Security Standards for the Financial Technology Sector in India

October, 2019

By **Vipul Kharbanda**

With technical inputs from **Prem Sylvester**

The Centre for Internet and Society, India

Working Draft - Subject to further Consultations and Revisions

Introduction

Information security standards provide a framework for the secure development, implementation and maintenance of information systems and technology architecture. Regulatory policies often cite several information security standards as a baseline that is to be complied with in order to ensure the adequate protection of information systems as well as associated architecture. Information security standards for the financial industry provide consideration to the specific risks and threats that financial institutions may face, making them an integral part of the process of ensuring business and operational sanctity.

There is an urgent economic interest in ensuring robust security of the financial technology sector within the country. This interest is amplified considerably due to the policy push seeking to shift India towards the realisation of a 'cashless society'. This recent policy push has in part led to the ubiquitous adoption of technology-centric financial services such as PayTM, PhonePe, Mobikwik and others. The current landscape with respect to security standards for financial institutions in India appears to be multi-pronged; with multiple standards in place for companies to implement.

One of the major stumbling blocks when dealing with the Fintech sector is the lack of a universally accepted definition of the term. FinTech is generally understood as an amalgamation of "finance" and "technology," but there is divergence on whether the centre of gravity of FinTech is the former or the latter.[1]

Definitions that focus on the financial services offered by FinTech describe technology as an enabler. Arner et al[2] simply state that "FinTech refers to technology enabled financial solutions, or the new marriage of financial services and information technology," or as Thakor puts it[3], FinTech is the "use of technology to provide new and improved financial

[1] Fintech Literature Review - Forthcoming

[2] Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P., The Evolution of Fintech: A New Post-Crisis Paradigm? (October 1, 2015). University of Hong Kong Faculty of Law Research Paper No. 2015/047; UNSW Law Research Paper No. 2016-62. Available at SSRN: https://ssrn.com/abstract=2676553 or http://dx.doi.org/10.2139/ssrn.2676553

[3] Anjan V. Thakor, Fintech and banking: what do we know?, Journal of Financial Intermediation, 2019, 100833, ISSN 1042-9573, https://doi.org/10.1016/j.jfi.2019.100833.

services." FinTech is often described in terms of the companies that offer such financial services, combined with "modern, innovative technologies[4]." Magnuson[5] emphasizes FinTech as a "new breed" of companies "that specialize in providing financial services primarily through technologically enabled mobile and online platforms." Varga expands definitions of FinTech by noting[6] that the goal of such companies is to develop "novel, technology-enabled financial services" whose ultimate aim is to "transform current financial practices." The Financial Stability Board (FSB) summarizes FinTech as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions, and the provision of financial services."[7]

Other definitions describe FinTech in terms of the technological innovations that interact with financial services in a variety of ways - specifically, digital innovations and technology-enabled business model innovations[8] and novel technologies adopted by financial institutions which are ultimately used to improve the quality of financial services[9]. Drasch et al. expect FinTech companies to bring these technology solutions and innovations to the financial sector to provide more effective financial products and services that bring the sector into the digital age[10]. Others refer to FinTech as an industry that uses (mobile-centered IT[11]) technology to enhance the efficiency of the financial system[12]."

[4] Dorfleitner, G., Hornuf, L., Schmitt, M., & Weber, M. (2017). Definition of FinTech and Description of the FinTech Industry. FinTech in Germany, 5–10. doi:10.1007/978-3-319-54666-7_2

[5] Magnuson, William J., Regulating Fintech (August 26, 2017). Vanderbilt Law Review, Forthcoming; Texas A&M University School of Law Legal Studies Research Paper No. 17-55. Available at SSRN: https://ssrn.com/abstract=3027525

[6] Varga, David. (2017). Fintech, the new era of financial services. Vezetéstudomány / Budapest Management Review. 48. 22-32. 10.14267/VEZTUD.2017.11.03.

[7] *Financial Stability Implications From Fintech*. 2017. Ebook. Financial Stability Board. https://www.fsb.org/wp-content/uploads/R270617.pdf.

[8] Philippon, T. (2016). The FinTech Opportunity. doi:10.3386/w22476

[9] Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. Journal of Network and Computer Applications, 103, 262–273. doi:10.1016/j.jnca.2017.10.011

[10] Drasch, B. J., Schweizer, A., & Urbach, N. (2018). Integrating the "Troublemakers": A taxonomy for cooperation between banks and fintechs. Journal of Economics and Business. doi:10.1016/j.jeconbus.2018.04.002

[11] Kim, Yonghee & Park, Young-Ju & Choi, Jeongil & Yeon, Jiyoung. (2015). An Empirical Study on the Adoption of "Fintech" Service: Focused on Mobile Payment Services. 136-140.

[12] McAuley, Daniel. 2015. "What Is Fintech?". *Medium*. https://medium.com/wharton-fintech/what-is-fintech-77d3d5a3e677.

