



Invested in America

June 6, 2012

The Honorable Lael Brainard
Under Secretary for International Affairs
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

Dear Ms. Brainard:

Re: European Commission Proposed Data Protection Regulations (2012/0011)

The Securities Industry and Financial Markets Association (“SIFMA”)¹ appreciates the opportunity to provide comments on the European Commission’s proposed General Data Protection Regulation (“Regulation”), published on January 25, 2012. The Regulation contains proposed new rules on applicable law governing the protection of individuals with regard to the data processing of personal data and on the free movement of such data. Our members support many of the objectives behind the Regulation, including improved legal certainty and reduced administrative burdens on companies. Unfortunately, the proposed new rules fall short in many important respects. As drafted, the Regulation is overly broad because of its focus on internet service providers (“ISPs”) and would potentially apply to U.S. financial institutions that have no reasonable expectation of being subject to European laws.

SIFMA represents financial institutions including broker-dealers, banks, asset managers and other participants in the global financial markets. SIFMA is a member of GFMA, along with the Association for Financial Markets in Europe (“AFME”), which previously communicated comments related to the Regulation to the U.K. Ministry of Justice on March 6, 2012.² SIFMA and AFME have consistently raised concerns about legislative and regulatory reforms that are duplicative or in conflict with existing requirements which could cause fragmented transatlantic capital markets.

SIFMA is concerned the Regulation is targeted at unregulated industry sectors, but applies

¹ SIFMA brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA’s mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (“GFMA”). More information about SIFMA is available at <http://www.sifma.org>.

² Letter from AFME and BBA to Ministry of Justice (March 6, 2012), available here www.bba.org.uk/download/7512

equally to the financial services industry which is already subject stringent regulation and oversight in both the United States and EU. These legal and regulatory requirements are specifically tailored to address the unique nature of the financial services industry, which includes the protection of client data, as well as issues relating to market integrity and stability. Financial services regulation has evolved to take account of the specific characteristics of financial products and services, and the resulting regulations strike a balance between consumer and industry interests.

We recognize the importance of robust and relevant privacy and data security protections for all industry sectors but believe strongly that any regulation, whether in the United States or globally, should take into account that legal, policy and privacy frameworks vary considerably around the world. Data protection laws are at different stages of development across the globe, which creates significant challenges for multi-national businesses because they must comply with numerous and differing (and sometimes conflicting) local laws and regulations.³ Ideally, any changes to data privacy regulation would be globally consistent and interoperable. Such consistency would increase compliance, promote international competitiveness and reduce companies' costs. At a minimum, any new requirements must be carefully analyzed in the context of the existing framework to avoid unintended consequences and barriers to information flows, which would constrain continued trade and economic growth.

In addition to these general comments, we outline below some of our specific concerns with the European Commission's proposal which have extraterritorial impact and provide some possible solutions. We would welcome the opportunity to meet with you to discuss these issues further.

Areas of Concern

A. "Offering of goods and services" is too broad and could include passive sales

The proposed Regulation would apply to entities located outside the EU that "offer goods or services" to EU residents (art. 3(2)(a)). The term "offering services" could include situations where a U.S. financial institution has an account holder resident in Europe, but takes no affirmative steps to market to EU residents (*i.e.*, the U.S.-based firm does not advertise in Europe, does not offer a local website in the jurisdiction, etc.). Because of European banking and insurance regulations, SIFMA members are not permitted to market financial services in Europe directly without becoming subject to local registration requirements. Nevertheless, many SIFMA members have customers who are resident in Europe for any number of reasons. Under its current drafting, the proposed Regulation would apply to such instances. Here are a few illustrative examples:

³ Notably, the Regulation is just one of many data protection proposals undergoing revision. The Organization for Economic Cooperation and Development (OECD) initiated a review of their model framework last year while the Asia-Pacific Economic Cooperation Forum (APEC) is currently working on new cross-border implementation arrangements. Additionally, the Administration has developed its own privacy blueprint and is working with the Federal Trade Commission and the Commerce Department to promote these principles. It should also be noted that Taiwan, Singapore and the Philippines just passed new privacy laws which come into force this year.

