



Securities Industry Association

120 Broadway, New York, NY 10271-0080, (212) 608-1500, Fax (212) 608-1604

1401 Eye Street, NW, Washington, DC 20005-2225, (202) 296-9410, Fax (202) 296-9775

info@sia.com, <http://www.sia.com>

November 19, 1998

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

Re: Comments on Draft International Safe Harbor Privacy Principles

Dear Mr. Fredell:

Thank you for Ambassador Aaron's letter dated November 4, 1998 explaining and requesting comment on the Department of Commerce's Safe Harbor Principles ("Principles"). The securities industry's position on the privacy issue is well known: The Securities Industry Association¹ ("SIA") opposes the imposition of new privacy standards on the securities industry. The existing comprehensive regulatory structure of the securities industry and the self-interest of industry members in protecting their clients' privacy have protected -- and will continue to protect -- the privacy of the industry's customers. New privacy standards would raise the costs of doing business with no corresponding benefits to the customer. ²

In this regard, SIA appreciates and supports the Department's continued efforts to address the business concerns raised by the European Union's Directive on Data Protection in a manner which appropriately reconciles those concerns with reasonable Privacy considerations. The Safe Harbor Principles represent a significant step forward in clarifying the obligations under the Directive and in keeping those obligations within reasonable bounds. Nonetheless, SIA has a number of suggestions that would make the Principles even more effective.

First, SIA supports the comments submitted by the Coalition of Service Industries ("CSI") regarding the Principles. SIA is a member of CSI and strongly recommends that the Department incorporate CSI's proposed edits both in the Principles themselves and in the Frequently Asked Questions ("FAQ") section of the Principles document.

In particular, SIA supports CSI's proposed elaboration of the distinction between factual and proprietary information. In the securities industry, there are critical situations where it could be damaging both to securities firms and to financial markets generally for a firm to disclose its proprietary information about an individual. A securities firm typically would welcome disclosure

of a customer's factual information to ensure that the firm's records are accurate. But disclosing to a customer the criteria and results of a firm's proprietary internal decision-making processes could be quite harmful. Indeed, SIA thinks that such a requirement could chill the prudent evaluations of creditworthiness and the suitability of investments that members of the securities industry must undertake.³ In short, individuals may need access to their personal information in order to ensure that an organization's data is accurate. They should not, however, be permitted to second-guess how an organization makes business decisions using that information. Thus, SIA supports CSI's refinement of the "reasonable access" requirement with respect to proprietary information.

SIA also supports CSI's suggestions regarding the enforcement provisions of the Principles. Those provisions currently leave wide room for interpretation. CSI's proposed edits would improve the efficacy of the principles by setting forth in more detail what businesses must do to be in compliance. The securities industry, for example, already has extensive complaint and arbitration procedures in place, under the auspices of both the Securities and Exchange Commission ("SEC") and self-regulatory organizations such as the National Association of Securities Dealers-Regulation ("NASD-R"). The Principles should state clearly that such a respected and proven arbitration system will be a sufficient enforcement regime under the safe harbor. CSI's proposed additions substantially further that goal by noting that "complaint[s] to a government agency with enforcement powers" and "dispute resolution procedures established by self-regulatory bodies" should allow an organization to satisfy the Principles' enforcement provisions.

In addition, SIA supports CSI's recommendation to clarify that an opt-out choice is not required when an organization uses or transfers a customer's information in order to provide the customer with the service that the customer originally sought from the organization. Indeed, SIA urges the Department to clarify further that an opt-out choice is not required for transfers among affiliated organizations that provide the same general line of services as the service initially requested by the customer. When affiliated organizations transfer information among themselves, it is often difficult to draw sensible lines between (1) those uses that are related to the uses for which a customer initially provided the information, and (2) those uses that are unrelated to the initial uses. Indeed, financial services companies often employ multiple affiliated entities to provide interrelated services that cannot be easily separated from the initial service sought by the customer.⁴ The Department therefore would greatly simplify the task of defining these companies' obligations if it broadened the scope of the opt-out exception to permit organizations to transfer information among affiliates in order to provide services that are in the same general line of business as the service initially sought by the customer.

Furthermore, SIA supports CSI's suggestions regarding (1) the inapplicability of the Principles to public information, and (2) when notice must first be provided to consumers. Both of these recommendations are practical refinements of the Principles.

