




Financial RegTech Newsletter

March 2021



Click to launch 

In this issue

The RBI's Master Direction on Digital Payment Security Controls, 2021

01

Other regulatory news

03

Regulatory news

02

Global regulatory news

04



The RBI's Master Direction on Digital Payment Security Controls, 2021



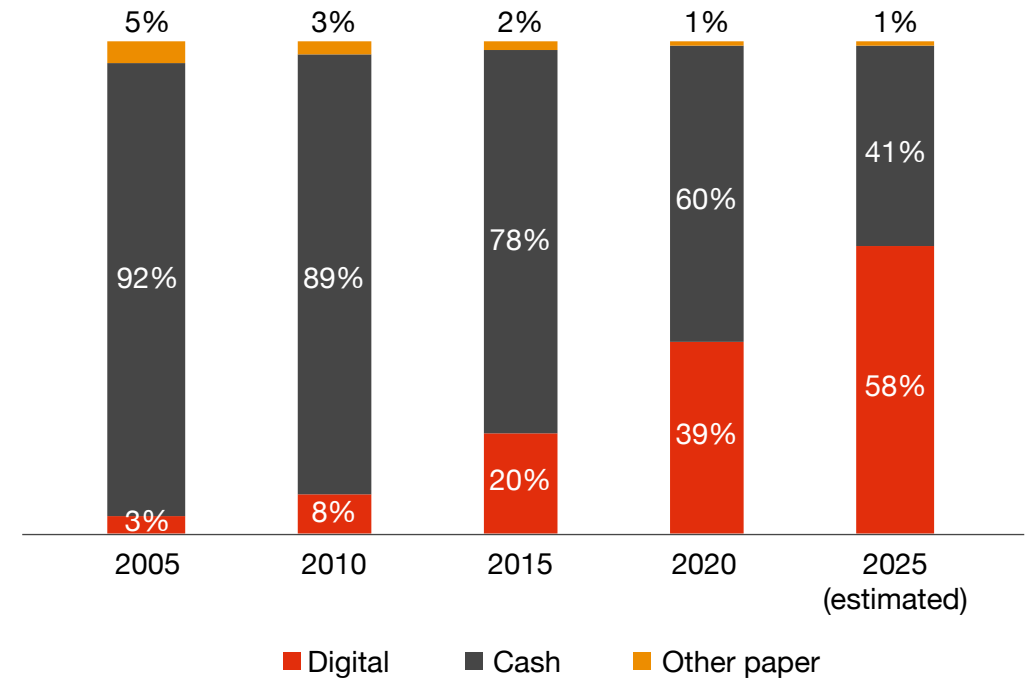
The Master Direction on Digital Payment Security Controls released by the Reserve Bank of India (RBI) on 18 February 2021 provides necessary guidelines and common minimum standards that regulated entities (REs) should adhere to in the areas of governance and security for digital products and services.¹ The RBI has given significant importance towards the security of digital transactions, considering the growth of digital payments systems in India.

This edition of PwC's Financial RegTech newsletter provides an overview of the RBI's Master Direction on Digital Payment Security Controls, 2021.

1. Introduction

The Master Direction requires all REs to set up robust governance and security structures, catering to secure internet and mobile banking, digital and card payments, among others. This comes against the backdrop of increasing adoption of digital payments, aided by a Government push as well as lifestyle changes owing to the COVID-19 pandemic. As per the latest reports by a leading technology advocacy group, the adoption of digital payments has increased manifold in the last five years and is expected to account for 58% of all transactions by 2025.²

The share of digital payments is expected to grow to 58% by 2025



Source: NASSCOM

¹ <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0>

² <https://community.nasscom.in/communities/digital-transformation/fintech/india-digital-payments-2020-launching-the-first-adoption-index-time-is-now.html>

Timelines and applicability

The guidelines have been issued to create a safe and secure environment for customers, thereby increasing the speed of adoption. These directions shall come into effect within six months of issuance, unless they have already been notified separately via a circular or an advisory.

The provisions under the Master Direction will be applicable to the following regulated entities:

- scheduled commercial banks (except regional rural banks)
- small finance banks
- payments banks
- credit card issuing non-banking financial companies (NBFCs).

Governance and management of security risks

Regulated entities are required to formulate their policy for digital payments products and services with the following main tenets:

- necessary controls to protect the confidentiality of customer data
- the availability of requisite infrastructure with secure and scalable products, allowing minimal service disruption
- ensuring effective dispute-resolution mechanisms
- risk assessment, including operational risk and fraud risk along the lines of technology used, dependency on third-party service providers, provision of interoperability and reconciliation processes.

