asifma
Growing Asia's Markets

28 March 2019

Department for Promotion of Industry and Internal Trade
Udyog Bhawan
New Delhi 110011
INDIA

Cc: SEBI, RBI, Ministry of Finance

To Whom it May Concern,

Re: Concerns of International Financial Services Institutions Regarding Current Drafting of India's National e-Commerce Policy

The Asia Securities Industry & Financial Markets Association (**ASIFMA**)[1] and its members are grateful for the opportunity to comment on the Department for Promotion of Industry and Internal Trade of India's Draft National e-Commerce Policy (the "Policy").

ASIFMA represents a diverse range of leading financial institutions including banks, asset managers, law firms and market infrastructure service providers – many of which have a deep and keen interest in engaging with India's capital markets, including offering services and facilitating investment into India to support and grow an efficient and competitive national economy. India is a key player in the international banking ecosystem, and a well-established and respected outsourcing location for many of our members' global banking operations.

While we admire and respect the Indian Government's objective to enable its citizens to benefit fully from ongoing digitization of commerce and acknowledge the need for governments to consider measures to protect the security and integrity of consumer data, we have concerns with the current drafting of the Policy.

ASIFMA is concerned with the limited detail on how this policy will be implemented in practice. We are particularly concerned that, as drafted, the scope of the Policy is extremely broad. While the Policy seeks to target non-financial, commerce and/or trade activities conducted using electronic platforms, the definition in the drafting captures financial services offered online, including financial institutions' electronic platforms – which are already regulated with respect to the safe handling of data and protection of customer confidentiality.

[1] ASIFMA is an independent, regional trade association with over 100 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

ASIA SECURITIES INDUSTRY & FINANCIAL MARKETS ASSOCIATION | Unit 3603, Tower 2 Lippo Centre | 89 Queensway Admiralty, Hong Kong | Tel: +852 2531 6500 www.asifma.org

Specifically, banks' financial services offerings and the electronic platforms on which they are offered are today subject to regulatory requirements under the Reserve Bank of India's (RBI) Electronic Trading Platforms Directions (2018)[2] which the industry is working to implement. Further, financial institutions are already subject to other sectoral regulations, such as Securities and Exchange Board of India's (SEBI) rules on the protection of customer confidentiality.

Whether it is the intention of the Policy or not, subjecting the financial sector to overlapping national and sectoral rules introduces unnecessary complexity and substantial regulatory uncertainty for financial services institutions. As a general principle, good policymaking seeks to ensure conflicting and/or duplicative requirements are avoided.

Therefore, we propose specifically excluding the financial services industry from the scope of the Policy, given that the financial services industry is already subject to RBI and SEBI supervision and requirements regarding the safe handling of data and customer confidentiality. At a minimum, if the industry is not excluded, rules resulting from this policy that apply to regulated financial services, should only be issued by RBI and SEBI which have the appropriate oversight and expertise in sector specific issues, as well as established relations with financial services providers. This will avoid unnecessary disruption and minimises the potential for conflicting requirements. RBI and SEBI (and indeed the Ministry of Finance) may then liaise with the Department for Promotion of Industry and Internal Trade on policy outcomes.

In addition to excluding the financial services sector from the Policy's scope, we further propose specific exclusion of select key banking infrastructure such as the global SWIFT network that today underpins the Indian banking and financial industry on both regional and international levels, enabling for substantial market efficiencies.

Separate to the above, ASIFMA seeks to draw your attention to the Global Financial Market Association's recently released 'International Principles to Improve Data Security and Mobility'[3] paper, which we provide alongside this letter. This sets out the emergence of digital economies and the importance of protecting consumers, investors and the integrity of financial data in a global context, before offering five critical considerations policymakers and regulators must take into account when seeking to protect consumer and investor privacy while supporting flows of information necessary to support national competitiveness in newly emerging areas of trade and commerce. Such principles may be helpful in the future development of India's National e-Commerce Policy and, for convenience, I have summarised them overleaf.

The inherent interconnectivity of digital commerce, for example, is what drives added benefits for existing economies. In order to reap these benefits and create a sustainable way forward, cooperative agreements between governments on cross-border enforcement, supervision and data sharing in addition to consumer protection is a critical first step. This will enable knowledge-based economies such as India to reap the scale and network benefits from tapping the global digital economy.

[2] Available online **here**.
[3] Available online **here**.

ASIFMA would of course welcome the opportunity to discuss any of the matters raised here with the Department for Promotion of Industry and Internal Trade and other agencies of the Indian Government. If you have any further questions, please contact me (mausten@asifma.org or +852 2531 6510) or Matthew Chan, ASIFMA's Executive Director and Head of Policy and Regulatory Affairs, at mchan@asifma.org or +852 2531 6560.

Sincerely,

Mark Austen
Chief Executive Officer
Asia Securities Industry & Financial Markets Association

International Principles to Improve Data Privacy, Security and Mobility

The financial services industry supports global regulatory authorities' legitimate concerns to protect the privacy of consumers and investors and the integrity of financial data. We encourage global regulators to consider the following principles and adopt best practices to improve data protection and mobility—which we believe are mutually reinforcing—while continuing to foster data privacy.

