QUESTIONS AND ANSWERS:
PRIVACY PROTECTIONS OF THE GRAMM-LEACH-BLILEY FINANCIAL SERVICES MODERNIZATION ACT

Q. What is the purpose of the *Financial Services Modernization Act*? Why is it important?

A. Enacted in 1999, this law modernizes the financial services industry by replacing outdated, Depression-era laws separating insurers, banks, and securities firms. For the first time since the 1930s, banks, insurance companies, and brokerages may affiliate with one another and diversify the services they can offer to their customers. These changes promote greater competition among providers of financial services. Diversified financial institutions can now offer customers more choices and better service with greater efficiency at lower cost.

Q. Which financial services institutions does the new law impact?

A. The new law affects the entire financial services industry. Every financial company—including insurance companies, banks, and securities firms—must comply with the consumer privacy provisions contained in the law.

Q. Does the new law benefit consumers?

A. The new law promotes innovation and competition within the financial services industry. As a result, the financial services marketplace will become more efficient and consumer friendly by offering consumers more choices. This ultimately will save consumers money while allowing firms to better meet clients' needs. Competition among financial services firms will promote the development of new, innovative products. The Treasury Department estimates consumers will save $18 billion a year as a result of the new law, and those savings could show up in benefits such as reduced fees on credit cards and banking services.

Q. How does the act protect the confidentiality and security of customer information?

A. The act provides the most comprehensive consumer privacy protections ever enacted at the federal level, including:

- Financial services companies are required to adopt and disclose privacy policies;
- Consumers are given the choice to "opt out" of having their information shared with third parties for marketing purposes; and,
- The practice of obtaining or disclosing someone's financial information under false pretenses—known as pretext calling—is outlawed.

Q. Are additional state regulations necessary?

A. No, not now. Clearly, many legislators and consumer advocates are concerned about protecting customer privacy in an era when personal information increasingly is being collected and shared. However, consumer privacy is well protected in the new federal act and many other pre-existing laws.

After the new law takes effect on November 12, there will be an 18-month study on how information is used across affiliates in financial institutions. Until the study is finished, state legislators should allow consumers to make their own decisions in the free market before concluding that additional laws are necessary.

Q. Does the act provide consumers with choices about how their information is used?

A. Yes, the law empowers consumers with the choice to "opt out." When consumers choose to opt out, they forbid financial institutions from sharing personal financial information with third parties. This is a competitive model for privacy protection, requiring—for the first time in federal law—disclosure of privacy and confidentiality policies. With this information consumers can then decide whether to do business with a particular firm.

Q. How does the sharing of financial information benefit consumers?

A. Sharing financial information improves service and lowers costs for consumers. Consumers benefit when a financial services company has a comprehensive picture of their personal needs and can offer products and services to meet their specific circumstances. Consumers also benefit from faster decisions and more efficient services—on loans and other credit, on insurance and other financial products—that result when companies do not have to collect the same information again and again. The financial services industry has worked for strong privacy protections to ensure that their customers' trust and confidence remains high.

Q. How would consumers be affected if financial services firms could not share information?

A. Financial services firms need to share information in order to provide their customers with the best advice and selection of suitable investment opportunities. Information sharing lowers the cost of financial transactions and makes conducting them easier and faster. For example, credit would be more difficult to obtain. Experts say that mortgage rates could be as much as two percent higher if financial information was not readily and easily available. Information sharing also is key to detecting and preventing fraud—it gives retailers the confidence to accept checks and enables financial firms to recognize unusual credit card or debit card behavior that may indicate the card is being used fraudulently.

Q. How can I be assured that my privacy will be protected?

A. Clear, rigorous privacy laws protect financial consumers. In fact, the new law subjects all financial companies to the most extensive privacy requirements that have ever been imposed in the United States. The law makes it a federal crime to obtain private, personal information under false pretenses. It also prohibits financial services companies from disclosing account numbers to outside parties for direct marketing, telemarketing, and emails. It gives consumers the legal right to say no or opt out of the sharing, transferring, or selling of their personal financial information by financial institutions to unrelated third parties.

