

PERSONAL INFORMATION IN FINANCIAL SERVICES: THE VALUE OF A BALANCED FLOW

Fred H. Cate

Executive Summary

The most valuable resource held by any financial institution is public trust. Historically, the focus of the financial services industry's trust relationship with customers has been on the responsible handling of information—protecting against unnecessary disclosure or fraudulent use, ensuring the accuracy and security of that information, *and using information productively— so that the customer benefits*. Few customers commit their personal information to financial institutions without the expectation of personal benefit: interest on a savings account, money to buy a house or car, insurance against unanticipated loss, gains in the stock market to provide for a comfortable retirement.

The responsible use of information to serve the needs of customers is the very definition of the trust relationship that financial institutions have such a long history of achieving and it is exactly what most people expect of the financial services industry. *It is the balance between respect for personal information and its responsible, productive use that has yielded exceptional benefits for consumers and contributed to the longest sustained economic growth in modern history. Opt-in legislation and limits on affiliate-sharing threaten to destroy that balance, and with it the many benefits that have resulted from responsible information use and the economic prosperity to which that use has contributed.*

The Beneficial Uses of Personal Information by Financial Institutions

The importance of information-sharing in the modern American economy cannot be overstated. The rapid and reliable availability of accurate and complete personal information is essential to—it is no exaggeration to say that it is the very foundation of—virtually all financial services. The benefits of responsible information-sharing include:

➤ Improving the Speed, Availability, and Affordability of Credit and Other Financial Services

The almost universal reporting of personal information about consumers is the foundation of consumer financial services in the United States and, in the words of economist Walter Kitchenman, a “secret ingredient of the U.S. economy’s resilience.” The responsible use of personal information enhances the speed of credit, insurance, and many other financial services decisions; reduces the cost of virtually all financial services; gives consumers real choices; facilitates consumer mobility; and “democratizes” opportunities.

➤ Providing Efficient, Reliable Service

The sharing of personal information is essential to the services that financial institutions provide to their customers. In fact, many transactions performed today by financial institutions require access to customer information across affiliates. For example, debit and credit card transactions, one-stop-shopping, consolidated statements and customer service, and comparison-shopping for insurance and investments all require standardized, reliable sharing of customer information.

➤ Identifying and Meeting Customer Needs

Information-sharing allows financial institutions to provide their customers with tailored services that recognize and respond to their individual needs. Financial institutions notify customers who maintain high balances in checking accounts of the availability of higher return investments; analyze customer data to protect customers against inappropriately risky investments; offer customers with recurring credit card balances lower-interest home equity loans; provide customers with bundled services at a single lower price; aggregate all of a customer's accounts to satisfy minimum balance requirements; make instant decisions whether to increase credit lines; create new investment and insurance products; and offer co-branded products, such as affinity credit cards. These uses of data allow the institution to provide customers with valuable, targeted opportunities.

➤ Informing Consumers of New Opportunities

Financial institutions use their own information, as well as data from public records and other sources, to inform consumers most likely to be interested in new products and services. Target marketing dramatically reduces the cost of soliciting customers, thereby lowering their costs and improving the likelihood that a customer will in fact be interested in the service or product; reduces the impact on the environment; and allows new and smaller businesses to compete more effectively with well-established competitors.

➤ Preventing and Detecting Fraud

The financial services industry uses personal information to prevent and detect fraud, recognize atypical behavior that may signal unauthorized credit card or debit card use, share information about lost or stolen cards with affiliates, reduce fraudulent insurance applications and claims, recover stolen funds, and deter money laundering.

➤ Ensuring Solvency and Facilitating Safety

Access to customer information helps ensure the solvency of the U.S. financial services industry. That information helps companies innovate, attract customers with new services and products, control costs, target market, prevent and detect fraud, make better decisions about loans and credit opportunities and avoid delinquencies and bad debts. *In short, access to personal*

information, in the words of Federal Reserve Board Chairman Alan Greenspan, makes individual financial institutions “more creditworthy and efficient,” and the U.S. financial services sector “more transparent and stronger in general.”

Responsible information-sharing also facilitates compliance with legal obligations. Regulators and auditors use standardized data to identify unusual transactions and accounts, evaluate the risk associated with different portfolios, and compare institutions and portfolios nationwide. Internally, many financial institutions centralize their compliance activities in a central unit, responsible directly to the CEO or President. This helps ensure effective oversight across all affiliates and guarantee the independence of institution officials responsible for compliance.

➤ Improving Efficiency and Lowering Costs

Financial institutions rely on personal information to operate more efficiently and reduce costs to consumers. Affiliated companies can combine their data systems and operations, thereby acquiring information systems more cost-effectively, avoiding the costs of maintaining redundant systems, and employing fewer technicians. Information-sharing also allows financial institutions to outsource many basic business operations, such as customer account servicing, records management, claims administration, auditing, check-printing, and certain compliance functions. Integrated data systems and third-party contractors offer enhanced services, customer convenience, and lower costs.

