Charles R. Johnston
Director and Senior Vice President
International Government Affairs

1101 Pennsylvania Avenue NW
Suite 1000
Washington, DC 20004

T +1.202.879.6836
F +1.202.204-0974
johnstonc@citi.com

March 14, 2013

Ms. Lisa Barton
Acting Secretary
United States International Trade Commission
500 E Street, SW
Washington, DC 20436

RE: Investigation Number 332-531, Digital Trade in the U.S. and Global Economies, Part 1

Dear Ms Barton:

Pursuant to Federal Register Notice dated January 14, 2013, this letter of transmittal and attachment constitute Citi's submission for Investigation Number 332-531, Digital Trade in the U.S. and Global Economies, Part 1. This submission is non-confidential.

Should you have any questions or need further information regarding this submission, please contact me at my office number: +1(202) 879-6836.

Respectfully submitted,

Charles R. Johnston
Director and Senior Vice President
International Government Affairs
Citi

Challenges to Cross Border Data Processing of Personal Information

This paper is submitted in connection with the investigation by the U.S. International Trade Commission (USITC) into the role of digital trade in the U.S. and global economies. In particular, this submission focuses on the identification of trends in national and regional regulatory schemes that adversely impact cross border data processing and hosting operations[1] of financial institutions involving personal information. Specific discussion of the drawbacks and negative consequences which flow from implementation of such regulatory schemes is addressed. In addition, recommendations which facilitate interoperability of cross border data processing regulatory regimes and safeguard customer information are proposed.

Citigroup (Citi) offers its insights below and suggests that the U. S. International Trade Commission take these into account in its investigation. Increased interoperability will facilitate global digital trade, enhance competition and provide customers with increased choice and service quality.

I. Background: Data Processing is the Foundation to the Delivery of Citi's Global Operations and Services.

Citi has approximately 200 million customer accounts and conducts business in more than 1,000 cities in over 160 countries and jurisdictions around the globe. Citi's customer base is comprised of consumers, corporations (including the world's largest multinational corporations), governments and institutions. A broad range of financial products and services are provided to customers, including consumer banking and credit, corporate and investment banking, securities brokerage, transaction services, and wealth management. Customers rely on Citi's ability to facilitate trade and capital flows in real time in all of its locations. Citi's data processing operations are the foundation which facilitates the delivery of these products and services around the globe.

II. Types of Local Restrictions Impacting Cross Border Data Processing

As a global financial institution, Citi's data processing operations must be compliant with a wide variety of legal and regulatory requirements impacting cross border data processing of personal information in the jurisdictions in which it operates. Discussion of four trends observed in national legal requirements are considered below.

A. Restrictions Requiring Establishment of Domestic Data Centers

[1] As a preliminary matter, it should be noted that the term "processing" refers to a wide array of activities and operations on the digital continuum including collection, access, use, transfer, disclosure, storage, retention and back up operations (i.e. disaster recovery or continuity of business). Specific operations will be identified when appropriate. Data Hosting is the storing of information in a secure facility (i.e. data center) with redundant capabilities.

A number of countries have enacted laws or implemented regulations which limit the cross border transfer of data by imposing local data center restrictions which require domestic processing of customer personal information. Country requirements vary. Some countries, such as Venezuela, prohibit offshore data processing and requires that data centers reside in Venezuela. Others countries require that both the data centers and disaster recovery centers are in-country. For example, Indonesia has mandated that by October 2017, electronic service operators (a term which includes banks) onshore their data center and disaster recovery center operations. China and Argentina also have variations of local data center restrictions. Argentina restricts offshore processing except when such processing is done in the location of the head office or a subsidiary of the head office. China has a similar offshore data center restriction but the restriction is specifically limited to data processing activities that involve consumer customers as opposed to corporate customers.