Importantly, *Gramm-Leach-Bliley* requires that consumers be made aware of how a financial company protects their financial information. The new law requires financial services companies to inform their customers of their privacy policies and practices at the start of their business relationship and then at least once a year for the duration of the relationship. Companies must tell consumers about their financial information-sharing practices both within their corporate family and with unrelated third parties. Companies also must disclose the type of information that is shared. Finally, companies must let consumers know how they protect and secure consumers' financial information.

These provisions protect consumer privacy more stringently than ever before.

Q. How will the new financial privacy protections be implemented?

A. Seven federal agencies developed regulations to implement the privacy protections of *Gramm-Leach-Bliley*. The agencies are: the Federal Reserve Board; the Securities and Exchange Commission; the Office of the Comptroller of the Currency; the Federal Trade Commission; the Federal Deposit Insurance Corporation; the Office of Thrift Supervision; and, the National Credit Union Administration. They published their rules in mid-May. For more information, visit their Web sites.

Q. How will states be affected by implementation of the Act?

A. The new law does not pre-empt state laws that may provide greater privacy protections. Where state laws are stronger than the national law, they remain in effect. In addition, states are permitted to enact laws with stricter privacy provisions than federal law.

DEVELOPING YOUR PRIVACY POLICY: ISSUES TO CONSIDER

Laws enacted by Congress last year require financial services companies to take certain steps to enhance privacy protections for nonpublic, personal information. Below are some of the key issues your company should consider to comply with the provisions of the *Gramm-Leach-Bliley Financial Services Modernization Act*. Please consult with your legal and compliance officers to make certain that your company's privacy policies and practices adhere to the new federal requirements.

ESTABLISH A PRIVACY POLICY AND NOTIFY CLIENTS

All financial institutions must clearly, conspicuously, and annually disclose their policies for collecting and sharing customers' nonpublic, personal information.

This notification—written or electronic—must be provided to:

- **consumers** (those who do not have an ongoing relationship with the firm, as customers do), with certain exceptions, before this information is shared with non-affiliated third parties; and,
- **customers** when they establish a relationship with a financial institution and annually thereafter.

In their privacy policies covering nonpublic, personal information, financial institutions should include:

- categories of:
  —information that is collected;
  —information that is disclosed to affiliates and non-affiliated third parties; and,
  —persons within the financial institution who receive such information;
- how the information of former customers is shared;
- procedures to protect the security and confidentiality of information; and,
- disclosures required by the *Fair Credit Reporting Act*.

While the regulations require financial institutions to comply on November 12, 2000, the regulators will not begin enforcing *Gramm-Leach-Bliley* until July 1, 2001.

PROVIDE AN OPPORTUNITY TO "OPT OUT"

Both **consumers** and **customers** must be given notice of procedures and a reasonable means to prevent their financial institutions from transferring their nonpublic, personal information to a non-affiliated third party.

ESTABLISH PROHIBITIONS ON ACCOUNT INFORMATION DISCLOSURES

All financial institutions may not disclose account numbers for credit card, deposit, or transaction accounts to any non-affiliated third parties for use in phone, mail, and email marketing.

ABIDE BY REGULATIONS SAFEGUARDING SECURITY, CONFIDENTIALITY OF CONSUMER INFORMATION

Financial institutions must follow regulators' standards to: ensure the security and confidentiality of customers' information; protect against any anticipated threats or hazards to the security or integrity of such records; and, protect against unauthorized access to records that may harm or inconvenience the customer.

For more details, see the Web sites of the Federal Reserve (http://www.federalreserve.gov) and the Securities and Exchange Commission (http://www.sec.gov).

EMPLOYEE/CLIENT NEWSLETTER ARTICLE

The following article could be used in your employee and client newsletters. You may want to insert specific descriptions about your firm's policy.

