proposes, among other requirements, that a serving copy of all personal data collected from individuals in India shall be stored in India. In addition to this, there are stringent conditions for cross border transfer of personal data, which indirectly may necessitate storing personal data only in India.

Further, certain categories of data, which are designated by the Central Government as *critical personal data* are permitted to be stored only in India. This is in addition to a number of data protection rights granted to individuals, including the right to confirmation, access and correction of data, the right to be forgotten and the right to data portability.

Financial data has been categorized as *sensitive personal data* for which there are stringent requirements for collection and processing. It still remains to be seen if the Central Government will designate financial data as *critical personal data*. Although some of the requirements specified in the Bill are progressive and in line with international standards, they are likely to result in higher costs for business. The data localization requirement and restrictions on cross border transfers are especially problematic since the data storage infrastructure costs are often prohibitive for most businesses to operate.

3. INDUSLAW VIEW

The judgement in the Aadhaar Case will require a number of fin-tech companies to rethink their business models. The inability to use the Aadhaar based e-KYC authentication will require those companies who currently use it, to engage more resources in their customer due diligence process, resulting in increased cost of acquiring customers.

[4] Available at <https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142> (Last updated on December 29, 2017).

[5] Available at < http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>.

These companies may be forced to pass on this cost to the customer, which may price out certain categories of the population from using the service provided. Further, the operational challenges of undertaking the customer diligence *offline* may also operate as a deterrent, preventing customers from using services offered by fin-tech companies.

There have been proposals that the government bring in a law to specifically allow private companies to use Aadhaar based authentication. It should be noted that one of the grounds, which the Supreme Court ruled against private entities using Aadhaar based verification, was that it could result in *commercial exploitation* of an individual's biometric and demographic information. It may therefore prove politically difficult to legislate for this aim.

That aside, the onus now rests with the government or the RBI to propose an equally efficient alternate measure to ease the difficulty that private companies will now face in their customer due diligence process. One potential suggestion is the verification of customer identity by using the *QR code* mechanism, which allows the customer to share demographic details and a photograph in offline mode such that there is no transfer of transaction details to the central database of Aadhaar.

While this may resolve some of concerns of the Supreme Court, since it does not involve the mandatory disclosure of Aadhaar number, or the access to transaction details of the individual, it may still require face-to-face, in person verification to ensure that the concerned individual is the person in the photograph. Other alternatives should be explored which allow for non face-to-face verification, similar to what the earlier e-KYC mechanism using Aadhaar number had allowed.

The Aadhaar Case is silent on the critical question of whether data already collected by private entities is required to be deleted. A direction to this effect was only made in the dissenting opinion of Justice Chandrachud, but it was solely in relation to details collected by telecom service providers and more clarity will inevitably be required.

Recent changes to the FDI policy, which have reduced the stringent conditions for foreign investment in the *other financial services* sector (which often covers the services provided by several fin-tech companies), reflect the intention of encouraging foreign investments in the fin-tech sector. However, recent legal developments have made it increasingly difficult for companies to operate in the fin-tech sector or for India to position itself as a technology-centric sector, which is likely to have an effect on foreign investment.

Authors: Suneeth Katarki | Namita Viswanath | Savithran Ramesh

Sector: Government & Regulatory | Telecommunications, Media & Technology

Date: October 11, 2018

DISCLAIMER

This alert is for information purposes only. Nothing contained herein is, purports to be, or is intended as legal advice and you should seek legal advice before you act on any information or view expressed herein.

Although we have endeavored to accurately reflect the subject matter of this alert, we make no representation or warranty, express or implied, in any manner whatsoever in connection with the contents of this alert.

No recipient of this alert should construe this alert as an attempt to solicit business in any manner whatsoever.