

**SUBMISSION BY SIFMA IN RESPONSE TO THE CONSULTATION
ON THE EUROPEAN COMMISSION'S COMPREHENSIVE APPROACH
ON PERSONAL DATA PROTECTION
IN THE EUROPEAN UNION**

1. Introduction

The Securities Industry and Financial Markets Association (SIFMA) welcomes the opportunity to comment on the European Commission's Communication on a Comprehensive Approach on Personal Data Protection in the European Union, and applauds the Commission for undertaking this important review and initiative.

2. Presentation of SIFMA

2.1 What is SIFMA?

The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of more than six hundred securities firms, banks, and asset managers throughout the world. SIFMA's offices are located in New York and Washington, D.C. SIFMA is the U.S. regional member of the Global Financial Markets Association (GFMA).

2.2 SIFMA's mission

SIFMA's mission is to develop policies and practices in order to strengthen financial markets. By building trust and confidence in the financial industry SIFMA intends to encourage capital availability, job creation, and economic growth. Encouraging effective data protection goes to the heart of SIFMA's mission of building trust and confidence in the financial services industry. Without effective protection of the personal data of their customers, financial institutions would lack the public trust that is so critical for their operation.

3. Overview

SIFMA's members include some of the largest financial institutions in the world. Those institutions collect and process massive amounts of personal data every day, and SIFMA is proud to report that there have been relatively few incidents of loss or unauthorized use or access to personal data among SIFMA members. The data protection track record

of the financial services industry is quite good compared to other industries. This is partly due to the fact that the financial services industry is already subject to stringent laws and regulation on the protection of personal data. Consequently, SIFMA members are accustomed to, and fully support, the data protection principles contained in Directive 95/46/EC. In addition to the data protection rules set forth in Directive 95/46/EC, SIFMA members are subject to rigorous bank secrecy laws in Europe that strictly limit the ability of financial institutions in Europe to transfer personal data to other entities without the express consent of the customer.

While SIFMA embraces the principles of Directive 95/46/EC, SIFMA finds that the current European regime could be improved:

1. Existing rules are not sufficiently harmonized in Europe, making it difficult or sometimes impossible for its members to adopt pan-European policies.
2. Some Member States require too many prior notifications, creating bureaucratic bottlenecks and costs, without discernable benefit to the protection of individuals.
3. Current rules on transatlantic transfers of personal data do not take into account the specificities of the financial services industry, which is subject to stringent privacy rules in the U.S. The Commission's "adequacy" determinations for transfers to the U.S. should take account of the special laws that apply to enterprises in the financial services arena.
4. Binding corporate rules (BCRs) are an excellent means to facilitate the transfer of data among large corporate groups, but their adoption still requires too many separate national approvals.
5. The use of data protection officers (DPOs) in large corporations should be encouraged.

4. Better Harmonisation of Existing Rules

Many of SIFMA's members operate throughout Europe, and regret that the high level principles of Directive 95/46/EC translate in practice into distinct national regimes with different substantive and formal requirements applying in each Member State. The current lack of harmonisation makes the adoption of pan-European business practices and policies by SIFMA members difficult. As pointed out by the Commission, one of the objectives of Directive 95/46/EC is to contribute to the creation of the internal market by creating uniform rules applicable to the processing of personal data throughout the EU:

"The Directive enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection, on the one hand, and the achievement of the internal market -- the free flow of personal data in this case -- on the other. Fifteen years later, this twofold objective is still valid and the principles enshrined in the Directive remain sound."¹

The internal market objective has only been partially achieved. Local data protection legislation, and the interpretation by local data protection authorities (DPAs), too often create diverging requirements for data processing practices. The opinions of the Article 29 Working Party are helpful, but more harmonisation is needed.

SIFMA believes that it should be possible for its members to adopt policies and procedures on a pan-European basis, including for data protection. Currently, policies have to be modified to comply with the particularities of each national legislation and DPA. Some differences arise because of local employment law. But others are purely due to diverging national data protection laws and DPA practices.

To improve harmonisation and the creation of the internal market, SIFMA would welcome the creation of a European data protection body subsuming the existing Art 29 WP but also with the active involvement and supervision of the European Commission. The recently-created BEREC² in the telecommunications sector could serve as a possible model. The Commission, or such future body, should have power to adopt recommendations for certain kinds of pan-European data processing operations, but only after widespread industry consultation. The revised directive should then include a requirement that Member States take "utmost account" of the recommendations issued by the Commission or by such new European body, and that any variance from the recommendation be duly justified by the relevant DPA based on special local circumstances.