- 21 March 2019 -

1. ***Recognize that the ability to transmit data across national boundaries and store data in different jurisdictions, with adequate protections, is fundamental to supporting a secure, innovative, and prosperous global financial system, as well as fostering global economic growth.*** *Policymakers have a significant interest in reducing barriers to safe and efficient data flow to create an enabling environment to grow the digital economy. Regulations and legal requirements on data protection can function as non-tariff barriers to trade and restrict economic activity when they are not aligned with international standards and best practices. By recognizing the impact that privacy and data protection policies have on international trade and investment, policymakers can tailor their approach to meet their objectives to protect individuals' rights to privacy while also bolstering the fight against financial crime and enabling economic growth. Policymakers should support common frameworks that multinational financial institutions can implement in a global operating environment. Cooperative agreements between governments on cross-border enforcement, supervision and data sharing can be put in place to support access to data, while addressing financial market integrity and sovereign risks. Developing interoperability between the privacy laws and regulations of different jurisdictions, such as APEC has done through the Cross-Border Privacy Rule, enables safe and efficient cross-border data flow to improve international trade, catalyze investment, and bolster the uptake of digital channels for trade. For example, as Brexit approaches it is essential that there is clarity as to the ability of business to continue to transfer personal data between the EU and UK.*

2. ***Engage with industry to align regulatory requirements and encourage adoption of international best practice in data security and mobility.*** *We encourage governments to consult financial services institutions to better understand standards and best practices used to protect data as it is stored and transferred across borders. Eliciting private sector input prior to formulating regulations for privacy and data protection could avoid unintended consequences for trade, investment and economic growth. We also encourage policymakers to reference existing frameworks for managing cybersecurity risk. ISO 27103, the NIST CSF and the Financial Services Sector Profile represent aligned risk management frameworks at the international, national and sector specific levels. We also encourage further adoption of the "International Principles for Cybersecurity, Data and Technology."16 The path forward in an increasingly digital and technology advanced world includes cooperative agreements between governments to address cross-border resilience, privacy and security, and of markets keen to develop and/or mature their digital-related frameworks and capacity, instead of data localization requirements." Generally speaking, regulators should develop alternative approaches to data localization policies.*

3. ***Recognize that, with adequate control and supervision, cross-border data mobility supports data protection and system resilience.*** *Well-intentioned, overly restrictive data localization rules may in fact undermine the resilience of the global financial system and individual institutions. Privacy cannot be protected without effective security, which depends on how data is shared and stored, not where. Processing and sharing appropriate consumer data across borders is critical to preventing abuse, particularly in the context of cybersecurity and sanctions/anti-money laundering enforcement. Undue limitations on cross-border data access inhibit firms' ability to effectively set and enforce technology controls, monitor threats to company networks and infrastructure, and share information with partners and law enforcement agencies to mitigate broader systemic risks. In addition, requirements to store data in fragmented or disparate facilities can create additional points of entry for bad actors to infiltrate networks. Outsourced or consolidate regional data centers or information technology (IT) hubs enable firms to dedicate resources to data and technology security, and ensure there are robust resilience capabilities, such as for data back-ups. In that way, data localization adversely affects firms' business continuity and disaster recovery plans.*

4. ***Enable targeted cross-border information sharing.*** *Financial institutions must provide appropriate, timely data to regulators to fulfil their regulatory obligations in different jurisdictions. Restrictions on cross-border data flow can introduce compliance risk for firms, as privacy laws and blocking statutes introduce conflicts of law for multinational firms subject to multiple regulatory reporting regimes. Accordingly, data localization policies can prevent financial regulators from having the data necessary to do their jobs effectively, as well as undermine firms' efforts to comply with regulatory requirements. For instance, financial institutions need to share information with their affiliates across borders to obtain information necessary to file suspicious activity reports (SARs) under relevant AML regulations applicable worldwide. We call on policymakers to be mindful of the impact that data localization policies have on firms' abilities to continue to carry out important investor protection protocols, including AML, KYC, or financial crime investigations. We encourage data protection authorities to coordinate with other financial crime and cyber authorities when defining parameters for the use of data to allow targeted cross-border data transfer necessary to fulfil regulatory obligations and enhance investor protection.*

5. ***Enable adequately secure outsourcing arrangements that improve the efficiency and competitiveness of financial services providers.*** *Outsourcing arrangements are critical to improving the efficiency of the financial services industry, enabling firms to provide superior customer service, maintain competitiveness internationally, and reduce operational costs to boost investments in other areas that deepen local capital markets. Multinational financial institutions often outsource operationally-intensive functions to other affiliates within their group to leverage in-house capabilities in a competitive, efficient, and effective manner. Doing so improves efficiency by enabling financial institutions to maximize use of existing infrastructure, and in turn, increase investments in more productive ways. However, policies that restrict outsourcing arrangements in the financial services sector often result in the de facto localization of data onshore, which deters firms from entering or expanding in a market, undermining economic growth and disadvantaging local consumers. Subject to other overarching regulatory requirements, policies governing outsourcing should be principles-based, technology and entity neutral, and impartial to geographic location, to allow financial institutions to utilize outsourcing arrangements according to their own business models and risks whereas the relevant authorities should not look to introduce new requirements or restrictions beyond existing outsourcing regulations.*

Available online at http://www.gfma.org/correspondence/item.aspx?id=1064