SAMPLE NEWSLETTER ARTICLE

Privacy in the Information Age:
The Financial Services Industry Finds the Right Balance

When Congress last year passed major changes to modernize laws governing the financial services industry, legislators included several provisions that enhance the customer privacy protections that have long been a hallmark of securities firms, banks, and insurance companies.

By July 1, 2001, we, as must all financial institutions, will have to clearly, conspicuously, and annually disclose to our consumers our policies for collecting and sharing nonpublic, personal information. Specifically, these policies must disclose:

- categories of nonpublic information that are collected;
- the kinds of nonpublic, personal information disclosed to affiliates and third parties and the categories of persons who receive such information;
- how nonpublic, personal information of former customers is shared; and,
- procedures to protect the security and confidentiality of nonpublic, personal information.

[Insert paragraph about the firm's specific privacy policy.]

"OPT-OUT" RIGHTS

The new laws also require that customers be given the means by which they can prevent the transfer of nonpublic, personal information to a non-affiliated third party before this information is disclosed to that third party.

[Insert paragraph about firm's specific approach.]

ESTABLISH PROHIBITIONS ON ACCOUNT INFORMATION DISCLOSURES

All financial institutions must have in place procedures that prevent the disclosure of an account number for credit cards and deposit and transaction accounts to non-affiliated third party marketers.

[Insert paragraph about firm's specific provisions.]

SECURITY, CONFIDENTIALITY SAFEGUARDS

Financial institutions must follow regulators' standards to: ensure the security and confidentiality of customers' information; protect against any anticipated threats or hazards to the security or integrity of such records; and, protect against unauthorized access to records that may harm or inconvenience the customer.

[Insert information about your firm's policy.]

A GOOD BALANCE

These laws and regulations, coupled with our firm's long-standing policies strike a good balance between protecting your privacy and enabling us to provide you with more varied and better services.

We, like the rest of the financial services industry, have a long-established tradition of discretion and respect for clients' personal privacy. We reinforce this daily in the way we routinely handle sensitive client information as part of our day-to-day operations. Nothing is more important to our business than the trust and confidence our customers have in us.

SAMPLE OP-ED

Protecting Clients' Privacy

Our firm and the entire securities industry go to great lengths to protect the privacy of clients' personal financial information. This is one reason why public trust and confidence in the industry is so high. The high marks investors give firms for their services reflect a simple business reality: by putting the interests of our customers first and helping them to succeed, we, in turn, do well.

We think that our ability to share financial information within our company enables us to more effectively serve our customers in several ways. By knowing about investors' finances and goals, we are better informed to make suitable investment recommendations. Information-sharing protects individuals against fraud by enabling us to more precisely monitor and detect where and when fraud may occur. We can also lower the cost of doing business for customers, such as offering better mortgage rates, and providing faster turn-around on loans and insurance applications.

That said, we understand the value and importance of keeping our clients' information secure. When customers open accounts, we tell them about our own privacy protections and the 20 different federal laws that also provide safeguards.

The latest and most significant is the *Gramm-Leach-Bliley Financial Services Modernization Act*, which established four new requirements regarding the use of a consumer's nonpublic personal information. Beginning early next year, all financial institutions must annually disclose their privacy policy. Customers must be given the right to "opt out" of the use of their nonpublic, personal information by a nonaffiliated third party. Account numbers cannot be provided to any nonaffiliated, third-party marketer. Finally, the industry and regulators are working to establish policies to protect the security and confidentiality of customer records.

These efforts build on several other federal laws. The *Fair Credit Reporting Act* gives consumers the ability to halt the sharing of credit applications or other personal information with affiliated companies. This law also mandates that financial institutions notify consumers about any information sharing and gives consumers the authority to stop unwanted credit solicitations by blocking the use of the information provided. Another law, the *Right to Financial Privacy Act*, protects consumers from improper disclosure of personal information by financial institutions to federal government officials or agencies. Finally, the *Telephone Consumer Protection Act*, gives consumers the right under federal law to stop telemarketing calls from a particular company.

Taken together, these laws are among the toughest imposed on any industry.