In the following sections, we will analyse the Fraud Risk Management and Reconciliation Framework mandated by the RBI in its Master Direction.

The share of digital payments in transactions in India is estimated to grow up to 58% in 2025 from 3% in 2005.

The RBI's Master Direction mandates all regulated entities to set up robust governance and security controls for digital payments, with elaborate fraud risk management and reconciliation.

2. Fraud Risk Management

REs are expected to define automated rules for identifying and alerting customers in case of suspected behaviour, failed authentication, etc. The configuration aspects of these rules and preventive controls should be well documented and implemented.

System alerts to cover these rules shall include (but not limited to) the following parameters:

- high transaction velocity (any digital activity such as fund transfers, withdrawals, e-payments and addition of beneficiaries) in a short time period, especially for customers who have never used digital payments channels
- high-risk Merchant Category Code (MCC) parameters
- counterfeit card parameters, such as a string of invalid Card Verification Values (CVVs) and personal identification numbers (PINs)
- new account parameters, such as excessive activities in a new account
- unusual patterns with respect to time zones, geolocations and internet protocol (IP) addresses
- behavioural biometrics
- transactions originating from identified compromised points
- transactions to/from digital wallets/numbers which have been identified as fraudulent
- transactions that are declined or have no transaction code, etc.

A systematic process for fraud analysis shall be put in place to identify the reasons and formulate preventive mechanisms for such incidents. Additionally, the RBI also mandates that regulated entities should come up with the following operational changes to augment their Fraud Risk Management tool:

- arrange for training sessions that will help the staff understand fraud control tools and their usage, investigative techniques and RBI regulations
- upskilling staff for them to use the fraud detection tool effectively by setting and updating rules, monitoring exceptions, differentiating false positives from actual fraud and enabling fraud reporting and escalation matrix
- maintaining updated contact details of service providers, intermediaries and all other stakeholders, as well as formulating standard operating procedures (SOPs) for handling incidences.

A characteristic of Fraud Risk Management is sending system alerts to flag transactions on unusual patterns such as high transaction velocity, high-risk Merchant Category Codes (MCC), invalid CVVs and PINs, rogue IP addresses, etc.

Banks and financial institutions should focus on upskilling their staff on the fraud management tool, RBI guidelines and SOPs to handle fraud incidences.

Reconciliation Mechanism

The RBI also mandates the introduction of a real-time/near real-time reconciliation mechanism for all digital transactions between REs and other stakeholders such as payments system operators, card networks, payments system processors, FinTech aggregators, payments gateways and technology partners. Such a reconciliation framework will enable better detection and prevention of suspicious transactions. It should be used within 24 hours of the transaction and receipt of settlement files.

The RBI mandates the introduction of a real-time/near real-time reconciliation framework for all digital transactions between REs and other stakeholders in order to detect and prevent suspicious transactions.

Customer protection, awareness and grievance redressal mechanism

Additionally, REs are also required to undertake the following measures:

- They are advised to incorporate usage guidelines and training materials for end users of digital applications. They must make it mandatory for end users to read and agree to the terms and conditions during onboarding as well as first usage after each major update.
- A separate section which clearly specifies the processes, forms, guidelines and contact information for end users to lodge customer grievances should be incorporated.
- The RBI's existing instructions on Online Dispute Resolution (ODR) should be included and adhered to with minimal manual intervention.

- It is important to educate customers about the need to maintain physical and logical security of devices and digital payments products. They should also be informed about the risks and benefits of the digital payments ecosystem, as well as their rights and responsibilities in upholding the security policy.
- A mechanism in digital applications should be present that would allow end users to flag transactions as fraudulent so that REs are immediately notified. On receiving such notifications from the customer, the entity shall report such transactions to all involved stakeholders to mitigate losses at the earliest.

- Mandatory agreements should be signed with end users on usage guidelines during onboarding and after every major update of digital payments application.
- An automated ODR system with minimal manual intervention should be set up.
- End users can flag fraudulent transactions using digital payments platforms.



Conclusion

The RBI has come up with stringent guidelines to develop a robust ecosystem, taking into account the meteoric growth in the adoption of digital payments channels and the increasing use of such channels for fraudulent activities. At the centre of this framework lies the mandate for an elaborate Fraud Risk Management system coupled with a near real-time reconciliation mechanism to detect and prevent suspicious transactions.

Additionally, the RBI has also come up with various guidelines related to internet banking, mobile payments and security controls for card payments.