One area where harmonisation is necessary is in relation to the requirements for consent, and in particular the form of consent necessary when using different media (mobile phone versus in-person meeting, for example). The existence of different national requirements for consent can represent a serious barrier to the development of pan-

¹ Communication from the Commission to the European Parliament, the Council, the Economic and social committee and the Committee of the Regions: "A comprehensive approach on personal data protection in the European Union", 4 Nov 2010, p. 2.

² Body of European Regulators in Electronic Communications, created by Regulation (EC) No. 1211/2009 of the European Parliament and of the Council of 25 November 2009.

European services in the financial sector, thereby harming achievement of the internal market. Overly prescriptive rules should be avoided, particularly where those rules are likely to vary between Member States, or quickly be outdated by technological developments.

5. Simplification Or Elimination Of Current National Notification Requirements

SIFMA favors a reduction in the number of *ex ante* notification and authorization requirements. For SIFMA members doing business in Europe, national notification requirements increase the cost and complexity of doing business in Europe without increasing the level of protection afforded to European consumers.

In SIFMA's view, there is no direct correlation between *ex ante* filings and substantive protection of consumer privacy. In the banking industry, financial institutions have for many years been subject to strict bank privacy and data security laws, and those laws have been effective in preventing unauthorized disclosure of personal information. But the effectiveness of bank privacy and data security laws is not linked to the existence of any prior notification regime. Bank privacy and data security laws are generally regarded as effective, largely because their violation will create grave consequences for the relevant financial institution. *Ex post* enforcement is a better guarantee to effective application of rules than *ex ante* notifications.

SIFMA believes that effective data protection requires enterprises to adopt relevant technical and organisational measures to foster data protection as part of the enterprise's daily operational requirements. Yet such measures should focus on the substance of data protection compliance.

In SIFMA's view, *ex ante* filing obligations do not contribute to a culture of compliance, and instead create costs or even barriers to good data protection practices. The adoption of BCRs exemplifies the current problems associated with national filings and authorisations. While considerable progress has been made in simplifying the adoption of BCRs, the need to obtain separate national authorisations in a number of Member States creates a needless barrier to widespread adoption of BCRs. These separate national authorisations should be removed. Indeed as a general matter, prior notification or authorization requirements should be the exception rather than the rule.

It may be useful for the Commission to conduct a study of current *ex ante* notification and authorization requirements in Member States, and effect a cost-benefit analysis of those regimes compared to a situation that relies solely on *ex post* enforcement. SIFMA's view

is that *ex ante* notifications give rise to significant costs but do not create any added value in terms of effective compliance with data protection principles. But this conclusion should be confirmed through an empirical study.

6. Facilitating Secure Transatlantic Transfers Between Entities Subject to Effective Privacy Legislation

The current European regime considers that recipients of personal data in the United States do not provide adequate protection, regardless of the legal regime under which those recipients operate. This is because the U.S. does not have a global data protection law similar to the Directive 95/46/EC. U.S. enterprises can overcome the presumption of inadequate protection by subscribing to the Safe Harbor regime, or by signing standard contractual clauses, or by adopting BCRs. However, this approach ignores the fact that U.S. law provides adequate protection for personal data in certain industries, especially those in the financial services sector.

SIFMA members already are subject to wide-reaching obligations to safeguard the security, confidentiality and integrity of customers' information under the Gramm-Leach-Bliley Act (GLBA) and Fair Credit Reporting Act (FCRA), among other sector-specific laws.

FCRA promotes the accuracy, fairness, and privacy of personal data assembled by "consumer reporting agencies" (CRAs), including data provided by SIFMA members. The FCRA establishes a framework of fair information practices that include rights of data quality, data security, identity theft prevention, use limitations, requirements for data destruction, notice, user consent, and accountability. FCRA applies to a number of different categories of persons and entities (depending on the particular provision of FCPA) -- not only to CRAs. For instance, under the FCRA, a person (whether an individual, a financial institution, or some other entity) may obtain a "consumer report" -- such as a consumer credit report -- from a CRA only in limited, specified circumstances where a "permissible purpose" for obtaining such a report exists and the person certifies that the person has such a permissible purpose. Any person that furnishes information about a consumer to a CRA also has numerous responsibilities, including participating in investigations regarding the accuracy of information the furnisher has reported about a consumer when the consumer has disputed such information. Any person that holds sensitive information about consumers must also ensure the proper disposal of such information when it is no longer needed. The FCRA Red Flags Rules also requires financial institutions and certain other creditors to maintain identity theft prevention

programs. FCRA also places certain restrictions on the ability of any person to share and use certain types of consumer information among affiliates.

