INVESTMENT COMPANY INSTITUTE®
ICI Global
WASHINGTON, DC • BRUSSELS • LONDON • WWW.ICI.ORG

Comment Letter on EU Data Protection Directive, May 1999

May 14, 1999

Mr. Eric Fredell
Task Force on Electronic Commerce
International Trade Administration
Department of Commerce
14th and Constitution Avenue, NW
Washington, DC 20230

Re: Comments on International Safe Harbor Privacy Principles

Dear Eric:

The Investment Company Institute[1] appreciates the opportunity to provide comments on the international safe harbor privacy principles and the draft "frequently asked questions" made public by the Department of Commerce recently. The safe harbor has the potential to afford significant benefits to many US companies that transfer personal data from the EU to the US and face the possibility of a data blockage under the EU's Data Protection Directive. We appreciate the efforts of the Department of Commerce to develop clear and predictable guidance for US firms.

We believe that the value of the safe harbor for the US investment company industry largely will depend on three things: first, whether specific regulations with respect to privacy adopted by our traditional regulators are given appropriate deference; second, whether the transition period for compliance with the safe harbor is long enough to allow regulators to act and companies to respond; and third, whether the safe harbor principles of choice and onward transfer clearly and unambiguously permit a mutual fund organization to use and transfer data for purposes that are not incompatible with the relationship between the fund and its shareholders. This letter focuses on each of these, then provides some specific comments on the safe harbor principles and FAQs.

Specific privacy regulations adopted by securities regulators must be given appropriate deference.

As you know, investment companies and investment advisers are principally regulated by the Securities and Exchange Commission (SEC). Broker-dealers that sell fund shares are principally regulated by the National Association of Securities Dealers (NASD). These regulators understand the structure and organization of mutual fund organizations and, as a result, are in the best position to craft rules that would appropriately regulate the protection of individual privacy in the industry.[2] Should one of these regulators promulgate a rule specifically relating to privacy, firms that are subject to and in compliance with it should qualify for the safe harbor, regardless of whether the rule precisely mirrors the safe harbor principles.

For example, the NASD has proposed a rule specifically dealing with the confidentiality of broker-dealer customer data used for marketing purposes.[3] In comments on the proposed rule, the Institute argued that the NASD should require disclosure, rather than an opt out procedure, for certain types of information-sharing within an investment company complex. This would take into account the unique structure of the industry and recognize the fact that investors who purchase shares of a mutual fund are entering into a relationship with the entire fund family. Should the NASD agree with the Institute on this issue, we believe that there should be a presumption that firms complying with the rule adequately and effectively protect their customer data.

Deference to securities regulators is all the more appropriate given their important enforcement role. The NASD and SEC will actively monitor compliance with any privacy rules they impose and will take enforcement action or make revisions to the rules as appropriate to deal with any problems that arise. The benefits to consumers of active NASD and SEC involvement in enforcing privacy rules for the benefit of customers should more than outweigh any possible dimunition of data protection through deference to their rules. Moreover, deference is necessary in order to avoid having the industry bear the wholly unnecessary expense of complying with

duplicative, substantially similar, privacy regulations.

We strongly believe that the safe harbor principles should clearly state that if an organization is subject to a US statutory or regulatory provision that specifically addresses privacy, it would qualify for the safe harbor even if that statutory or regulatory provision does not precisely match up in certain respects with the specific elements contained in the principles. [4] This could be accomplished by either deleting the word "effectively" in the first sentence of the fourth paragraph of the preamble[5] or replacing it with a word that connotes deference, such as "specifically."

The transition period must be long enough to allow US firms to come into compliance with the safe harbor.

The transition period must be long enough to accommodate regulatory and systems changes. The NASD rule proposal underscores the need for a long transition period. It is imperative that the transition period be long enough to allow the NASD to complete its rulemaking process and for companies to respond. We believe that, at a minimum, the transition period should be eighteen months long.[6] That should allow sufficient time for the proposed NASD rule to be acted upon and for companies subject to that rule to come into compliance with it.

Eighteen months would also allow companies to make the systems changes that inevitably will be required to comply with the terms of the safe harbor or any NASD rule. Many investment companies and investment advisers have imposed Y2K systems upgrade moratoriums that will make it impossible to begin to make those changes until the second quarter of 2000. Thus, it seems unlikely that companies would be able to complete necessary systems changes with respect to new privacy regulations before the end of 2000 at the earliest.

In the event that neither the NASD nor the SEC acts with respect to privacy, we understand that investment companies and investment advisers individually would have to self-certify compliance with the safe harbor principles. To do so, companies will need an appropriate period of time to come into compliance with the principles.

The principles of notice, choice and onward transfer must allow for uses of information that are not incompatible with the relationship between an investment company and its shareholders.

The safe harbor should allow for uses of information that are not incompatible with the use for which the information was collected and that are consistent with the expectations of investment company shareholders based upon proper notice. In our comments on the earlier safe harbor draft, the Institute argued that, for example, a broker that collects information in order to enter into a brokerage relationship with a customer should, by providing appropriate notice, be able to use that information to offer the customer the full range of products and services that might be suitable for that customer.[7] In our view, using the information in that manner would be related to and compatible with the brokerage relationship – the use for which the information was originally disclosed.