Typically, local governments' stated rationale for imposing local data center restrictions is that these restrictions (i) facilitate and ensure the confidentiality and security of customer personal information and/or (ii) enhance home country regulatory supervision over inherent or core banking activities.

B. Laws Directly Regulating Cross Border Access to Personal Information

Countries can also impede cross border data processing by regulating the "disclosure" of personal information through local bank secrecy laws. Bank secrecy laws prohibit or restrict the disclosure of bank customer information to a third party. Typically, customers can waive this prohibition by consenting to the disclosure of their customer banking information. While customers can revoke their consent, the use of consents is one mechanism for the transfer of information. This is particularly true in jurisdictions that do not have a national data privacy or other comparable law.

In some jurisdictions, such as Mexico, customers can not waive bank secrecy prohibitions by consenting to the disclosure of their transactional or deposit information. Other countries, such as Poland or Panama, may permit customers to waive bank secrecy prohibitions but requirements for a compliant consent are so specific that it is impracticable to obtain customers' consent.

C. Restrictions Impacting Relationships Between Affiliates and Third Parties

Many country laws restrict processing of information between affiliates and third parties.[2] Local legal requirements, particularly those relating to data protection, bank secrecy, and outsourcing, typically do not distinguish between cross border data processing involving financial institutions and their affiliates, as opposed to data processing between financial institutions and unrelated third parties. Depending upon the jurisdiction, an affiliated service provider is subject to the same regulatory requirements concerning Privacy Notices, customer consents, contractual provisions or regulatory notifications and/or approvals as a third party service provider.

[2] For the purposes of this statement, the term "affiliates" refers to those companies that are related to one another through common ownership or control by the parent company (i.e. members of the same corporate group). By contrast, the term "third parties" refers to unaffiliated entities.

D. Divergent Data Protection Regulation

Conflicting approaches to data protection safeguards can also adversely impact the cross border transfer of personal information. The European Union's (EU) current consideration of the Draft General Data Protection Regulation[3] is another example of a regulatory regiment which, if implemented, could significantly and adversely impact cross border transfers of individual personal data in several respects. First, the Draft Regulation is extra-territorial; it imposes restrictions on conduct outside of the EU. Second, the Draft Regulation provides that the current adequacy determinations of the EU Commission and data protection authorities in support of international transfers to third countries will expire two years after the Regulation enters into force. Finally, data protection authorities will no longer have the ability to approve alternate forms of model contracts or other contractual provisions without using a new consistency mechanism which will impose an additional level of bureaucracy and delay in cross border transfers of data.

III. Drawbacks of Local Restrictions Impacting Cross Border Data Processing

A. Local Data Center Restrictions

Local data center processing does not afford customers the same benefits that would be derived from processing through large offshore mainframe environments. These regionally centralized facilities are purposely built to provide the highest level of resiliency to house information technology equipment (servers, storage, network) and provide IT services and support to Citi customers in an environmentally controlled and secure location. These centers also offer customers improved service quality such as real time processing of customer transactions and operational and technical support. Local data center restrictions prevent customers from enjoying these considerable benefits. Onshore data centers can not replicate the benefits of the large offshore mainframe environments which are, as a practical matter, extremely cost prohibitive to replicate on a national level.

Local data center restrictions contribute to increased costs and inefficiencies. They require implementation of additional layers of in-country procedures and processes to support technology or operational needs (i.e. call center operations, payroll administration, or satisfaction of reporting or compliance requirements) which would otherwise be achieved through the regional data center. Establishment of local data centers diverts funds away from implementation of new initiatives and applications to support these in-country processes and compliance activities. For example, regional restrictions do not allow financial institutions to take advantage of the efficiencies to be gained by process and system automation and implementation to achieve comprehensive auditing capability. They may also cause financial institutions to pull out operations, or decline to conduct operations, in a particular jurisdiction because of cost and staffing considerations associated with establishing a local data center.