The GLBA provides data privacy rules applicable to “financial institutions,” a term defined broadly to cover entities significantly engaged in financial activities such as banking, insurance, securities activities, and investment activities. The GLBA imposes data privacy obligations such as the obligation to securely store personal financial information, and provide data subjects with the right to opt-out of some sharing of personal financial information.

The GLBA and the regulations issued under the GLBA help to protect valuable customer information and to prevent data breaches. Through exceptionally broad definitions, GLBA protections apply to virtually all personal information about individual consumers held by more than 40,000 financial institutions in the United States - including less traditional "financial institutions" such as check-cashers, information aggregators, and financial software providers. Consumers now must be provided with:

- Notice of the institution's practices regarding information collection, and disclosure, which must be clear, conspicuous, and updated each year;
- Opt-out choice regarding the institution's sharing of information with non-affiliated third parties (unless any exception applies), and in certain instances, with affiliates;
- Security in the form of policies, procedures, systems, and controls to ensure that personal information remains confidential;
- Protection against inappropriate re-disclosure or re-use of personal information that is shared with third parties; and,
- Enforcement of privacy protections via the full panoply of enforcement powers of financial institutions' regulatory agencies (federal bank regulators, the Securities and Exchange Commission, state insurance authorities, and the Federal Trade Commission). Federal bank regulatory agencies regularly examine financial institutions under their supervision for compliance with GLBA and FCRA (as well as with all other laws to which financial institutions are subject).

Moreover, the GLBA and its implementing regulations require financial institutions not only to limit the disclosure of customer information, but also to protect that information from unauthorized accesses or uses. The GLBA regulations also provide guidelines

counselling financial institutions on appropriate actions in response to a breach of security of sensitive data, including notification of consumers and/or law enforcement authorities.

The GLBA also provides that it does not pre-empt state laws that are more protective of consumers. A number of U.S. states, including California, have enacted such laws, which tend to resemble GLBA but add additional protections, such as requiring a consumer's opt-in consent for certain types of information sharing.

Finally, U.S. regulations require SIFMA members to carefully select, contractually bind, and conduct ongoing monitoring of, third party service providers that receive personal data.

SIFMA urges the Commission to adopt "adequacy" rulings that recognize the specificities of different industries in the U.S., and the different laws that apply to those industries. Where the recipient of personal data is a U.S. enterprise subject to the GLBA, for example, the legal protections that exist in the U.S. are every bit as great as if the recipient were located in a European Member State. The Commission should therefore create a safe harbour permitting transatlantic transfers when the recipient is subject to specific industry-focused legislation that provides an adequate level of protection compared to EU standards. The current European regime improperly assumes that a transfer of personal data to a financial institution in the U.S. is the same as a transfer to a U.S. mail order house, when in fact the U.S. privacy laws applicable to those two industries are completely different.

7. Creation of a Single, Harmonised, Data Breach Notification Obligation

SIFMA members recognize that there may be data breach circumstances that warrant notification to affected individuals and/or regulators. However, it has not been shown that mandatory notification pursuant to prescriptive rules is necessary or appropriate. Should the Commission pursue the development of mandated notification, then we urge that it do so through careful and thorough deliberations on the criteria for triggering such notification and the practical impact and value for providing such notifications. In addition, the Commission should ensure that the requirements are adequately harmonized throughout Europe. Failure to do so could result in unintended negative consequences to the recipients and providers of such notice.

8. The Obligation to Appoint Data Protection Officers (DPOs)

SIFMA agrees with the proposal to introduce data protection officers across the Community. Corporations exceeding a certain size should be encouraged to have duly qualified DPOs because the appointment of DPOs contributes to the creation of a culture of data protection compliance within the corporation. Consistent with the internal market, it should be possible for corporations to name a single European DPO who would interface with all national DPAs and with European data protection authorities (Art 29 WP and/or any future European data protection body). The European DPO would be able to appoint national DPOs, but this would not be an obligation. Consistent with the way large corporations operate, it should be possible for the DPO function to be centralized at a group level, just as the IT or legal function may be centralized at one European site, and then support the group's business units throughout Europe.

* * *

If you have any questions, please call Melissa MacGregor, Managing Director and Associate General Counsel, SIFMA at 202-962-7385.

cc: Winston Maxwell, Hogan Lovells LLP
Christopher Wolf, Hogan Lovells LLP