Arner et al. note that the term "FinTech" is not confined to specific sectors of the existing financial industry (e.g. financing) or business models (e.g. peer-to-peer (P2P) lending), but instead covers the entire scope of services and products traditionally provided by the financial services industry[13]. Gomber et al.[14] refer to FinTech companies as both start-ups and established IT companies (often without a history in banking and/or financial services) entering the financial domain and evolving at the intersection of information and communication technology, specifically via the Internet and automated information processing, thereby disrupting the financial sector. Eickhoff reiterates that these companies operate at the intersection of (i) financial products and services and (ii) information technology, and they are usually (iii) relatively new companies (often startups) with (iv) their own innovative product or service offerings[15]. FinTech, therefore, is constructed such that it has three dimensions[16]: an input (namely the combination of technology, organization and money flow), mechanisms (create or improve or change, disrupt, apply technology to finance, create competition on the market) and an output (creation of new services or products or processes or business models). Milian et al. employ Christensen's (2003) theory of disruptive innovation to categorize these outputs of FinTech as "Sustainable Fintechs," for established financial service providers that work to protect their market positions by using IT through incremental innovations, and "Disruptive Fintechs" that are new companies and start-ups that challenge established providers by offering new technological products and services.[17]

We are thus presented with a mixed bag of definitions of FinTech. While the breadth of approaches in the literature to defining FinTech offers us a broad range of factors to consider, it also complicates attempts to create a comprehensive definition of the same. We agree with Dorfleitner et al.[18] who note that it is not possible to construct a restrictive definition of "FinTech" that applies to all of the entities traditionally associated with the

[13] Arner et al. (2015).
[14] Gomber, P., Koch, J.-A., & Siering, M. (2017). *Digital Finance and FinTech: current research and future research directions. Journal of Business Economics, 87(5), 537–580.* doi:10.1007/s11573-017-0852-x
[15] Eickhoff, M., Muntermann, J., & Weinrich, T. (2017). What do FinTechs actually do? A Taxonomy of FinTech Business Models. *ICIS*.
[16] Zavolokina, Liudmila; Dolata, Mateusz; Schwabe, Gerhard (2016). FinTech – What's in a Name? In:Thirty Seventh International Conference on Information Systems, Dublin, Ireland, 11 December 2016 -14 December 2016
[17] E.Z. Milian, M.d.M. Spinola, M.M. de Carvalho, Fintechs: A Literature Review and Research Agenda, Electronic Commerce Research and Applications (2019), doi: https://doi.org/10.1016/j.elerap. 2019.100833
[18] Dorfleitner et al.(2017).

term. The area has an amorphous and evolving shape, and it is uncertain if and/or when its boundaries may set. However, for the purpose of laying a foundation for understanding its functions and regulatory responses, we summarize the reviewed definitions to arrive at the following: FinTech describes a broad range of companies who develop technology-centred products that enhance the functionality of financial services as were typically offered by incumbent financial institutions (including banks & non-banking financial companies). We do not incorporate in this definition the form such enhancements may take, or the motivations for such enhancement, for reasons we will explain in later sections.

Need for these Rules

There may be an assumption amongst some that all Fintech entities are governed by the Reserve Bank of India which has a number of detailed guidelines regarding security standards. However, not all Fintech entities come under the jurisdiction of the Reserve Bank of India, which only has the powers conferred on it specifically under the Reserve Bank of India Act, 1934. Similarly the Securities and Exchange Board of India as well as the Insurance and Regulatory Development Authority only have powers to regulate entities specific to their sectors.

The burden of regulation the security standards of Fintech entities which do not fall under the regulations issued by the abovementioned authorities falls on the Information Technology Act, 2000, ("IT Act") and more specifically on the rules issued issued pursuant to section 43A of the IT Act, called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules").

Section 43A of the IT Act requires body corporates to comply with 'reasonable security practices and procedures' in order to avoid liability for negligence in dealing with data causing wrongful loss or gain. The explanation to Section 43A states that in the absence of a contract specifying the security practices adopted by the body corporate, reasonable security practices and procedures will be those as specified in the SPDI Rules. Unfortunately even the SPDI Rules do not lay down any specific security standards or protocols but say that entities

would be assumed to have implemented reasonable security practices and procedures if they have undertaken measures that are commensurate with the information assets being protected with the nature of business.

The only specific standards that the SPDI Rules prescribe or refer to are the ISO27001 (or any other standards developed by an industry body which have been duly notified by the Central government). This means that if a body corporate has implemented the ISO27001 standard they shall be deemed to have complied with reasonable security practices and procedures as long as such standards have been certified or been audited on a regular basis. The financial sector in India has to date not developed any sectoral security standards that have been approved by the Central government (as required by the SPDI Rules), meanwhile, we have learned from conversations with FinTech startups that ISO 27001 is an expensive standard for small businesses to implement. Therefore, there appears to be a need for a set of security standards or guidelines that Fintech entities can look to implement which are specific and detailed enough to perhaps form a checklist but easier and more economical to implement than the ISO27001 standard or even the industry specific PCI DSS standard. It is precisely to fulfil this need that the Centre for Internet and Society, along with (any future partners) have prepared these Draft Information Technology (Fintech Security Standards) Rules ("Fintech Rules") in order to ensure that not only the data of users is dealt with in a secure and safe manner but also that the smaller businesses in the Fintech industry have a specific standard to look at in order to limit their liabilities for any future breaches.