My company believes it is important for us to have the ability to share information about our clients only if and when it is appropriate. If our brokers are to advise clients effectively about the suitability of certain investments, they must have the best and most complete information available to gauge their clients' financial ability to take risks and determine their long-term financial goals.

Our customers clearly benefit from information-sharing within our company. We have enhanced the speed at which we can make decisions on financial services and lowered our costs of doing business. And we've been able to increase the choices in services that we offer to our clients.

What we must avoid is the implementation by each state of disparate versions of privacy requirements. This is a recipe for chaos, making compliance not only cumbersome but also expensive and confusing for employees and consumers. It's important that we—the public and policymakers alike—all understand that additional privacy measures by states may have the unintended consequence of damaging consumers' interests.

Sharing information within our company helps us maximize the services that we can provide to our clients, creating, in effect, a financial services supermarket with a wide range of products all under one roof. This convenience and the potential savings to consumers are real strengths.

This is the future. Investors will increasingly demand the ability to pay bills, buy and sell stocks, and purchase homeowners insurance from one account. Their financial needs are also becoming more complex as they personally become increasingly responsible for building and managing their retirement nest eggs. An approach that links insurance, securities, and other products together to work for the consumer is the business model that will be most successful. And it's being driven by consumers. This trend—within the framework of strong, existing privacy protections—will offer consumers new opportunities to prosper. We will continue to do what we have always done—put our clients first.

EXISTING PRIVACY LAWS

Approximately 20 different federal laws already regulate information sharing and provide consumers with a plethora of privacy protections. Five, in particular, play principal roles in regulating information sharing by financial institutions.

I. GRAMM-LEACH-BLILEY FINANCIAL MODERNIZATION ACT OF 1999

Title V established a set of comprehensive privacy laws at the federal level applicable to any firm that provides financial services. The new law established four new requirements regarding the nonpublic, personal information of a consumer:

- **Annual Disclosure Of Privacy Policy**
  A financial institution must annually disclose to consumers its policy and practices regarding the protection and disclosure of nonpublic, personal information to affiliates and nonaffiliated third parties.
- **Customer "Opt Out" Of Disclosures To Third Parties**
  Consumers have the right to prevent the disclosure of nonpublic personal information to a nonaffiliated third party—commonly referred to as the right to "opt out." Third parties may not re-disclose that information.

There are important exceptions designed to resolve the practical problems with an opt-out provision. For example, opt out does not apply in cases where information sharing is necessary to produce a consolidated customer statement, complete a transaction, or service the customer's account. It also does not apply to information disclosed to market the financial institution's own products or services offered through joint agreements with another financial institution.

- **Prohibition On Disclosure Of Account Information**
  A financial institution may not disclose customer account numbers to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.
- **Regulatory Standards To Protect Security And Confidentiality**
  Financial institution regulators are to establish "standards" (related to the physical security and integrity of customer records) that would (1) ensure the security and confidentiality of customer records; (2) protect against any anticipated threats to the security of such records; and, (3) protect against unauthorized access to such records that could result in substantial harm or inconvenience to the customer.

The law also established rulemaking and enforcement authority for federal banking and securities agencies to each prescribe implementing regulations.

The law also makes it a federal crime to fraudulently obtain or cause to disclose customer information from a financial institution. This provision is aimed at the abusive practice of "pretext calling," in which someone misrepresents the identity of the person requesting the information or otherwise misleads an institution or customer into making an unwitting disclosure of customer information.

II. THE FAIR CREDIT REPORTING ACT

This law contains many important privacy safeguards. It gives consumers the ability to stop the sharing of their credit application information or other personal information (obtained from third parties, such as credit bureaus) with affiliated companies. The law permits sharing of information with affiliates regarding the consumer's performance on the loan or other "experience" resulting from the relationship between the consumer and the financial institution.

Moreover, it is important to note that the *FCRA* allows only affiliated companies to share such an application or credit bureau information, after provision to the customer of notice and an opportunity to opt out. If a financial institution were to share such information with an unaffiliated third party, it could become a consumer-reporting agency, subject to burdensome, complex, and onerous requirements of the existing *FCRA*.