Another drawback to local data center restrictions is that they are typically overly broad and are not very clear in describing the specific activities that they seek to prohibit. They generally do not address what

[3] The Draft General Data Protection Regulation as modified by the January 8, 2013 Albert Report (Draft Regulation).

functions are restricted. In particular, they tend not to indicate whether offshore access to customer data is permissible. This lack of clarity makes it difficult to plan operations and impede the ability of financial institutions to make optimal use of their global services to the benefit of their customers.

Local data center requirements that require that both the data center and the disaster recovery center are to be onshore do not offer customers optimal security of their personal information. Offshore placement of disaster recovery centers protects customers from domestic natural or man-made disasters. For example, onshore data center operations in the Asia Pacific's "Ring of Fire" which is composed of 75% of the world's active and dormant volcanoes, would benefit from offshore disaster recovery operations.

Local data center restrictions implemented to further the stated goal of protecting personal information do not actually further this objective and for this reason, can be counterproductive. Because the objective is to protect individual customer data, restricting offshore data processing of multinational and corporate customers is unnecessary and unduly constraining. This is particularly true in light of the fact that multinational and corporate customers expect that global platforms will be utilized to provide efficient and safe migration of information to support highly complex transactions in real time. Furthermore, with respect to protection of individual customer information, greater security of customer personal information can be provided in offshore data centers for the reasons detailed above.

Another rationale advanced for local data center restrictions is that they enhance home country regulatory supervision over inherent or core banking activity. In these cases, systems which are not used for inherent banking functions for personal and domestic corporate account holders should be permitted to be placed in offshore data centers. Examples of non-core banking functions include Risk Management, Treasury, Trade, Finance or Internet banking functions or anti-money-laundering (AML) monitoring.

In addition, numerous country regulators exercise control over offshore data processing by mandating that specific controls are put in place with respect to outsourced activity. These include obligating financial institutions to conduct due diligence of third party service providers and to execute contracts which contain sound security, informational and confidentiality protections. Appropriate controls are also established through contract requirements which mandate that the service provider (i) establish continuity of business plans, (ii) segregate customer data of the subcontracting entity from other data processed by the service provider, and (iii) give the subcontracting financial institution the right of access and inspection to the service provider's operations and records that pertain to the outsourced services. Many local country requirements impose a variant of these safeguards including Australia, Hong Kong, Indonesia, and India.

In addition to the controls identified above, in a number of countries, the banking regulator must approve the outsourcing arrangement. There is also an increasing trend among regulatory authorities to impose a requirement that a financial institution obtain a regulatory letter assuring rights of access and inspection ("Assurance Letter") over the outsourced activities. For example, in addition to imposing a number of the controls noted above, the Monetary Authority of Singapore (MAS) requires that in instances where the service provider is a regulated entity, the MAS must receive written confirmation from the service provider's supervisory authority that the MAS will be permitted rights of access to bank information and

documents, as well as rights of inspection of the service provider's premises. In light of many country regulators' ability to mandate that financial institutions implement these types of controls, local data center restrictions do not offer any discernable benefit to offset the significant adverse consequences that such restrictions can have on competition, customer service, and product and technological innovation.

B. Disclosure Restrictions Under Bank Secrecy Requirements

Bank secrecy restrictions which do not permit customer consents to disclosure of the customer's personal information result in the establishment of domestic data centers. In these situations, the drawbacks associated with local data center restrictions, discussed above, are applicable. Bank Secrecy prohibitions which impose burdensome requirements for obtaining compliant specific consents require financial institutions to develop uniquely tailored solutions to achieve compliance with local restrictions. Data processing operations involving transfers of, or access to, significant numbers of customers' personal information are adversely impacted by these unduly constraining requirements. Such restrictions inhibit efficient operations by delaying implementation of initiatives and product offerings and impede the development of global platforms which enhance competition.