A question may arise as to why have such specific rules only for the Fintech industry and not for other entities which deal with sensitive and personal data or information. The answer to this is rooted in the structure of section 43A of the IT Act, which provides for monetary damages for negligence in dealing with sensitive and personal data. It is assumed that losses due to negligence in dealing with financial data would be easier to quantify in monetary terms, and perhaps would affect the users in a more direct manner than other forms of data.

Methodology

Structure of the Rules

All industries or sectors may not necessarily need to be regulated through legal mandates, moreover, in some cases the goals of the legal mandate may be better achieved through self regulation rather than state regulation. Self-regulation can take many forms, but at a very basic level it involves a private organization assuming responsibilities for its own rules and practices and also overseeing the enforcement of these as against a government regulator doing the same under law. This can be done by way of each organization tailoring its own codes of conduct or any industry body (such as a trade association) establishing a common code or a set of principles and each individual firm modelling its policies for the implementation of such a code. Such a model of governance though has been criticized due to an overall lack of accountability and transparency, incomplete realization of the principles promulgated in common codes and weak oversight and enforcement.[19] Though reverting back to a command and control regulatory model may not be the most efficient approach for many fledgling industries operating with new technologies as 1) the law would not be able to keep up with the latest developments and 2) excessive regulation could stifle the growth of such industries.

A middle path between the above two models is a co-regulatory framework which involves both the government and the industry coming together and sharing the responsibility of drafting and enforcing regulatory standards.[20] This allows the government and the industry body to negotiate proper regulatory goals, collaborate on the drafting of standards, and work in a cooperative manner to enforce the standards against firms which violate it. Furthermore, this approach may be better than the traditional regulatory regimes as 1) It draws on industry

[19] Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving beyond Voluntary Codes, 6 I/S J. L. POL. 355 (2011).
[20] Hans-Bredaw-Institut, Final Report: Study on Co-Regulation Measures in the Media Sector, 2006, (defining "co-regulation" as systems that "combine state- and non-state regulation" and contrasting it with self-regulation, which operates "without any state involvement").

knowledge and expertise; 2) It yields rules that are more cost-effective, workable, and innovative; 3) It also creates a stronger sense of industry ownership over rules and thus better compliance; 4) The consultative process leads to rules that are more politically practicable and efficient.[21] It is perhaps for this reason that the SPDI Rules also follow a co-regulatory mechanism, and these proposed Rules also seek to adopt a similar framework.

These Fintech Rules are not set up as a licensing requirement, i.e. Fintech Entities will not have to comply with these rules as a precondition to starting operations. They have been drafted in a manner similar to that of the SPDI Rules, i.e. as a measure to be implemented for Fintech Entities to absolve themselves of any liability against claims of negligence under section 43A of the IT Act. This means that there is no legal obligation on Fintech entities to comply with these rules, instead there is a commercial reason to do so, viz. if a Fintech entity adopts and implements the standards prescribed in these rules then they can legally absolve themselves from liability for damages on the grounds of negligence as specified under section 43A of the IT Act. Thus, there is a business case for Fintech entities to implement these standards rather than a legal obligation; this approach should ensure that the data of users is well protected while at the same time ensuring that there is no unnecessary burden on the fledgling Fintech industry. If a Fintech entity believe that it is too small or deals with extremely small amounts of data, it can take a commercial decision (risk) on whether to comply with these standards at all or follow its own policies. If it chooses the latter, then in case of a data breach, it will have the obligation to prove in court that its policies comprise reasonable security practices and procedures.

The Rules have only a single set of standards which all Fintech entities would be required to follow. These standards have been condensed and gleaned from the ISO 27001 standard as well as the Guidelines on Information Security, Electronic Banking, Technology risk management and cyber frauds issued by the Reserve Bank of India. An attempt has been made to simplify and ease the requirements given under the standards in order that entities with limited resources such as small start-ups are also able to satisfy the standards while at the same time ensuring that customer data is not compromised. If it is felt during stakeholder consultations that these standards may not adequately protect the interests of

[21] Hirsch, The Law and Policy of Online Privacy: Regulation, Self-regulation, or Co-regulation? 34 SEATTLE UNIV. L. REV. 439 (2011).

users in certain scenarios, such as in the context of Fintech entities which have an extremely large number of users, or large turnover, or are extremely data reliant, etc., then a classification may be made and Fintech entities which, it is felt, should comply with stricter standards could be required to comply with ISO27001 or other similar standards.

