To: Whomsoever it may concern

Sub: India Domestic Messaging Traffic

SWIFT India Domestic Services Private Limited ("Swift India"), a joint venture between Swift SC and 11 banks in India, was incorporated in 2012 to provide financial messaging services in India. Since then it has been our constant endeavour to bring the best-in-class messaging services to the Indian community.

The RBI data localisation requirements, as set out in the RBI's Circular dated April 6, 2018 and RBI FAQs of June 26, 2018, on the Storage of Payment System Data in India apply to authorised payment systems and banks and require that the regulated entities ensure that domestic payments data be stored in a system only in India. While such data are allowed to be processed overseas, regulated entities must ensure that the data-

(1) must be deleted from all systems abroad and brought back to India not later than one business day or 24 hours from payment processing, whichever is earlier; and
(2) stored in India only.

Neither Swift India nor Swift SC is the subject of the RBI data localisation requirements, and customers are reminded that the responsibility of compliance with the requirements will always lie with the regulated entities.

Swift India processes India domestic financial messages outside of India in SWIFT SC's global Operating Centres. To assist customers with their compliance with the RBI data localisation requirements, Swift India recommends that India domestic messages be only sent through the Swift India domestic messaging network. This is a Closed User Group that requires a separate BIC (typically in the format XXXXINBI), and no cross-border messages are allowed to be sent or received. Messages sent through the Swift India domestic messaging network will be deleted within 24 hours. Further, please note that only FileAct and InterAct are available on the Swift India domestic messaging network.

As such, domestic messages not sent through the XXXXINBI BIC could put a regulated entity at risk of being non-compliant with the RBI data localisation requirements. Please note that Swift India or Swift SC disclaims any liability which may arise out of or in connection with the regulated entities' non-compliance with applicable local laws or regulations. Customers are advised to observe our recommendation for sending India domestic messages, which has been designed to assist with compliance with the RBI data localisation requirements.

Thank you.
SWIFT India Domestic Services Private Limited
Mumbai / June 2023

Encl.: RBI's Circular dated April 6, 2018 and RBI FAQs of June 26, 2018, on the Storage of Payment System Data in India

SWIFT India Domestic Services Private Limited

Registered and Corporate Office:
Unit No.1801, 18 floor, B-Wing, The Capital,
Plot No. C-70, G Block, Bandra Kurla Complex,
Bandra (E), Mumbai 400051, India
CIN : U74120MH2012FTC239126

Phone: + 91 22 61966900
Fax: + 91 22 66156974
Email: contactus@swiftindia.com
Web : www.swiftindia.com

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2017-18/153
DPSS.CO.OD No. 2785/06.08.005/2017-2018 6 April 2018

The Chairman and Managing Director / Chief Executive Officers,
Authorised Payment Systems /
All Scheduled Commercial Banks including RRBs /
Urban Co-operative Banks/State Co-operative Banks /
District Central Co-operative Banks /Payment Banks / Small Finance Banks and Local Area Banks

Madam / Sir,

Storage of Payment System Data

Please refer to paragraph 4 of the Statement on Development and Regulatory Policies of the First Bi-monthly Monetary Policy Statement for 2018-19 dated April 5, 2018. In recent times, there has been considerable growth in the payment ecosystem in the country. Such systems are also highly technology dependent, which necessitate adoption of safety and security measures, which are best in class, on a continuous basis.

2. It is observed that not all system providers store the payments data in India. In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries/ third party vendors and other entities in the payment ecosystem. It has, therefore, been decided that:

i. All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.

ii. System providers shall ensure compliance of (i) above within a period of six months and report compliance of the same to the Reserve Bank latest by October 15, 2018.

iii. System providers shall submit the System Audit Report (SAR) on completion of the requirement at (i) above. The audit should be conducted by CERT-IN empaneled auditors certifying completion of activity at (i) above. The SAR duly approved by the Board of the system providers should be submitted to the Reserve Bank not later than December 31, 2018.

3. The directive is issued under Section 10(2) read with Section 18 of Payment and Settlement Systems Act 2007, (Act 51 of 2007).