Example 1: Mr. Jones, a U.S. citizen and resident, holds an account with a U.S. bank. Mr. Jones is sent to Europe for his job. The U.S. bank continues to provide services to Mr. Jones. In that situation, the U.S. financial institution is “offering services” to an EU resident, thereby bringing the U.S. financial institution within the applicable law rules of the Regulation.

Example 2: Ms. Bernard, a French resident, purchases an apartment in Florida, and contracts a mortgage loan with a U.S. bank. The U.S. bank is offering services to Ms. Bernard and is therefore subject to the Regulation.

Example 3: Mr. Weber, a German resident, sees an advert for a credit card on the U.S. website of a U.S. bank. Mr. Weber provides the address of his Palm Beach holiday apartment. If the U.S. bank processes his application, it is offering services to Mr. Weber and is subject to the Regulation.

In all of these examples, the U.S. bank has taken no affirmative steps to market to EU individuals and would have no reasonable expectation that EU law would apply. As a result, SIFMA believes that the criteria for “offering services” to EU residents are too broad. The language of the proposed Regulation should be modified to state that it applies to non-EU firms that “target” or “hold themselves out” to EU residents, instead of firms that “offer services” to EU residents. If the current wording were to be maintained, U.S. financial institutions would be improperly drawn into the EU Regulation in circumstances when they have no reasonable nexus with Europe.

B. “Monitoring of behaviour” could include U.S. bank anti-money laundering operations

Under the current language of the proposed Regulation, the Regulation would apply to any non-EU entity, in all sectors of the economy, that monitors the behavior of EU residents (art. 3(2)(b)). Under U.S. anti-money laundering laws, U.S. financial institutions must implement systems that monitor transaction activity in order to detect suspicious conduct. These monitoring systems will inevitably monitor behavior of EU residents, even in situations where the U.S. financial institution has no EU customers. For example, if a French student attending school in the United States receives a monthly wire transfer from his parents in France, the student’s U.S. bank will implement a transaction monitoring system in accordance with U.S. law. The system creates a risk profile corresponding to the wire transfers that the student receives from his parents, characterizing the transfers as “low risk.” Because the system indirectly monitors behavior of the parents, the Regulation would apply.

To avoid this conflict of regulations, SIFMA recommends that the “monitoring” criteria be deleted from the draft Regulation or, in the alternative, a safe harbour should be created to exclude any monitoring that is implemented pursuant to legal or regulatory requirements.

C. The Regulation would apply if U.S. financial institutions use a processor in Europe

Article 3(1) states that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a processor in the Union. U.S. financial institutions may use data processors located in the EU to process personal data related to non-EU individuals. This provision raises the question of whether the use of an EU processor will subject the U.S. financial institution to the Regulation. For example, if a U.S. bank uses a data center in the Czech Republic to process and back-up certain operations relating to U.S. customers, the Regulation appears to give those U.S. customers rights under the Regulation because the Regulation states that it applies to the processing in the Czech Republic.

SIFMA recommends that the Regulation be clarified such that where a non-EU controller makes use of a processor in the EU, that usage will not in and of itself create rights for data subjects under the Regulation that would not have existed otherwise.

D. Transatlantic Transfers of Personal Data

a. Adequacy Decisions by the European Commission

SIFMA members are subject to stringent data protection and confidentiality obligations under U.S. laws applicable to the financial services sector. For many years, SIFMA has argued that these laws are at least as stringent as European laws, particularly those laws adopted pursuant to the Gramm-Leach-Bliley Act which apply to banks and broker-dealers (for example, Regulation S-P under the Securities Exchange Act of 1934). However, under the current European data protection directive, the European Commission has not found that the United States offers adequate protection of personal data. Because the U.S. is not deemed to provide adequate protection, SIFMA members must enter into data transfer agreements with each of their affiliates in Europe. The European affiliates must in many cases notify or seek authorization from the local data protection authority before the data may be transferred.

These current requirements are burdensome and inappropriate given the high level of data protection obligations that apply to SIFMA members by operation of U.S. law.

SIFMA applauds article 41(1) of the proposed Regulation, which would allow the European Commission to issue adequacy decisions for a certain “processing sector” in a third country. This would permit the European Commission to make an adequacy finding for entities in the financial services sector in the U.S.