PLEASE NOTE: This exercise was started with the limited scope of coming up with a specific set of data protection standards for the Fintech sector, and for the purposes of these Rules we have made certain assumptions which include adequacy of the definition of "sensitive personal data and information" as well as the provisions relating to collection, transfer or disclosure (sections 5, 6, and 7) under the SPDI Rules. We may in the future increase the scope of the project and reopen the discussion on one or more of those issues.

DRAFT MODEL FINTECH SECURITY STANDARDS

In exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.--

1. Short Title and Commencement - (*1*) These Rules may be called the Information Technology (Fintech Security Standards) Rules, 2019.

(*3*) They shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

2. Definitions

(1) In Rules, unless the context otherwise requires,

(a) "body corporate" shall mean any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

Expl: This explanation has been adopted from section 43A of the Information Technology Act, 2000 since it is an expansive definition which covers almost all entities which would have a significant enough presence to require regulation while leaving out individuals working solely as individuals and not as a commercial venture.

(b) "cyber security incident" shall mean any real or suspected adverse event in relation to cyber security that violates an explicit or implied security policy resulting in unauthorized access, denial of service/ disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;

Expl: This definition has been adopted from the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

(c) "Chief Information Officer" shall mean the person so designated by a Qualified Fintech Entity under sub-clause (1) of Rule 4;

(d) "Fintech Entity" means a body corporate which deals with technology-centred products that enhance the functionality of financial services as were typically offered by incumbent financial institutions (including banks and non-banking financial companies), and the term Fintech shall be construed accordingly.

Expl: Please refer to the Background note for more details on this definition.

(f) "Offering services in India" shall mean (a) enabling legal or natural persons in India to use the Fintech services offered by it; and (b) having a substantial presence in India.

Explanation: The term "substantial presence in India" may be said to exist where the Fintech Entity has an establishment in India. In the absence of an establishment in India, the criterion of a substantial presence shall be determined on the basis of the existence of a significant number of users or the targeting of activities in India. The targeting of activities can be determined on the basis of relevant circumstances, including factors such as the use of Indian currency, providing local advertising, handling of customer relations, such as by providing customer service in local languages generally used India, etc.

Expl: These terms and the Explanation have been adopted from the new E-evidence Directive of the European Union since they provide a good balance between those offering services in India but excludes entities who have a miniscule presence or whose activities are not geared towards India so that compliance does not become a burden to commercial activity.

(g) "Personal Data" shall mean data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of any aspect of the identity of such natural person, any identifiers intended to be associated with such natural person, any combination of such features or identifiers, or any combination of such features or identifiers with any other information..

Explanation: "A natural person can be considered as "identified" when, within a group of persons, he or she is distinguished from all other members of the group . A natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it by taking into account all the means likely reasonably to be used either by a data fiduciary or by any other person to identify the said person ."

Expl: This is a modified version of the definition of personal data as proposed in the Draft Data Protection Bill, 2018 as presented to the Ministry of Electronics and Information Technology, by the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, on July 27, 2018. The modifications expand the definition in the original Bill to include identifiers meant to track natural persons. The modification also clarifies that "any aspect" of the identity of the person is covered by the definition. The Explanation regarding the terms "identified" and "identifiable" have been taken from the Article 29 Working Party in the EU, as was suggested in the CIS Submissions on the Draft Personal Data Protection Bill, 2018.[22] It must be noted that the Personal Data Protection Bill has a more restrictive definition of "financial data" as well as "sensitive personal data" however, we have not used these definitions here because for the following two main reasons (a) these Rules are not an entry restriction, in that Fintech Entities do not not have to comply with these Rules before they start operating, therefore even if the obligations thereunder are a little onerous, Fintech Entities can do a cost benefit analysis and if they believe that the data they possess does not pose a big risk to

22 https://www.medianama.com/wp-content/uploads/Centre-for-Internet-and-Society-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf

the customers, then they may choose to ignore all or some of the security standards prescribed here (and open themselves to liability in case of a breach); (b) restrictive definitions such as the ones for "financial data" and "sensitive personal data" always carry the risk of some kind of (potentially useful) data being missed out, perhaps even because such data sets were not conceptualised at the time of drafting the Rules.

(h) "Qualified Fintech Entity" shall mean a Fintech Entity offering services in India and possessing, dealing or handling any Personal Data of their customers.

Expl: This definition ensures that only entities which are offering services in India have to comply with the security standards prescribed in this regulation. This qualification ensures that not all Fintech entities around the world get covered by this legislation unless they have a significant presence or interest in India.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Security Standards

(1) Notwithstanding anything contained in any other law for the time being in force, a Qualified Fintech Entity shall have an obligation to maintain confidentiality in relation to any Personal Data of its users that is dealt with, handled by or in its possession.

Expl: This is a generic obligation to maintain confidentiality in relation to the financial data of their users.

(2) All Qualified Fintech Entities shall have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.(1) These information security policies shall be reviewed by

the Fintech Entities annually and, if required, updated and upgraded as may be necessary to ensure that the Personal Data is safe.(2) Subject to the provisions of sub-section (3) below, a Qualified Fintech Entity shall be deemed to have put in place reasonable security practices and procedures if it has implemented such security practices and standards as prescribed in the Schedule to these Rules notified under this section.