The *FCRA* also mandates that other notices be provided to consumers in connection with the sharing of information. For example, financial institutions are required to notify consumers when adverse action is taken in connection with credit, insurance, or employment based on information obtained from an affiliate. This notice must inform the consumer that he or she also may obtain the information that led to the adverse action simply by requesting it in writing.

The *FCRA* also gives consumers the power to stop unwanted credit solicitations by blocking the use of their information from pre-screening by consumer-reporting agencies. Pre-screening is the process in which a consumer-reporting agency prepares a list of consumers who, based on the agency's review of its files, meet certain criteria specified by a creditor who has requested the prescreening. The *FCRA* also mandates that providers of credit include disclosures with every solicitation explaining that the offer results from a pre-screening and that the consumer has the right to be excluded from future pre-screenings by notifying the consumer-reporting agency.

III. THE ELECTRONIC FUND TRANSFER ACT

This act and its implementing regulation require that consumers be informed about a financial institution's information-sharing practices with regard to all accounts that may incur electronic fund transfers. This would include virtually all checking, savings, and other deposit accounts.

Financial institutions are required to provide consumers with extensive disclosures at the beginning of the consumer's relationship with the institution. As part of these initial disclosures, each financial institution must state the circumstances under which it (in the ordinary course of business) will disclose information concerning a consumer's deposit account to third parties. For purposes of this requirement, the term "third parties" also includes other subsidiaries of a financial institution's parent holding-company.

IV. THE RIGHT TO FINANCIAL PRIVACY ACT

Historically, the most significant privacy concern of consumers relates to **government** access to their financial records. The purpose of the *Financial Privacy Act* is to protect consumer records maintained by financial institutions from improper disclosure to federal government officials or agencies.

Specifically, the act currently prohibits disclosure to the federal government of records held by certain financial institutions without providing notification to the consumer whose records are sought and the expiration of a "waiting period," during which the consumer may challenge and prevent disclosure through legal action.

V. THE TELEPHONE CONSUMER PROTECTION ACT

This law gives consumers the right under federal law to stop telemarketing calls from a particular company. Under *TCPA*, companies can make telemarketing calls to residential telephones only if:

- the call occurs between 8 a.m. and 9 p.m. (local time at the called party's location);
- the caller provides certain identifying information to the consumer; and,
- the company maintains a company-specific "do-not-call" list of persons who do not wish to receive telephone solicitations made by or on behalf of the company.

If a consumer wishes to opt out of future telemarketing calls from a particular company, the consumer only needs to indicate that he or she does not wish to be called again. The company then must add the consumer's name to the company's "do-not-call" list.

In addition, *TCPA* protects consumers by restricting the use of automatic telephone-dialing devices and prerecorded or artificial telephone messages.

The Direct Marketing Association also maintains "customer exclusion files" so that individuals may remove their names from lists compiled or maintained by the agencies and companies that are members of DMA. Names remain in the exclusion file for five years.

Written requests for withdrawal (including name, address, and Social Security number, if issued can be sent to the organizations listed below. These organizations are responsible for notifying the agencies and companies to remove the name from their lists. Mail Preference Service, c/o Direct Marketing Association; P.O. Box 9008; Farmingdale, NY 11735-9008, and the Telephone Preference Service; c/o Direct Marketing Association; P.O. Box 9014; Farmingdale, NY 11735-9014.

This was written by James Chessen, chief economist with the American Bankers Association, which granted SIA permission to reprint it as part of the tool kit.

SAMPLE SPEECH

Financial Privacy in the Information Age

Thank you. And thanks to all of you for inviting me here today. I'd like to offer some thoughts on a subject that we've all been hearing about quite a lot lately: privacy. Of course, there's a direct connection between the escalating concerns about privacy and that technological phenomenon called the Internet that's transforming our lives on a daily basis. As the Internet has increased our access to information of all kinds, it's placed the privacy issue squarely on the front burner and turned up the heat. So today I'd like to take on the task of shedding a little of reason's light on this difficult issue.