To that end, SIFMA recommends that the U.S. government and the European Commission work together to determine whether the European Commission can, *even before adoption of the Regulation*, issue an adequacy decision relating to U.S. financial institutions that are subject to data protection obligations by virtue of U.S. financial services regulations. SIFMA members are already subject to stringent data protection rules in the U.S., and the current bureaucratic requirements imposed by European data protection laws for transatlantic transfers are disproportionate. They create bureaucratic complication without corresponding benefit for EU citizens.

b. Simplification of Binding Corporate Rules

Binding corporate rules (“BCRs”) are an excellent idea in theory, but in practice they have been difficult to implement because of the requirement of obtaining approvals from multiple data protection authorities (“DPAs”) in Europe. SIFMA welcomes proposed Article 43 of the proposed Recommendation that would make it possible to implement BCRs with the approval of a single DPA. SIFMA hopes that the apparent simplicity associated with single DPA approval of BCRs is not derailed by an overly complex “consistency mechanism” under Article 57 of the proposed Regulation.

E. Consent should not be revocable in all circumstances

The proposed Regulation reinforces the data subject’s rights with regard to consent. Article 7 states that consent is not valid where there is a “significant imbalance” between the position of the data subject and the controller, and that the data subject has the right to withdraw his or her consent at any time. Article 17 requires that when a data subject withdraws his or her consent, all processing must stop, and the data controller and any processor must erase the data.

For the financial services industry, these provisions raise several concerns. First, consent that is linked to a contract (for example a loan agreement, or an account agreement) should not be revocable except in accordance with the contract’s terms. For example, a European affiliate of a U.S. financial institution issues debit/credit cards to EU customers. The customer agreement provides that the customers’ personal data will be processed at a central site in the U.S. and that the data may be shared among companies within the financial institution’s group. The customer uses his rights under the Regulation to revoke his or her consent to this processing, but wants to maintain his cardholder agreement. This would put U.S. financial institutions in the impossible situation of putting into place custom-made data processing operations for each individual customer depending on that particular customer’s consent parameters. These problems are compounded where there are joint customers for some or all of the affected accounts and products.

Second, if consent is not valid where there is a “significant imbalance” between the data subject and the data controller, many of the contracts relied upon by the financial services industry could potentially be challenged as invalid. For example, as part of a loan agreement, an EU individual agrees that the bank may process personal data of the borrower collected from other sources, including from sources held by the bank’s U.S. affiliates, for the purpose of determining the borrower’s financial situation and ability to reimburse the loan. The EU individual claims that his or her consent to this provision is invalid because of the “significant imbalance” that exists between the borrower and the bank.

Naturally consent is not the only basis on which personal data may be processed. However, consent is an important legal concept that determines, among other things, whether a valid contract has been formed. SIFMA is concerned that Article 7 may interfere with established legal rules on consent in the context of contractual relations, and therefore recommends deleting the Regulation’s provisions on consent. At a minimum, Article 7 should, or else stipulate that the provisions relating to consent are without prejudice to rights

and obligations that may exist under applicable contact law, and that the provisions of Article 7 apply only to situations where consent is the only basis for processing.

The right to be forgotten and the right to Data Portability should not apply to the financial services industry. Created with the Internet industry in mind, the right to be forgotten and the right to data portability have broad-reaching ramifications for the financial services industry. The impact of these new rights for the financial services industry has not been sufficiently evaluated.

a. Right to be forgotten.

SIFMA members are concerned that the right to be forgotten will have serious consequences for the financial services industry, which have strict recordkeeping obligations in many jurisdictions and also rely on historic data to evaluate credit and insurance risks. Furthermore, financial institutions, especially broker-dealers and investment advisers, may be required to retain certain records for a period of years under U.S. recordkeeping requirements. For example, U.S. broker-dealers are required to retain communications with customers for at least 3 years under Exchange Act Rules 17a-3 and 17a-4, and litigation document requests may require longer hold periods. Such records could not be deleted even if a customer exercised the right to be forgotten.

Furthermore, the right to be forgotten would potentially interfere with a bank's or an insurance company's legitimate interest in maintaining data for the purpose of detecting fraud and evaluating credit and insurance risks. For example, an insurance company keeps a record of a French customer's claims and policy history for the purpose of detecting inconsistent statements and false claims. The customer exercises his right to be forgotten, at which point the insurance company must either erase the data about the customer (art. 17(3)), or archive it for purposes of proof only (art. 17(5)). The customer then makes a new application for insurance containing information contradicting information previously given to the insurance company.