Expl: This is the main section providing an obligation to put in place adequate and documented security systems which should be commensurate which the nature of the business of the entity. This requirement of the systems being commensurate which the nature of the business has been adopted from Rule 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 which automatically puts an obligation on the entity to ensure that the security systems for sensitive information are more stringent than for other information. There is an added obligation to ensure that the systems are upgraded from time to time to ensure that they are capable of meeting the latest challenges. The way these Rules are structured, Fintech Entities that believe they are too small to be able to spend any resources on data security have an option to not put in place the security systems provided herein, but if they do not then they expose themselves to the risk of paying damages under Section 43A of the IT Act.

(3) Any industry association of Fintech Entities or an entity formed by such an association, which has developed codes of best practices for data protection shall get its codes of best practices duly approved and notified by the Central Government for effective implementation. All Qualified Fintech Entities in the relevant sector, whether registered with the industry association or not, shall be required to implement any such codes notified by the Central Government within a reasonable time, which shall not exceed a period of one year from the date of such notification.

Expl: This sort of a co-regulation mechanism has been adopted from the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 with the added requirement that once such codes are notified by the Government, all Fintech Entities in the relevant sector will have to follow those codes, whether they are a

member of the industry body (whose code has been approved) or not. This sentence has been added to ensure that Fintech Entities do not escape their obligation by not joining industry bodies or in case a particular sector has more than one industry body. The period of 1 year has been specified for implementation of the Codes notified by the government, this addition was suggested during the external consultations on the Draft.

4. Breach Notification to CERT-In

(1) Every Qualified Fintech Entity shall appoint a senior member of the management as the Chief Information Officer with such roles and responsibilities as mentioned in the Schedule. A Fintech Entity offering services in India which experiences a cyber security incident, shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the incident to the Indian Computer Emergency Response Team (CERT-In) as per the requirements of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(2) The incident notice by the Fintech Entity above shall (a) describe the nature of the cyber security incident including where possible, the categories and approximate amount of the data records concerned; (b) communicate the name and contact details of the Chief Information Officer or other contact point where more information can be obtained; (c) describe the likely consequences of the cyber security incident; (d) describe the measures taken or proposed to be taken by the Fintech Entity to address the cyber security incident, including, where appropriate, measures to mitigate its possible adverse effects.

Expl: This clause reiterates the obligation to report incidents which is contained in the CERT-In Rules. The clause has been included here for the purpose of clarity and in order to not cause any confusion it refers back to the CERT-In Rules. The extra requirement of what the notice should contain has been adopted and modified from the EU GDPR. The reporting obligation here is to

all Fintech Entities offering services in India whether dealing with personal information or not, which is why the term Qualified Fintech Entities is not used here.

5. Breach Notification to Users

(1) A Qualified Fintech Entity which experiences a cyber security incident which is likely to result in any loss or damage to such users, such Fintech Entity shall communicate such incident to the users without undue delay, which shall in no case be beyond 72 hours of the discovery of the cyber security incident.

(2) The incident notice by the Fintech Entity above shall (a) describe the nature of the cyber security incident including where possible, the categories and approximate number of users concerned and the categories and approximate number of Personal Data records concerned; (b) communicate the name and contact details of the Chief Information Officer or other contact point where more information can be obtained; (c) describe the likely consequences of the cyber security incident; (d) describe the measures taken or proposed to be taken by the controller to address the cyber security incident, including, where appropriate, measures to mitigate its possible adverse effects.

Expl: This clause has been adopted and modified from the EU GDPR. The safe harbor given in the GDPR which exempts data processors not dealing in vital data, from reporting personal data breaches in certain circumstances (such as encryption, etc) have not been included in this definition as of now since this sets a higher standard for reporting. The data breach has to be reported to the users without undue delay. There is no requirement to report the incident immediately so that Fintech Entities are able to conduct their own internal investigations to determine the reasons and extent of the data breach before they report it to the users. This would ensure that users are given as much information as possible so that they do not panic unnecessarily. However, in order to ensure that unscrupulous entities do not take advantage of this provision and unduly delay the notification, a hard deadline of 72 hours has been prescribed.

6. Exclusion

No provisions of these Rules shall apply to Bodies corporate which are under the regulatory supervision of the Reserve Bank of India, the Securities and Exchange Board of India or the Insurance and Regulatory Development Authority and are required to follow security standards specifically prescribed by said authorities.

Provided that this Rule 6 shall not apply to Fintech Entities which are under the regulatory supervision of the Reserve Bank of India, the Securities and Exchange Board of India or the Insurance and Regulatory Development Authority but are not required to follow any security standards specifically prescribed by said authorities.

Expl: The explanation clarifies that if a Fintech Entity is governed by security standards prescribed by the RBI, SEBI or IRDA, which may have their own security standards for entities regulated by them, then such entities do not have to comply with these guidelines.