I'll begin by introducing several examples that illustrate the need for balancing the benefits of privacy with its very real costs. Next, I'll point out two privacy initiatives currently afoot that I think are misguided. After that, I'll bring you up to date on what the securities industry is doing—and has been doing—to protect customers' privacy. I'll conclude with some thoughts about how we ought to proceed from here. I think you'll see that privacy is something our industry has taken seriously for a long time, and that recent developments have strengthened our commitment in that area.

In the abstract, privacy seems like a good thing. It appears to be one of those fundamental values that everyone supports. Yet even when we're dealing with a fundamental value, it's possible to get too much of a good thing. So we always have to ask the questions, "How much is enough?" and "How much is too much?".

Let's look at a more down-to-earth example. On the one hand, complaining about "junk mail" in this country has been elevated to the status of a national pastime. Yet when we're confronted by the prospect of increasingly targeted solicitations made possible by refinements in database marketing techniques, some of us get uncomfortable. And the question is, what do we really want? More privacy? Or more solicitations for goods and services that are of genuine interest to us? Perhaps we'd also have to factor in the lower costs for those goods and services that are made possible by greater marketing efficiency. I think you can see that whatever choice we make involves a difficult balancing act.

Next, consider the recent controversy surrounding DoubleClick, one of the new breed of Internet advertising agencies. As you may have heard, DoubleClick was planning to merge a large consumer

database with "anonymous on-line activity across Web sites," as the company's CEO put it recently in a *Wall Street Journal* editorial. The resulting protests and threats of lawsuits forced the company to put its plans on hold.

I certainly can't claim to be familiar with all of the ramifications of the DoubleClick case. But it is worthwhile to reflect on the fact that, just a few short years ago, the Internet was headed squarely towards a subscription-only model. Under that model, there wouldn't be any ads, but you'd have to pay a fee for surfing your favorite Web sites. That's a far cry from what we have now—free access to an incredible variety of Internet resources. Like network television, the Internet has evolved to a largely free medium because of advertising. And what makes companies willing to pay for advertising is the confidence that they can reach prospects who are interested in what they have to sell. That requires a certain amount of information about who those prospects are and what they buy.

The DoubleClick case and others like it have generated a number of proposals at the state level for more stringent privacy regulations. The securities industry is firmly opposed to this way of dealing with the problem. In today's national market for financial services, firms cannot reasonably comply with 50 different—and sometimes conflicting—standards for privacy protection. We believe that this scenario would be costly and counterproductive. We also feel that the securities industry, which has demonstrated the ability to effectively safeguard confidential information, should not be subject to standards designed for other industries that might have different needs and priorities on this issue.

When I think about a state-by-state approach to privacy protection, I'm reminded of the story, which I hope is apocryphal, of the police who were chasing a criminal through the streets of a city. When the criminal fled into a building, their first thought was to surround the building. But then they realized that the building was so large, and had so many exits, that they didn't have enough policemen on the scene to do that. So they surrounded the empty building next door, which was smaller and had fewer exits. In similar fashion, state legislatures should be encouraged to take the time to think through an issue carefully before acting. Otherwise, the result could be policies that are costly and misguided.

I suggested at the outset that the securities industry balances its need for sensitive information with effective privacy safeguards. I'd now like to back up that claim with a few specific examples.

Support for customer privacy in the securities industry derives from a broad framework of constitutional and common law principles, state and federal statutes, Securities and Exchange Commission rules, and self-regulatory organization rules that prohibit the improper use of sensitive information. The most recent of these is the *Gramm-Leach-Bliley Financial Modernization Act*, which was signed into law by President Clinton on November 12, 1999. This law introduced a number of important financial reforms, but I'll limit my comments

to what it says about privacy. First, the law requires all financial institutions to disclose their privacy policies to customers at the outset of the relationship and at least once a year thereafter. In addition, customers can "opt out" of information-sharing arrangements—that is, they can choose not to allow their name and other personal information to be shared with non-affiliated third parties.