As a result, SIFMA recommends that the financial services industry be excluded from the right to be forgotten, or else circumscribe the right to be forgotten to the right currently granted to data subjects under article 12(b) of the 1995 Data Protection Directive.

b. Data portability

The right to data portability also raises significant concerns for the financial services industry. To our knowledge, the European Commission has conducted no impact assessment regarding the right of portability as applied to the financial service industry. Neither the need for the measure nor its cost for the financial services industry has been evaluated. We are highly concerned about the potential costs of such a measure and how the measure would interact with other regulatory obligations that weigh on the financial services industry.

For example, Mr. Smith wishes to move his account from Bank A to Bank B. Invoking the right of data portability, Mr. Smith requests Bank A to deliver the following information to him in an electronic format permitting easy portability to Bank B:

- Mr. Smith's full account history for the last fifteen years;
- All Mr. Smith's direct debit instructions and standing wire transfer instructions;
- All loan and investment simulations prepared while Mr. Smith was a client.

Bank A already has regulatory obligations under U.S. banking and securities laws in connection with data that Bank A must retain and deliver to Mr. Smith. The information requested by Mr. Smith goes beyond these other regulatory obligations, and would create a significant cost for Bank A that Bank A will not be able to recover from Mr. Smith.

As with the right to be forgotten, SIFMA recommends that the financial services sector be excluded from the obligation of data portability. Such an obligation would create enormous costs for the sector, and would potentially conflict with other regulatory obligations to which the bank is subject.

F. Data breach notification should reflect current best practices

Preventing and mitigating data security breaches is of critical importance to SIFMA members and it is a responsibility we take very seriously. Based on many years of industry experience in this area, SIFMA believes the proposed breach notification requirements should be adjusted to reflect current best practices and set realistic expectations. In particular, the obligation to notify the DPA "without undue delay and, where feasible, not later than 24 hours after having become aware of it" provides for no minimum threshold for breach notification and so is disproportionate; it should be based on materiality of the breach and the risk of harm to affected individuals. The provision as written does not improve protection for individuals; it merely creates an additional, unnecessary and costly burden for both the DPAs and data controllers. It should also be noted that the requirement is at odds with the current advice given to data controllers by the UK Information Commissioner's Office (ICO), and to electronic communications services providers who already have a compulsory breach notification obligation. In their initial response to the GDPR, the ICO has expressed concern that this requirement goes too far and should be "restricted to serious breaches only."

SIFMA recommends that the data breach notification be based on a materiality standard which is proportionate to the risk of harm to individuals.

G. Sanctions should be reasonable and appropriate

Appropriate sanctions against material breaches can be part of an effective regulatory framework. However, the proposed maximum fine of 2% of annual worldwide turnover is

disproportionately high in relation to the risk of harm to an individual that might arise from a breach of the regulation. For example, one global bank has estimated their fines could reach \$1.6 billion. In addition, for global companies engaged in many different businesses, some of which may not even process personal data, it is not fair or appropriate to effectively penalize business operations that are not associated with or implicated by a particular breach. SIFMA recommends a revised sanction which is more proportionate to the potential harm to individuals.

* * *

Thank you for taking the time to consider our concerns and recommendations. We would be happy to provide more detailed information should you need it. If you have any questions or comments, please contact Melissa MacGregor, Managing Director and Associate General Counsel of SIFMA, at 202-962-7385 or mmacgregor@sifma.org.

Sincerely,

A handwritten signature in blue ink, appearing to read "Ken Bentsen", with a stylized flourish at the end.

Kenneth E. Bentsen, Jr.
EVP, Public Policy and Advocacy

cc: Ambassador William Kennard
Ambassador Philip Verveer
The Honorable David Cohen
Mark Sobel, Deputy Assistant Secretary, U.S. Department of the Treasury
William Murden, Director, Office of International Banking and Securities Markets,
U.S. Department of the Treasury
Susan Baker, Susan Baker, U.S. Department of the Treasury, Financial Attaché for
Europe
Winston Maxwell, Partner, Hogan Lovells