7. Applicability of other Rules

Subject to the provisions of these Rules, Qualified Fintech Entities shall comply with the provisions contained in Rules 4 (*Body corporate to provide policy for privacy and disclosure of information*), 5 (*Collection of Information*), 6 (*Disclosure of Information*) and 7 (*Transfer of Information*) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Expl: These Rules were drafted with the limited scope of coming up with a specific set of data protection standards for the Fintech sector. We have made certain assumptions which include adequacy of the provisions relating to privacy policy, collection, transfer or disclosure (Rules 4, 5, 6, and 7) under the SPDI Rules. A detailed revisions of those provisions is outside of the scope of this project. Further, such a detailed revision may turn these rules into another Data Protection Act, which is not the aim of this exercise.

SCHEDULE I

FINTECH SECURITY GUIDELINES

Every Qualified Fintech Entity shall put in place procedures and processes to ensure robust information security procedures as specified below:

1. IT Governance

IT governance should be overseen by senior members of the management, particularly the CEO and CIO. Every Qualified Fintech Entity must have a person designated as the Chief Information Officer (CIO). The person designated as CIO may also hold other designations. These members must oversee and manage IT strategy and policy with a strategic planning process.

IT policies and procedures must:

- lay down standards for hardware or software prescribed by the proposed architecture;
- lay down strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development;
- detail operational procedures for IT infrastructure, such as data centre operations;
- implement appropriate measures to ensure adherence to customer privacy requirements applicable to relevant jurisdictions;
- implement appropriate measures to comply with legislative, regulatory and contractual requirements on the use of systems and software where IPR, copyrights and on the use of proprietary software products are applicable;
- consider inter-dependencies between risk elements in the risk assessment process;
- ensure procedures to assess the integration and interoperability of complex IT processes (such as problem, change and configuration management) exists.

2.Information Security Governance

Information Security (or Infosec) governance as an area of IT governance, must consider information security as a critical strand of business strategy, with appropriate measuring, monitoring and reporting of InfoSec parameters, and the management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level.

A comprehensive security programme needs to include the following main activities:

- Development and ongoing maintenance of security policies;

- Sharing of roles, responsibilities and accountability for information security across the organization;
- Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures;
- Periodic risk assessments and ensuring adequate, effective and tested controls for people, processes and technology to enhance information security;
- Ensuring security is integral to all organizational processes;
- Processes to monitor security incidents;
- Effective identity and access management processes;
- Generation of meaningful metrics of security performance.

A senior level official who has the necessary levels of access in the enterprise, working with the CIO, should be designated as Chief Information Security Officer, responsible for articulating and enforcing the policies that FinTech companies must use to protect their information assets apart from coordinating the security related issues/implementation within the organization as well as relevant external agencies.

3. Critical components of information security

1.Policies and Procedures

In addition to those mentioned in section 1 extended to InfoSec, there are other specific considerations:

(i) Identification, authorisation and granting of access to IT assets (by individuals and other IT assets)[23];

(ii) Addressing the various stages of an IT asset's life to ensure that information security requirements are considered at each stage of the lifecycle[24];

(iii) Management of technology solutions for information security like a firewall, anti-virus/anti-malware software, intrusion detection/prevention systems, cryptographic systems and monitoring/log analysis tools/techniques[25];

[23] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 15.
[24] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 15.
[25] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 15.

(iv) Clearly indicating acceptable usage of IT assets including application systems that define the information security responsibilities of users (staff, service providers and customers) in regard to the use of IT assets[26];

(v) Exception policy for handling instances of non-compliance with the information security policy;[27]

(vi) Penal measures for violation of policies and the process to be followed in the event of violation.[28]

2. Risk Assessment

The risk assessment for the enterprise must, for each asset - physical, informational, computer, and/or digital etc - within its scope, identify the threat/vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance or contractual perspective.

3. Defining roles and responsibilities

All defined and documented responsibilities and accountabilities must be established and communicated to all relevant personnel and management.

4. Access Control

(i) Access to information assets needs to be authorised by an enterprise only where a valid business need exists and only for the specific time period that the access is required. The various factors that need to be considered when authorising access to users and information assets, inter-alia, include business role, physical location, method of connectivity, remote access, time, anti-malware and patch updation status, nature of device used and software /operating system[29].

(ii) A mutual authentication system may be considered[30].

(iii) Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures.

[26] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 15.
[27] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 14.
[28] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 15.
[29] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 19.
[30] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 20.

5. Design Controls

Planning and design level controls need to be in place to ensure that information security is embodied in the overall information systems architecture and the implemented solutions are in compliance with the information security policies and requirements of the enterprise.

