asifma
Growing Asia's Markets

18 April 2019

Mr. Randal K. Quarles
Chair of the Financial Stability Board
Board of Governors of the Federal Reserve System
Constitution Ave NW & 20th Street NW Washington, D.C. 20551

Mr. Klaas H.W. Knot
Vice Chair of the Financial Stability Board
De Nederlandsche Bank
Postbus 98
1000 AB Amsterdam
Westeinde 1, 1017 ZN

Mr. Ashley Alder
Chair of IOSCO
35/F, Cheung Kong Center, 2 Queen's Road
Central, 000
Hong Kong

Mr. Masatsugu Asakawa
Vice Minister of Finance for International Affairs
Ministry of Finance
3-1-1 Kasumigaseki
Chiyoda-ku
Tokyo 100-8940

Mr. Ryozo Himino
Vice Minister for International Affairs
Financial Services Agency
3-2-1 Kasumigaseki
Chiyoda-ku
Tokyo 100-8967

Mr. Kimihiro Etoh
Executive Director in charge of Financial Stability
Bank of Japan
2-1-1 Nihonbashi-Hongokucho
Chuo-ku
Tokyo

Mr. Shinichi Uchida
Assistant Governor
Bank of Japan
2-1-1 Nihonbashi-Hongokucho
Chuo-ku
Tokyo

Addressing Fragmentation in Asian Markets: Data Localisation – GFMA's Data Privacy, Security and Mobility Principles

Dear Sirs,

Following our letter dated 28 February 2019 to the Japan G20 Presidency, the International Organization of Securities Commissions and to the Financial Stability Board, the Asia Securities Industry & Financial Markets Association (ASIFMA)[1] seeks to share an important set of principles for Data Privacy, Security and Mobility, which we have developed recently along with the Association for Financial Markets in Europe (AFME) and the Securities Industry and Financial Markets Association (SIFMA) as part of the Global Financial Market Association (GFMA) alliance.

[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

These principles were written in response to the financial services industry's significant concerns regarding the increasing trend towards the introduction of data localisation requirements by national regulators that impact financial institutions which are already well regulated to ensure governance, systems and controls are in place to protect client interests, confidentiality, information security and data integrity in the delivery of financial services.

Increasing regulatory focus on data stems from concerns regarding privacy and data security among non-regulated entities in the broader economy; however, in the context of already regulated financial institutions poorly targeted data localisation rules can in fact *undermine* the resilience and security of financial systems and institutions. Further, incompatible new restrictions introduce conflicts of law in areas such as anti-money laundering (AML) safeguards where, for instance, international financial institutions need to share information across affiliates and jurisdictions to generate information necessary to file suspicious activity reports. Concerning examples of data localisation in the Asia Pacific region include China's Cybersecurity Law, India's draft Personal Data Protection Bill, Vietnam's Law on Cybersecurity, and Indonesia's Government Regulation No. 82/2012.

GFMA's 'International Principles to Improve Data Security and Mobility'[2] paper, which we provide alongside this letter, offer 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 a secure, efficient, and well-functioning international financial services sector. We put forward the principles as an important starting point for the development of international standards in this important area and, for convenience, I summarise them overleaf.

The financial services industry understands regulatory authorities' concerns regarding the protection and integrity of consumer data in the broader and largely unregulated digital economy. However, we believe rules on the use and processing of data need to be developed thoughtfully, taking into account cost-benefit considerations, overlaps and conflicts with existing requirements for regulated sectors such as financial services, and evolving international best practice in relation to the storage and security of data. There are alternative solutions that address privacy and data concerns effectively without requiring data localisation. We urge the G20, FSB and IOSCO to help protect international capital flows by encouraging more constructive approaches to data protection, including multilateral cooperative agreements between governments on cross-border enforcement, supervision and data sharing, in line with GFMA's Principles. As a starting point, policies on cybersecurity and/or data protection must take into consideration existing banking requirements on confidentiality and data protection and the interaction between national and sectoral regulations, excluding regulated sectors like banking as appropriate.

ASIFMA welcomes the opportunity to discuss any of the matters raised. If you have any 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 (mchan@asifma.org or +852 2531 6560).

Sincerely,

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

[2] Available online **here**.

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. ***Recognise 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 recognising 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, catalyse 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 localisation requirements." Generally speaking, regulators should develop alternative approaches to data localisation policies.*

3. ***Recognise that, with adequate control and supervision, cross-border data mobility supports data protection and system resilience.*** *Well-intentioned, overly restrictive data localisation 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 centres 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 localisation 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 localisation 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 localisation 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 maximise 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 localisation 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 utilise 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