The act does permit sharing of information among affiliates within a financial holding company as had been allowed before the new law. However, I would argue that this kind of sharing is a net positive for all concerned. Given the rapid consolidation within the financial sector—which is likely to accelerate as a result of *Gramm-Leach-Bliley*—many companies participate in several lines of business. Sharing information among these lines of business means better service and more opportunities to give the customer what he or she wants and needs. One of the reasons that customers choose a diversified financial firm is for the one-stop shopping it offers. It only makes sense to let such firms fulfill the role that customers expect of them.

Beyond *Gramm-Leach-Bliley*, there are other privacy safeguards that have been in place for quite a while. By common law, for example, a securities firm owes its customers the duties of loyalty and care. A firm that negligently discloses or intentionally benefits from confidential information at the expense of a customer could incur civil liability for its actions under these common law principles.

Similarly, certain abuses of a customer's confidential information would undoubtedly give rise to violations of federal and state securities laws as well as the regulations of the Securities and Exchange Commission, or SEC, the government agency that oversees the behavior of firms in the securities industry. For example, any firm or affiliated person that uses non-public information from a customer—without consent—to trade securities on its own behalf would run afoul of securities laws prohibiting fraud and misrepresentation and be subject to civil liability, SEC enforcement action, and possible criminal liability.

The securities industry also has self-regulatory organizations—SROs, we call them—that have rules addressing misuse of confidential information. And unlike many industry associations, our SROs have the authority and the staff to investigate and enforce violations of their rules. SRO rule violations can therefore lead to substantial penalties.

Aside from all of these industry-specific safeguards, there are laws on the books like the *Fair Credit Reporting Act*, which restricts the use and transfer of confidential financial information. Although the law was designed to apply to the activities of credit reporting agencies, it covers any individual or entity that collects or communicates information covered by the act, including securities firms. Another law, the *Right to Financial Privacy Act*, protects consumers from improper disclosure of personal information by financial institutions to the federal government.

Apart from the network of laws and regulations protecting customers in our industry, it's clearly in the self-interest of securities firms to avoid inappropriate uses of sensitive information. The preservation of confidentiality has been a point on which securities firms have competed since the industry's inception, and the competition has only intensified as customers' consciousness about privacy has been raised. Any firm that developed a reputation for taking that obligation lightly would quickly find itself with a rapidly shrinking customer base. Moreover, firms fiercely guard their customer information to prevent it from falling into the hands of competitors. They are not likely to do anything that would jeopardize that valuable asset. To do so would clearly be self-defeating.

Let me return for a moment to a point I made earlier. At the beginning of my talk, I discussed how unrestricted freedom could violate other rights—for example, the right to privacy. The opposite can also occur. If we tilt the scales too far in the other direction, privacy can infringe on the freedom of individuals and companies to handle information in ways that most of us would find completely harmless and even beneficial. We must pursue a balance between freedom and privacy that does justice to our customers' needs for confidentiality but also to the needs of this vibrant free-market society we live in.

The fact is, when it comes to privacy, the securities industry is doing what it has always done—protecting its customers' confidential information. Not only is it one of the most carefully regulated industries we have, but it's an industry where public trust and confidence have long been recognized as a *sine qua non* [seeneh quah known], a Latin phrase meaning an essential element of doing business. All we're asking for is to be judged by our own record and to be governed by regulations that make sense for our industry. Before we add more restrictions on information sharing, we should let existing laws work and educate consumers about those laws and the steps they can take to protect their privacy.

In closing, I'd like to share with you a story about the day J. Edgar Hoover, the former FBI chief, received a memorandum whose margins were too small for his liking. In big red letters he scrawled an angry warning across the top that read, "Watch the borders!" The next morning his frightened aides transferred 200 FBI agents to Canada and Mexico.

We have a choice in developing this country's regulations on privacy. We can overreact, as Mr. Hoover's aides did, or we can approach the matter calmly and rationally. Let's not rush to enact more regulations when current ones will do the job. And let's not try to fix what's not broken.

Thank you.