6. Personnel security

Personnel-driven risk must be mitigated through background checks and verifications, and verification of government ID. There also needs to be a periodic rotation of duties among users or personnel as a prudent risk measure. [31]

7. Physical security

Physical security of the data is to be maintained by ensuring that there is no unauthorised access to the equipment that contains personal data. This may be achieved through the following:

(A) In cases where the equipment containing personal data is within the possession and control of the Qualified Fintech Entity:

(i) Physical security risks are to be mitigated through zone-oriented implementations that are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone.[32]

(ii) The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but is not limited to, threats like chemical effects, dust, electrical supply interference, electromagnetic radiation, explosives, fire, smoke, theft/destruction, vibration/earthquake, water, criminals, terrorism, political issues (e.g. strikes, disruptions) and other threats based on the entity's unique geographical location, building configuration, neighboring environment/entities, etc[33].

(iii) An enterprise needs to deploy the following environmental controls with adequate protection measures:

- Secure location of critical assets providing protection from natural and man-made threats;

[31] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 22.
[32] Ibid.
[33] *Supra* 36 at 22.

- Restrict access to sensitive areas like data centres, which also includes detailed procedures for handling access by staff, third party providers and visitors;
- Monitoring mechanisms for the detection of compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access log reviews, etc.[34]

(B) In cases where the equipment containing personal data is not within the possession and control of the Qualified Fintech Entity, by ensuring that the third party which provides the service to the Qualified Fintech Entity adopts practices to ensure the physical security of the equipment which are commensurate with or as effective as those specified in Clause (A) above.

8. User Training and Awareness

There needs to be initial, and periodic, security and confidentiality training for all employees, appropriate to their roles and responsibilities[35].

9. Incident management

(i) Common incident types include, but not limited to, outages/degradation of services due to hardware, software or capacity issues, unauthorised access to systems, identity theft, data leakage/loss, malicious software and hardware, failed backup processes, denial of service attacks and data integrity issues.[36]

(ii) Major activities that need to be considered as part of the incident management framework include:

a. Developing and implementing processes for preventing, detecting, analyzing and responding to information security incidents

b. Establishing escalation and communication processes and lines of authority

c. Developing plans to respond to and document information security incidents

d. Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.

e. Developing a process to communicate with internal parties and external organizations (e.g., regulator, media, law enforcement, customers)

f. Organizing, training and equipping teams to respond to information security incidents

[34] *Supra* 36 at 22.
[35] *Supra* 36 at 22.
[36] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 23.

g. Periodically testing and refining information security incident response plans

h. Conducting post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future[37].

(iii) Incident management strategies would also typically assist in compliance with regulatory requirements. Institutions would also need to proactively notify CERT-In/IDRBT/RBI regarding cyber security incidents[38].

(iv) All security incidents or violations of security policies should be brought to the notice of the CISO[39].

10. Encryption

(i) Typical areas or situations requiring deployment of cryptographic techniques, given the risks involved, include transmission and storage of critical and/or sensitive data/information in an 'untrusted' environment or where a higher degree of security is required, detection of any unauthorised alteration of data/information and verification of the authenticity of transactions or data/information[40].

(ii) Since security is primarily based on the encryption keys, effective key management is crucial. Effective key management systems are based on an agreed set of standards, procedures, and secure methods that address key generation, storage, confidentiality, and recovery.

11. Data security

(i) Qualified Fintech Entities need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives, as indicated throughout.[41]

(ii) Policies regarding media handling, disposal, and transit should be implemented to enable the use of protection profiles and otherwise mitigate risks to data[42].

[37] *Ibid.*
[38] *Supra* 42 at 23.
[39] *Supra* 42 at 23.
[40] RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber frauds, 2011, Page 48.
[41] RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber frauds, 2011, Page 29.
[42] RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber frauds, 2011, Page 30.

(iii) Appropriate disposal techniques for both electronic and physical media should be applied to sensitive data like physical destruction, overwriting data, degaussing etc[43].

(iv) Qualified Fintech Entities should encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

(v) Data leak prevention (DLP) mechanisms may be implemented to:

- Locate and catalogue sensitive information stored throughout the enterprise;
- Monitor and control the movement of sensitive information across enterprise networks;
- Monitor and control the movement of sensitive information on end-user systems.

12. Vulnerability Assessment[44]

(i) Automated vulnerability scanning tools need to be used against all systems on enterprise networks on a periodic basis.

(ii) Qualified Fintech Entities should ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at least quarterly.

(iii) Vulnerability assessments must generally accept a low level of business risk.

(iv) The security function should have updated status regarding numbers of unmitigated, critical vulnerabilities, plan for mitigation and should share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation.

13. Establishing on-going security monitoring processes[45]

(i) Industry standard monitoring mechanisms may be implemented to log user, application, and network activity amongst other things across systems and infrastructure.

(ii) On a periodic basis, say monthly or quarterly basis, entities should review user and employee credentials to ensure they are up-to-date, and disable inactive credentials.

(iii) Qualified Fintech Entities also need to proactively monitor various authentic sources like CERT-In, security vendors, etc. for any security related advisories and take suitable measures accordingly.

[43] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 30.
[44] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 31.
[45] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 31-32.