We believe that the language in the current draft, and in particular, the use of the word "compatible", represents an improvement in this area. We believe it is critical that the principles of notice, choice and onward transfer in the safe harbor be interpreted to permit companies to efficiently provide customers with the service and the products that they have come to expect. For example, many integrated financial services firms offer account statements that cover banking, insurance, securities, and asset management balances in a unified way. Consumers consider this to be a significant positive development. In order to create these statements, and other similar value-added customer service benefits, personal information such as account balances must flow among the affiliated companies offering the various financial products. The restrictions on choice and onward transfer should not hinder firms from using information in these and other ways that are compatible with the use for which it was collected. The text of the safe harbor must make this clear.

Other specific comments on the safe harbor principles and FAQs.

Relative Weight of FAQs and Principles. In his cover letter, Ambassador Aaron specifically asks for comment on the weight to give the FAQs relative to the principles. The Institute believes that the FAQs should be given significant weight. The relationship between the FAQs and the principles should be similar to that between statutory provisions and regulations that expand upon them. In other words, the FAQs should have the same force of law that the principles enjoy.

Access. The Institute strongly supports inclusion of the bracketed language in the principle and the FAQ on access, and the idea that consumers' rights of access should be tempered by reasonableness.[8] It is not enough, in our opinion, to explain this point in a FAQ.

It should be clear from reading the principle and the FAQs on access that companies may consider "the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the information." To reinforce this point, we suggest adding the words "but not absolute" to the end of the first sentence of the first FAQ on access, so that the sentence would read: "Under the safe harbor principles, the right of access is fundamental to privacy protection, but not absolute."

The Institute also supports the notion, expressed in FAQs 1 and 2 to the access principle, that companies may deny access to the extent it would reveal confidential commercial information. Companies should not have to release information that is proprietary. The use of the term "confidential commercial information" is readily understood by US companies and their counsel, given its use in the Federal Rules of Civil Procedure. The use of the alternative term "trade secrets" and its definition in the Economic Espionage Secrets Act, as suggested by the EU, is too narrow for these purposes. Moreover, that term would be inappropriate given that it is intended for use in a criminal statute.

Self-Certification. The Institute strongly supports the concept of self-certification. However, the detailed reporting obligations outlined in the FAQ on self-certification are burdensome and unnecessary. For example, if a company self-certifies that it qualifies for the safe harbor, it necessarily will have a privacy policy that is available to the public. There is no need for that policy to be restated in a self-certification form, unless the Department of Commerce intends to subjectively review it—something that the Department and the Europeans have repeatedly said is not their intention. The Department's role should be limited to maintaining a list of companies, and contact persons at those companies, that have self-certified their compliance with the safe harbor terms.

* * *

We appreciate the opportunity to express these views.

Sincerely,

Mary S. Podesta
Senior Counsel

ENDNOTES

[1] The Investment Company Institute is the national association of the American investment company industry. Its membership includes 7,546 open-end investment companies ("mutual funds"), 457 closed-end investment companies, and 8 sponsors of unit investment trusts. Its mutual fund members have assets of about $5.730 trillion, accounting for approximately 95% of total industry assets, and have over 73 million individual shareholders.

[2] For example, unlike most other types of companies, most investment companies are externally managed. They do not have their own employees and their operations are conducted by various organizations. Information flows among these organizations—the fund, investment adviser, principal underwriter, custodian, administrator, and transfer agent, among others—during the normal course of investment company operations. Some of these flows may implicate privacy concerns that should be addressed; others clearly do not.

[3] Proposed Rule 3121, NASDR Notice to Members 97-12 (March 1997). As you know, the Institute supports rulemaking by the NASD as the appropriate means to deal with privacy issues involving investment companies and we are hopeful that the NASD will move forward with its rulemaking, taking into account the comments the proposal received. The NASD proposed rule sets forth requirements for information sharing with affiliates and non-affiliates and includes elements of notice and choice.

[4] It is important to note that we are not suggesting that investment companies and investment advisers qualify for the safe harbor solely by virtue of being heavily regulated by the SEC and NASD. Instead, we believe that to the extent the SEC or NASD specifically address privacy, there should be a presumption that the regulations that they promulgate are adequate, effective and appropriate for the US securities industry.

[5] That sentence currently reads: "Where an organization is subject to US statutory, regulatory, administrative or other body of law (or body of rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or a Municipal Securities Rule-making Board) that also effectively protects personal data privacy, it qualifies for the safe harbor to the extent that its activities are governed by such laws or rules."

[6] We note, in this regard, that European Union member states had three years between October 25, 1995 and October 25, 1998 to implement legislation giving the Directive local effect and that, in certain instances, companies in the EU have additional time before they must comply with all of its terms.

[7] Letter to Eric Fredell dated November 19, 1998.

[8] The current draft of the access principle reads: "6. ACCESS: Individuals must have [reasonable] access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate. [Reasonableness of access depends on the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the information.]"