A majority of digital payments end users are first-time users with little or no knowledge of digital platforms, the risks attached and various fraudulent techniques. The central bank has taken these aspects into consideration and stressed on the importance of customer education and staff upskilling. End users will be in a better position to utilise digital payments platforms when they are aware of their rights, responsibilities, risks attached and the various risk management and grievance redressal mechanisms available. It is essential for the entire ecosystem to work together in countering the risk of fraud.

The RBI's Master Direction is a significant step and will go a long way in mitigating the various risks that are attached with the digital payments ecosystem, thereby enhancing security and stability, and increasing adoption.

02 Regulatory news

Ways and Means Advances (WMA) limit for the first half of FY21–22

The RBI has fixed the WMA limit to INR 120,000 crore for the first half of FY21–22. It has also assured that in case the Government of India (GOI) uses 75% of this limit, fresh market loans will be floated. The interest rate for the WMA is fixed at the repo rate and that of overdrafts (OD) is fixed at the repo rate plus two percent.

The detailed notification can be accessed [here](#).

RBI extends the timeline for processing of recurring online transactions

In August 2019, the RBI published a framework for processing e-mandates on recurring online transactions done using cards and wallets. In January 2020, this framework was then extended to Unified Payments Interface (UPI) transactions as well.

In this framework, the usage of Additional Factor of Authentication (AFA) was mandatory for registration and processing of the first transaction for an amount of up to INR 5,000. The deadline for implementing the same was set to 31 March 2021.

However, some stakeholders have still not implemented this framework. To avoid customer inconvenience, the RBI has extended the implementation deadline by six months, i.e. September 2021. Stringent supervisory action will be initiated against stakeholders who are non-compliant post the extended timeline.

The detailed notification can be accessed [here](#).

Average base rate to be charged by NBFC-MFIs for the first quarter of FY21–22

According to a [circular](#) dated 7 February 2021, the RBI issued a notice to non-banking financial company-micro finance institutions (NBFC-MFIs) regarding the pricing of credit given by them. The circular stated that the central bank will consider the average base rate of five largest commercial banks to derive the base rate for the next quarter. This average rate will be published by the RBI on the last day of the working quarter.

In alignment with the above-mentioned circular, the average base rate for the first quarter of FY21–22, i.e. April 2021 to June 2021 is fixed at 7.81%.

The detailed notification can be accessed [here](#).



The South Asian Association for Regional Cooperation (SAARC) Finance Governor’s Symposium, March 2021

SAARCFINANCE is an association of central bank governors and finance secretaries of the SAARC region. RBI Governor Shaktikanta Das currently presides over the meetings of this association. This symposium was inaugurated by the RBI Governor on 2 March 2021.

The RBI Governor highlighted the importance of using technology by central banks in the areas of big data, digital currencies, regulatory technology (RegTech), supervisory technology (SupTech) and cyber security. The symposium included a keynote address followed by a panel discussion on ‘Cyber security in Central Banks’ and a presentation on ‘Comparison of Financial Sector Regulatory Regimes in the SAARC Region’.

The RBI Governor’s tenure as the SAARCFINANCE Chair comes to an end on 1 April 2021 and he handed over the position to the Governor of the Maldives Monetary Authority.

The detailed notification can be accessed [here](#).



03 Other regulatory news

SEBI issues Master Circular on Surveillance of Securities Market

The Securities Exchange Board of India (SEBI) has been issuing various circulars from time to time for effective surveillance of the securities market. The Master Circular is a compilation of all the circulars issued by the Integrated Surveillance Department which are operational. In case of any inconsistency between the Master Circular and the applicable circulars, the content of the relevant circular shall prevail.

The circular provides information on:

- i. trading rules and shareholding pattern in dematerialised mode
- ii. unauthenticated news circulated by SEBI-registered market intermediaries through various modes of communication
- iii. disclosures under SEBI (Prohibition of Insider Trading) Regulations, 2015.

The Master Circular can be accessed [here](#).

IRDAI permits short-term COVID-specific health insurance policies

The Insurance Regulatory and Development Authority of India (IRDAI) has permitted all general and health insurance companies to offer short-term COVID-specific health insurance policies. Considering the prevailing COVID-19 situation, the IRDAI has decided to allow all insurers to offer and renew policies including the 'Corona Kavach Policy' and the 'Corona Rakshak Policy'.

The circular can be accessed [here](#).

