

## Swaminathan J: Safe banking practices – protecting the young

Speech by Mr Swaminathan J, Deputy Governor of the Reserve Bank of India, at the Global Money Week 2024, Paris, 18 March 2024.

\* \* \*

Mr. Yoshiki Takeuchi, Deputy Secretary General, OECD, Ms. Mairead McGuinness, European Commissioner for Financial Services, Ms. Magda Bianco, Chair of OECD INFE and G20 GPFI, Mr. Connor Graham, youth representative from Enactus, assembled regulators from across the world, ladies and gentlemen. A very warm good morning to all of you. It gives me immense pleasure to speak to you today on a highly relevant topic - safe banking practices and protecting the young.

As we are all aware, the COVID-19 pandemic accelerated digitalisation in financial services, prompting a swift transition to online mode by service providers and customers. Accompanying this surge in digitalisation was also the proliferation of fintech platforms. Often operating outside the regulatory envelope and unconstrained by legacy systems that typically encumber traditional banks, fintech companies exhibit remarkable agility and adaptability in offering customised financial products.

These developments are indeed welcome. However, while they offer immense benefits such as accessibility and hyper-personalization, they also heighten the risk of misuse and fraud. They can expose consumers to risk of cyberattacks, data breaches, and often times, some financial harm. Consumers may struggle to resolve disputes or obtain compensation due to lack of transparency on the part of such players. These new risks must be addressed through robust regulatory frameworks, enhanced cybersecurity measures, and increased consumer awareness initiatives.

In this context, I would like to share some of the approaches adopted in India through regulation, supervision and most importantly, enhanced consumer awareness.

### Regulation and Supervision

In India, regulated entities are required<sup>1</sup> to implement multi-factor authentication for all payments through electronic modes and fund transfers, except for some explicitly exempted small value transactions. At least one of the authentication methodologies should be generally dynamic or non-replicable such as one-time password, mobile device binding, biometric, etc. Regulated entities are required to put in place security controls for internet banking, mobile payments application and card payments security.

Regulated Entities are also required to conduct risk assessment of the safety of digital payment products as well as suitability and appropriateness of the same vis-a-vis the target users, both prior to establishing the service and regularly thereafter. Further, they are required to have systems to identify suspicious transaction behaviour and mechanisms in place to alert customers of the same.

To protect customers, regulations<sup>2</sup> provide for zero liability for customers for losses due to negligence by the bank or a third-party breach. Where it is due to customer negligence, the liability is limited to the point of reporting.

RBI has also issued Guidelines on Digital Lending<sup>3</sup> which require regulated entities to provide a Key Fact Statement to the borrower before the execution of the contract. This statement must disclose the Annual Percentage Rate, the recovery mechanism, the grievance redressal mechanism, etc. Any fees or charges, including penal charges, which are not mentioned in the Key Fact Statement cannot be charged to the borrower.

Regulatory requirements are backed by a strong supervisory framework that inter-alia evaluates business conduct and IT system controls. Where warranted, RBI takes appropriate supervisory actions including imposition of business restrictions.

One of the notable initiatives of the Government of India is the Indian Cyber Crime Co-ordination Centre (I4C) for better coordination amongst law enforcement agencies. Under this initiative a National Cyber Crime Reporting Portal<sup>4</sup> has been set up with a 24x7x365 national helpline number to allow victims of cyber-fraud to report such crimes.

## **Customer awareness**

Despite all these measures, instances of unauthorised transactions due to compromised credentials from phishing attacks or customer negligence are not uncommon.

RBI therefore, makes concerted efforts to foster a culture of financial prudence and resilience through customer awareness and education campaigns. In consultation with other financial sector regulators, a National Strategy for Financial Education has been drawn up to enhance financial literacy. We have intensive awareness campaigns running across multiple mediums including print, radio and television under the banner of 'RBI Kehta Hai' ('RBI says'). Apart from integration with school curricula, initiatives such as the RBI All-India Quiz for school children on financial literacy aim to instil financial acumen from an early age. The RBI website hosts a microsite<sup>5</sup> on Financial Education in English, Hindi, and 11 vernacular languages, offering comic books, films, games, messages on financial planning, etc.

In collaboration with our regulated entities, innovative approaches such as street plays ('nukkad nataks'), flash mobs, folk arts, sports rallies and marathons have also been tried with much success. In partnership with banks and NGOs, Centres for Financial Literacy are being established at grassroot levels to boost community driven financial literacy.

Last month, RBI organised a 'Financial Literacy Week' on the theme "Make a Right Start – Become Financially Smart" targeted towards young adults, mainly students. The idea was to increase awareness on the advantages of inculcating financial discipline from an early age with inputs on saving, budgeting, power of compounding, banking essentials and cyber hygiene.

As we focus on safeguarding the young, let us not forget the vulnerability of our senior citizens to financial frauds and cybercrime. It is incumbent upon us to extend our efforts to ensure their financial security and well-being as well.

In conclusion, it is imperative that we remain vigilant and proactive in addressing the emerging risks and challenges. By implementing robust regulatory frameworks, enhancing cybersecurity measures, and promoting consumer awareness and financial literacy, we can mitigate the risks associated with digitalization and protect consumers from exploitation and fraud. Thank you for this opportunity, and I wish you fruitful discussions at the Global Money Week.

---

<sup>1</sup> Please refer Master Direction on Digital Payment Security Controls available at <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=12032>

<sup>2</sup> Please refer to RBI circular dated July 6, 2017 on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions available at <https://rbi.org.in/scripts/NotificationUser.aspx?Id=11040&Mode=0>

<sup>3</sup> RBI 'Guidelines on Digital Lending' issued on September 2, 2022, available at <https://rbi.org.in/scripts/NotificationUser.aspx?Id=12382&Mode=0>

<sup>4</sup> <https://cybercrime.gov.in/>

<sup>5</sup> <https://www.rbi.org.in/FinancialEducation/>