Yours faithfully

(Nanda S. Dave)
Chief General Manager-in-charge

भुगतान और निपटान प्रणाली विभाग, केंद्रीय कार्यालय, 14वीमंजिल, केंद्रीय कार्यालय भवन,शहीद भगतसिंह मार्ग, फोर्ट, मुम्बई - 400001
फोनTel: (91-22) 2264 4995; फैक्सFax: (91-22) 22691557; ईमेल-e-mail : cgmdpssco@rbi.org.in
Department of Payment and Settlement Systems, Central Office, 14th Flr, Central Office Building,
Shahid Bhagat Singh Road, Fort, Mumbai - 400001

FREQUENTLY ASKED QUESTIONS

Storage of Payment System Data

The Reserve Bank of India issued a directive vide circular DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 06, 2018 on 'Storage of Payment System Data' advising all system providers to ensure that, within a period of six months, the entire data relating to payment systems operated by them is stored in a system only in India.

Payment System Operators (PSOs) have sought clarification on certain implementation issues, from time to time, from Reserve Bank. The FAQs are intended to provide clarity on those issues to facilitate and ensure expeditious compliance by all PSOs.

1. Applicability of the direction

- The directions are applicable to all Payment System providers authorised / approved by the Reserve Bank of India (RBI) to set up and operate a payment system in India under the Payment and Settlement Systems Act, 2007.
- Banks function as operators of a payment system or as participant in a payment system. They are participants in (i) payment systems operated by RBI viz., RTGS and NEFT, (ii) systems operated by CCIL and NPCI, and (iii) in card schemes. The directions are, therefore, applicable to all banks operating in India.
- The directions are also applicable in respect of the transactions through system participants, service providers, intermediaries, payment gateways, third party vendors and other entities (by whatever name referred to) in the payments ecosystem, who are retained or engaged by the authorised / approved entities for providing payment services.
- The responsibility to ensure compliance with the provisions of these directions would be on the authorised / approved PSOs to ensure that such data is stored only in India as required under the above directions.

2. Where should the payment data be stored?

The entire payment data shall be stored in systems located only in India, except in cases clarified herein.

3. Clarification regarding data that needs to be stored in India

The data should include end-to-end transaction details and information pertaining to payment or settlement transaction that is gathered / transmitted / processed as part of a payment message / instruction. This may, interalia, include - Customer data (Name, Mobile Number, email, Aadhaar Number, PAN number, etc. as applicable); Payment sensitive data (customer and beneficiary account details); Payment Credentials (OTP, PIN, Passwords, etc.); and, Transaction data (originating & destination system information, transaction reference, timestamp, amount, etc.).

4. Storage of data pertaining to cross-border transactions

For cross border transaction data, consisting of a foreign component and a domestic component, a copy of the domestic component may also be stored abroad, if required.

5. Processing of payment transactions

- There is no bar on processing of payment transactions outside India if so desired by the PSOs. However, the data shall be stored only in India after the processing. The complete end-to-end transaction details should be part of the data.
- In case the processing is done abroad, the data should be deleted from the systems abroad and brought back to India not later than the one business day or 24 hours from payment processing, whichever is earlier. The same should be stored only in India.
- However, any subsequent activity such as settlement processing after payment processing, if done outside India, shall also be undertaken / performed on a near real time basis. The data should be stored only in India.
- In case of any other related processing activity, such as chargeback, etc., the data can be accessed, at any time, from India where it is stored.

6. Can the data processed abroad be retained abroad till the window for customer dispute resolution / chargeback is available?

As indicated above, the payment data sent abroad for processing should be deleted abroad within the prescribed time line and stored only in India. The data stored in India can be accessed / fetched for handling customer disputes whenever required.

7. Can the payment system data be shared with overseas regulators?

The data may be shared with the overseas regulator, if so required, depending upon the nature / origin of transaction with due approval of RBI.

8. Scope and coverage of the System Audit Report (SAR)

The System Audit Report (SAR), from a CERT-In empanelled Auditor, should inter-alia include Data Storage, Maintenance of Database, Data Backup Restoration, Data Security, etc.

9. Clarification in respect of entities earlier permitted to store banking data abroad?

In the case of banks, especially foreign banks, earlier specifically permitted to store the banking data abroad, they may continue to do so; however, in respect of domestic payment transactions, the data shall be stored only in India, whereas for cross border payment transactions, the data may also be stored abroad as indicated earlier.

Top