C. Restrictions Impacting Relationships Between Affiliates and Third Parties

As previously noted, local requirements typically do not distinguish between cross border data processing of personal information between affiliated entities and exchanges of information between financial institutions and unrelated third parties. This approach can result in considerable delays and inefficiencies in the delivery of services to customers, implementation of innovative customer initiatives, and rendering of customer technology and operational support to enhance customer service quality. The benefits to be achieved by such treatment are far outweighed by these disadvantages and inefficiencies. As long as the affiliated entities that exchange personal information are under common control and are subject to required to adhere to similar internal policies and procedures associated with the processing of such information, there a few discernable benefits to be achieved by imposing restrictions, such as the need to obtain separate regulatory approvals for transfers of information or Assurance Letter (described in Section III A), upon these affiliates.

It should be noted that the observation that there is no need to treat an affiliate in the same manner as a third party does not mean that third party data processing poses significant additional risks in safeguarding personal information. Third party data processing is appropriate when conducted pursuant to meaningful controls. These controls, as noted above in Section III A, provide local regulators and financial institutions with an effective means to protect personal information.

D. Divergent Data Protection Regulation

The Draft EU Data Protection Regulation contains troubling aspects which if implemented, would significantly impede cross border data processing. First, the extra-territorial application of the Draft Regulation could lead other jurisdictions to implement similar provisions. In fact, since the issuance of the first Draft Regulation, the Philippines has enacted a data protection law which has extra-territorial application. Also, the move to limit the validity of adequacy determination to two years is quite

significant. Not only would this contribute to considerable uncertainty as to how transfers will be impacted but, it could require expenditure of additional costs after companies have already made significant investments associated with the development of Binding Corporate Rules (BCRs) and model contracts. The inability of data protection authorities to approve alternate forms of model contracts or other contractual provisions without using the consistency mechanism also contributes to this increased level of uncertainty. Finally, compliance with financial and reporting requirements, including anti-money laundering requirements and obligations to protect customers from financial loss and crime, could be adversely impacted by these changes proposed by the Draft Regulation and could require country-tailored solutions to achieve compliance with local restrictions.

IV. Recommendations

Citi appreciates this opportunity to present its views on the trends in regulatory schemes that adversely impact cross border data processing and hosting operations of financial institutions involving personal information. A balanced approach to the regulation of cross border data processing which incorporates the following recommendations would protect the confidentiality and security of customer information while at the same time enabling financial institutions to utilize their global data processing networks to deliver services and products in an efficient and competitive manner.

1. A primary goal of any regulatory scheme concerning cross border data processing should be the establishment of global interoperability of national legal and regulatory requirements applicable to cross border data transfers and data processing.

2. Local data center restrictions should be discouraged and permit data processing in locations which support optimal security, resiliency, confidentiality of customer information and technical and operational support.

3. If local data center restrictions are to be utilized, they should be clear and narrowly tailored to address a specific need. For example, restrictions which seek to achieve protection of customer information should not require onshore processing of corporate customer information. Similarly, local data center restrictions which seek to protect the regulatory authorities' ability to supervise core banking activities should not require onshore processing of non-core activities.

4. Offshore placement of disaster recovery operations should be encouraged to offer customers optimal security of their personal information to mitigate the adverse consequences of natural or man made disasters.

5. Regulatory schemes should recognize that financial institutions have greater control mechanisms in place with respect to affiliate transactions than with unrelated parties. As long as the affiliate is subject to the same institutional controls as the transferring entity, separate approval processes should not be required in order to transfer personal information between affiliates.

6. A regulatory framework which encourages the use of Assurance Letters by country regulators and mandates the establishment of appropriate contractual controls provide country regulators with the ability to (i) safeguard customer data, (ii) retain regulatory supervision over outsourced activity, and

(iii) avoid the adverse consequences that local data center restrictions can have on competition, customer service, and product and technological innovation.

7. Customer choice and consent should be recognized and encouraged.

8. Sector specific regulation should be considered when designing any new legal or regulatory requirements.