Second, SIA supports the comments submitted by the American Council of Life Insurance ("ACLI"). SIA particularly highlights ACLI's concern that organizations not be required under the data integrity principle to keep updating information even if the organizations have no business purpose to do so. A firm, for example, will typically retain account information for some period of time after the account is closed, for a variety of legal, insurance, and commercial reasons. But unless the account is reopened, the firm has no need to update information about the

customer's address, employment, or investment objectives.

Third, SIA requests that the Department clarify precisely how organizations can qualify for the safe harbor. More specifically, the Department should clarify when the existence of an overarching regulatory framework will be sufficient to place organizations within the safe harbor. The preamble to the Principles states that "an organization qualifies for the safe harbor if it is subject to a statutory, regulatory, administrative, or other body of law that effectively protects personal information privacy." SIA wholeheartedly endorses this provision of the Principles, but the language should be strengthened and expanded (in either the Principles themselves or in the FAQ section) to make clear that comprehensively-regulated industries such as the securities industry qualify for the safe harbor so long as privacy-related concerns and complaints can be addressed within the regulatory framework. In that regard, we also would like to associate ourselves with the comments regarding the safe harbor submitted by the Investment Company Institute.

As SIA explained in its paper submitted to the privacy summit earlier this year, the securities industry already protects the privacy interests of investors. Between the regulations of the SEC, the requirements of self-regulatory organizations such as NASD-R, and the agency duties imposed on securities brokers by common law, securities firms are under intense business and regulatory pressure to serve customers honestly and with the highest ethical standards. Although this regulatory framework does not dictate specific rules concerning privacy, abuses of private information would be captured by many of the existing principles, statutes, and rules. Moreover, the securities industry clearly has a structure in place to respond to privacy issues as they develop. Indeed, SIA understands that NASD-R is currently considering new rules specifically designed to address privacy concerns.

In light of this regulatory framework, the Principles should be amended to clarify that securities firms (and other organizations operating under similar regulatory regimes) are protected under the safe harbor. When an organization is operating under intense regulatory scrutiny, the potential risk to individual privacy is substantially reduced. Indeed, regulated organizations such as securities firms are under constant supervision and subject to prompt, efficient enforcement mechanisms. As noted above, the preamble to the Principles already recognizes this basic fact by stating that regulated organizations are protected by the safe harbor. If any business sector should qualify under this provision, it is the securities industry. The Department, therefore, should expand the Principles to clarify that the regulatory framework governing the securities industry is precisely the type of regulatory structure that would bring an organization within the safe harbor.

Again, SIA commends the Department on its good work in this area, and we hope to continue working with you in this process going forward. If you have any questions, or wish to discuss these issues further, please do not hesitate to contact me, or Kristin Roesser on my staff.⁵

Sincerely,

Marc E. Lackritz
President

Footnotes:

¹ The Securities Industry Association brings together the shared interests of nearly 800 securities firms to accomplish common goals. SIA members -- including investment banks, broker-dealers, and mutual fund companies -- are active in all markets and in all phases of corporate and public finance. In the U.S., SIA members collectively account for approximately 90 percent, or \$100 billion, of securities firms' revenues and employ about 350,000 individuals. They manage the accounts of more than 50-million investors directly and tens of millions of investors indirectly through corporate, thrift, and pension plans.

² See Securities Industry Association, "Privacy Protection in the United States Securities Industry," June 23, 1998.

³ To the extent that securities firms are required by law to gather and analyze information about individuals, the Principles' exception for "regulatory compliance and supervision, and law enforcement requirements" would presumably override any access requirement under the Principles. For example, if a firm were expressly forbidden from informing a customer that the firm had filed a report of suspected money laundering regarding the customer, the Principles would presumably not obligate the firm to inform the customer of the report. If such a firm would not be protected against the Principles' access requirements, the Department should modify the Principles to so provide.

⁴ For example, we believe that if a customer requests financial planning services from an organization, that organization should be allowed to share information with its affiliates to provide related banking, insurance, or securities services to the customer without being constrained by the precise scope of the customer's initial request. We believe that the safe harbor should be flexible enough to allow for this type of situation, where requiring an additional opt-out both could be a nuisance to the customer and cause the customer financial harm by preventing a financial services organization from acting quickly in the customer's financial interest.

⁵ In suggesting that the securities industry should so qualify, we do not mean to suggest that others should not so qualify.