



June 22, 2018

The Honorable Steven Mnuchin
U.S. Secretary of the Treasury
1500 Pennsylvania Ave. NW
Washington, DC
20220

Dear Secretary Mnuchin:

Ahead of your meetings next week with Vietnamese Deputy Prime Minister Vuong Dinh Hue, we write to share our concerns with the Cyber Security Law (the Law) which was passed by the National Assembly on 12 June. This Law will adversely affect industry and the economy of Vietnam if implemented in its current form. We encourage you to make it a priority issue during your meeting with the Deputy Prime Minister. Specifically, given the lack of advance consultation for our industry, we request that the Vietnamese authorities utilize the flexibility the Law provides to exempt financial services.

Our concerns are in relation to both the *substance* of the Law and the *process* of how it evolved from introduction to final passage.

- In terms of *substance*, the Law imposes data localization requirements and cross-border data transfer restrictions. Offshore entities will be required to have headquarters or representative offices in Vietnam and store within Vietnam (a) the personal data of users in Vietnam and (b) other important data collected and/or generated from the use of Vietnam's national cybersecurity infrastructure.
- In terms of *process*, the Law which received passage is wider ranging in its data localization requirements than the business community had previously expected. In an earlier iteration, these provisions only applied if (a) 10,000 or more Vietnamese users used such services or (b) the Government requested it. That previous iteration was consulted upon but the data localization and data transfer regulations in the final Law were not subjected to the same degree of consultation as the earlier iteration and so has not been subject to the scrutiny that good policy making should adhere to.

Washington | New York

Transferring data across borders is crucial for the financial services industry to: (i) provide core products and services to customers; (ii) manage risk on a holistic basis across affiliates and borders; and (iii) comply with financial regulatory requirements in various jurisdictions, including Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. In addition, cross-border data flows are necessary to support the development of financial technologies (fintech), including blockchain applications.

Limitations on the free flow of data have serious implications for global firms, the end-users they serve, and economic growth. Policymakers engage in these localization practices in the belief that they will improve privacy and security, or that requiring local servers or computing facilities will foster innovation, spur technology transfer, or bolster domestic economic growth. But these objectives are best pursued through the enforcement of rigorous and high-standard systems which financial services providers are happy to maintain in place.

Furthermore, data localization requirements and policies that hinder the free flow of data increase cyber risks and erect barriers to trade, competition, and innovation. Data localization not only impairs financial services firms' ability to serve their customers and the Vietnamese economy, but also negatively impacts overall data security and creates inefficiencies. Moreover, the resources required for compliance with data localization laws often deter firms from entering or expanding in a market, limiting job creation and investment. The increased costs for those firms who do enter the relevant market are passed along to consumers, reducing their access to goods and services. The costs of data localization policies ultimately constrain the rise of digital trade, as well as global economic growth. The Information Technology and Innovation Foundation estimates that barriers to cross-border data flows decrease GDP in Vietnam by 0.7 to 1.7 percent.

The financial industry supports global regulatory authorities' legitimate concerns to protect consumer and investor data privacy and security. We also recognize that financial institutions must provide appropriate data to regulators for them to perform their regulatory and supervisory roles. However, policymakers should avoid translating those objectives into measures that amount in effect to digital protectionism and do not accomplish their ostensible objectives. These measures are ineffective and have many negative implications for the digital economy and economic growth.

We therefore hope that you can share our concerns with the Cyber Security Law with Deputy Prime Minister Hue and request that the Vietnamese authorities use the flexibility in implementation that the Law affords to exempt financial services. The risks to Vietnam's economy need to be debated further and the design of the Law analyzed in relation to the evidence of data localization's negative consequences. We hope that scope can still be found for industry and the Government of Vietnam to work together to avoid the adverse consequences that will flow from the Law being implemented as presently expected.

American Council of Life Insurers (ACLI)
American Insurance Association (AIA)
Council of Insurance Agents and Brokers (CIAB)
Futures Industry Association (FIA)
The Investment Company Institute (ICI)
Securities Industry & Financial Markets Association (SIFMA)

Cc:

Douglas Bell, Treasury

Daniel Bahar, USTR

Matthew Swinehart, Treasury

Lailee Moghtader, Treasury

Sarah Ellerman, USTR