SEBI advises registered entities, including market infrastructure institutions (MIIs) to comply with TRAI's TCCCP Regulations, 2018

It has come to SEBI's notice that unsolicited messages containing stock tips/investment advice with respect to listed companies are increasingly being circulated through bulk SMS, encouraging investors and the general public to invest in or purchase the stocks of certain listed companies. In order to curb the problem of unsolicited commercial communication, all SEBI-registered entities, including MIIs (which use bulk SMS for providing their services to the investors) are advised to ensure strict compliance with the Telecom Regulatory Authority of India's (TRAI) Telecom Commercial Communications Customer Preference Regulations (TCCCP), 2018. Non-compliance with the provisions of said regulations may result in the disruption of delivery of their messages.

The official circular can be accessed [here](#).



04 Global regulatory news



The European Securities and Markets Authority (ESMA) advises to the European Commission on data reporting service providers (DRSPs)

The advice primarily focuses on the fees, fines and penalties applicable and the derogation criteria. It aims to provide a simple framework by leveraging the existing frameworks for Trade Repositories and Securitisation Repositories, and streamlining the approach for assessment of the exemption criteria. Post the ESA's review, authorisation and supervision of authorised reporting mechanisms (ARMs) and approved publication arrangements (APAs) will transfer from the National Competent Authorities (NCAs) to ESMA.

ESMA has proposed application, authorisation and annual supervisory fees for DRSPs. It has adopted an approach for the calculation of fees for 2022, the first year of its supervision of DRSPs. It has also proposed a simplified timeline for payment of the fees.

In its technical advice on fines and penalties for DRSPs, ESMA has proposed on specific procedures and aspects. After submitting its technical advice to the Commission, ESMA will continue working with NCAs on a smooth transfer of supervisory responsibilities for the relevant DRSPs as of 1 January 2022.

The official notification can be accessed [here](#).

FCA launches a campaign to encourage individuals to report wrongdoing

The Financial Conduct Authority (FCA) has launched a new campaign encouraging individuals working in financial services to report potential wrongdoing, which also includes materials for firms to share with employees. Financial institutions should take advantage of the additional resources available and incorporate these into their whistle-blower programmes.

The official notification can be accessed [here](#).

ESMA evaluates the compliance with UCITS liquidity guidelines and highlights areas of vigilance

ESMA published the results of the 2020 Common Supervisory Action (CSA) on Undertakings for the Collective Investment in Transferable Securities (UCITS) liquidity risk management (LRM).

The 2020 CSA aimed to get a comprehensive market overview, including detailed insights into the practical implementation and quality of liquidity risk management processes. The COVID-19 outbreak gave further stimulus to deepening the exercise.

Compliance with the UCITS LRM ensures protection for investors, financial stability and orderly functioning of financial markets.

The official notification can be viewed [here](#).

LIBOR rate will cease to exist

The FCA has announced the dates that panel bank submissions for all LIBOR settings will cease, after which representative LIBOR rates will no longer be available. This is an important step towards the end of LIBOR. The Bank of England and the FCA urge market participants to continue to take necessary action to ensure that they are ready.

The official notification can be accessed [here](#).

ESMA supports increasing corporate transparency through the creation of ESAP

ESMA has submitted its response to the European Commission’s (EC) targeted consultation on the European Single Access Point (ESAP). It has proposed a phased approach, prioritising the financial and non-financial information of public companies. The ambition to set up the ESAP will increase investors’ trust in companies across the European Union (EU) and lower the cost of capital. ESMA believes that full benefit can be reaped only if the information available in the single database is comparable in terms of content and rendered in a structured and machine-readable format.

The official notification can be accessed [here](#).



Contact us



Mukesh Deshpande

Partner, Technology Consulting
PwC India
mukesh.deshpande@pwc.com
+91 98450 95391

Hardik Gandhi

Associate Director, Technology Consulting
PwC India
hardik.gandhi@pwc.com
+91 98193 79703

Umang Agrawal

Associate Director, Technology Consulting
PwC India
agrawal.umang@pwc.com
+91 97691 95355

Arvind Raj

Principal Consultant, Technology Consulting
PwC India
arvind.raj@pwc.com
+91 99693 58788

Anurag Gupta

Principal Consultant, Technology Consulting
PwC India
anurag.gupta@pwc.com
+91 77603 14901

Acknowledgements

This newsletter has been researched and authored by Samrat Biswas, Akanksha Mota and Prachi Gujare.





About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Find out more about PwC India and tell us what matters to you by visiting us at www.pwc.in

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2021 PricewaterhouseCoopers Private Limited. All rights reserved.

HS/April2021 - 12211