14. Security measures against Malware[46]

(i) Controls against malware and other malicious resources should be implemented through a combination of technology, policies and procedures and training at systems (hardware and software), network, and user level. This may be by implementing technological solutions such as firewalls, IDS, anti-malware software etc., in addition to training and awareness programs for users.

(ii) In addition to system-wide antivirus/anti-malware software, logs from firewalls, intrusion detection and prevention sensors, DNS servers and proxy server logs should be monitored on a daily basis for signs of worm infections and/or unusual network traffic

(iii) Email Attachment Filtering - Qualified Fintech Entities should filter various attachment types at the email gateway, unless required for specific business use.

15. Patch Management[47]

(i) An adequate patch and update management process needs to be in place to continuously address and mitigate technical system and software vulnerabilities quickly and effectively.

(ii) Organizations should measure the delay in patching new vulnerabilities and ensure the delay is not beyond the benchmarks set forth by the organization, which should be less for critical patches, say not more than a week.

(iii) Critical patches must be evaluated in a test environment before being updated into production on enterprise systems.

16. Change Management[48]

A change management process should be established, which covers all types of change. For example, upgrades and modifications to application and software, modifications to business information, emergency 'fixes', and changes to the computers/networks that support the application.

17. Audit trails[49]

[46] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 33-34.
[47] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 35.
[48] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 35.
[49] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 36.

(i) Qualified Fintech Entities must implement audit logging and should validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each transaction. These logs need to be retained for a period of at least 3 years.

(ii) Qualified Fintech Entities need to ensure that audit trails exist for IT assets satisfying business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. This could include, as applicable, various areas like transaction with financial consequences, the opening, modifications or closing of customer accounts, modifications in sensitive master data, accessing or copying of sensitive data/information; and granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.

(iii) Audit trails should be secured to ensure the integrity of the information through technological or other means. Retention of audit trails should be in line with business, regulatory and legal requirements.

18. Network Security[50]

Qualified Fintech Entities need to implement technology, policies and procedures to ensure adequate network. Network security revolves around the three key principles viz. confidentiality, integrity, and availability:

(i) Confidentiality - Confidentiality is concerned with preventing the unauthorized disclosure of sensitive information. Such disclosure may be intentional, such as breaking a cipher and reading the information, or it might be unintentional, such as due to the carelessness or incompetence of individuals handling the information.

(ii) Integrity - Integrity has three goals: (a) Preventing the modification of information by unauthorized users; (b) Preventing the unauthorized or unintentional modification of information by authorized users; and (c) Preserving the internal and external consistency.[51]

Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system and to the network.

[50] *Eric Cole*, "Network Security Bible", Second Edition, 2009, John Wiley & Sons, Chapter 4 - Information System Security Principles.

[51] Internal consistency ensures that internal data is consistent. For example, in an organizational database, the total number of items owned by an organization must equal the sum of the same items shown in the database as being held by each element of the organization.External consistency ensures that the data stored in the database is consistent with the real world. Relative to the previous example, the total number of items physically sitting on the shelf must equal the total number of items indicated by the database.

(iii) Availability - Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system and to the network.

19. Remote Access[52]

Good controls for remote access include the following actions:

(i) Disallowing remote access by policy and practice unless a compelling business need exists. Here, management approval would be required for remote access;

(ii) Regularly review remote access approvals and rescind those that no longer have a compelling business justification;

(iii) Appropriately and in a timely manner patching, updating and maintaining all software on remote access devices;

(iv) Implement secure hardware / software technologies to secure remote access, including measures such as encryption, VLANs, VPNs, 2FA etc.

(v) Maintaining strong audit mechanisms for remote access actions.

23. Wireless Security[53]

(i) Alongside extensive use of encryption to authenticate users and devices and to shield communications, wireless networks are recommended to use additional controls such as:

- Treating wireless networks as untrusted networks, allowing access through protective devices similar to those used to shield the internal network from the Internet environment;
- Using end-to-end encryption in addition to the encryption provided by the wireless connection;
- Using strong authentication and configuration controls at the access points and on all clients;
- Using an application server and dumb terminals;
- Shielding the area in which the wireless LAN operates to protect against stray emissions and signal interference;
- Monitoring and responding to unauthorized wireless access points and clients.

[52] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 46-47.

[53] RBI Guidelines on Information security, Electronic Banking, Technology risk management and Cyber frauds, 2011, Page 48-49.

(ii) All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by Information Security functionary of the enterprise. These Access Points / Base Stations need to subjected to periodic penetration tests and audits. Access points/Wireless NIC should not be installed /enabled on a bank's network without the approval of information security function.

(iii) Each wireless device connected to the network must match an authorized configuration and security profile, with a documented owner of the connection and a defined business need, or be denied access

(iv) Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.

(v) For devices that do not have an essential wireless business purpose, organizations should consider disabling wireless access in the hardware configuration (BIOS or EFI), with password protections to lower the possibility that the user will override such configurations.

(vi) Organizations should ensure all wireless traffic leverages industry standard encryption protocols.