➤ Serving the Underserved

The many services that financial institutions use information to provide are especially important for middle- and lower-income Americans. The middle class and previously unserved or underserved populations benefit most directly from lower financial services prices, the dramatic expansion of financial services, 24-hour online banking, reduced transaction costs of stock purchases and other investments, consolidated statements and service centers, universally accepted credit and debit cards, instant credit, and the creation and marketing of new investment products. Market-wide information sharing allows for a vibrant reinsurance market, which permits broader sharing of previously unacceptable risk. As a result, many Americans who were previously thought uninsurable, today can obtain reasonably priced policies. *Information-sharing has allowed the financial services industry to deliver benefits to those Americans who need them most.*

➤ Promoting Competition and Helping Small Companies

New and smaller financial institutions—such as community banks, independent insurance agents, and Internet brokerage services—use accessible personal information to compete more effectively with larger companies. Target marketing allows companies without extensive customer lists of their own or the resources to engage in mass marketing, to reach customers most likely to be interested in their products or services. The ability to outsource information processing and

marketing tasks permits companies to manage data effectively without investing in expensive information systems and personnel. Data-sharing allows new companies to emerge that specialize in single financial services products or services. Similarly, data-sharing is a prerequisite for *independent* agents and brokers, who offer their clients a wide range of products of services offered by many different companies. Enhanced competition increases opportunities for customers and reduces prices.

➤Facilitating E-Commerce and Innovation

Responsible information-sharing facilitates innovation in financial services and products and the ways in which they are provided to customers. In addition, one of the largest components of electronic commerce in the United States today is in the field of financial services. Online stock trades, insurance applications, and banking services—effectively all digital financial services—require sharing information.

The Threat of New Limits on Information Flows

To provide all of these and other opportunities, access to data is essential. Laws restricting affiliate-sharing or requiring ad hoc opt-in consent make the provision of these services, and the convenience and benefits they provide, untenable. It is no answer to condition these services and products on consumer consent, because it is impractical and prohibitively expensive to build and operate the systems that compare data in literally millions of accounts on an ad hoc basis. Virtually all of these information uses depend upon the routine availability of standardized, reliable, complete data. Moreover, the sheer cost of seeking consent would act as a dramatic disincentive to investing in innovation.

This does not mean that privacy is unimportant or unprotected, but rather that it must be balanced—as consumers do everyday—with the benefits that flow from the responsible use of personal information.

PERSONAL INFORMATION IN FINANCIAL SERVICES: THE VALUE OF A BALANCED FLOW

Fred H. Cate¹

I. The Importance of Balance

The financial services industry's use of personal information has been the subject of recent intense debate. The Gramm-Leach-Bliley Financial Services Modernization Act was almost derailed because of the controversy surrounding data privacy.² Ultimately, the Conference Committee adopted, and the House and Senate passed, a bill containing significant, effective protection for personal privacy. Subject to limited exceptions, the new law permits a financial institution to transfer any "nonpublic personal information" to nonaffiliated third parties so long as the institution "clearly and conspicuously" provides consumers with a notice about its policies and practices for disclosing personal information, and an opportunity to opt out of such transfers.³ The law requires financial institutions to inform customers of their policies toward sharing information among affiliates, but it wisely imposes no restrictions on such information-sharing. The Gramm-Leach-Bliley Act thus reflects and preserves the balanced approach to information privacy that has for so long characterized U.S. law.

Opponents of the Act, and of the balanced approach to privacy it represents, were quick to criticize it as not going far enough to protect privacy. Two of the most common attacks are that the new law does not require affirmative opt-in consent from consumers before financial institutions can collect or use information about them, and that the law does not regulate information-sharing among affiliates. The President had not yet even signed the Gramm-Leach-Bliley Act when Congressmen Ed Markey (D-Mass.) and Joe Barton (R-Texas) introduced in the House, and Senators Richard Shelby (R-Ala.) and Richard Bryan (D-Nev.) introduced in the Senate, identical bills that would require financial institutions to obtain affirmative opt-in customer consent before transferring personal information to any third party or even to an affiliate.⁴ This issue is also being pursued in state legislatures. In as many as half of the 41 states with legislatures in session this year, including some of the largest, legislators have introduced or are likely to introduce opt-in legislation that would apply to disclosures to affiliates as well as third parties.

¹Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington; Senior Counsel for Information Law, Ice Miller Donadio & Ryan, Indianapolis, IN. The author is grateful for the generous assistance of Marty Abrams, Nancy Baran, Richard Fischer, Sarah Jane Hughes, Julia Johnson, Michael Staten, Walter Kitchenman, and Harvey Pogoriler. The author alone is responsible for the contents herein.

²Gramm-Leach-Bliley Financial Services Modernization Act (S. 900), 106 Pub. L. No. 102, 113 Stat. 1338, 1436-1450, title V (1999).

³Id. §§ 502(a)-(b).

⁴Consumer's Right to Financial Privacy Act, H.R. 3320; Consumer's Right to Financial Privacy Act, S. 1903.

These legislative proposals are problematic for many reasons. They would change the delicate compromise worked out by the Conference Committee before the Gramm-Leach-Bliley Act has even taken effect, much less been tested in practice. They ignore the restrictions already imposed by existing federal law on financial institutions' use of personal information. For example, the Fair Credit Reporting Act already prohibits financial services companies from sharing third-party credit-related information about consumers with affiliates without first providing consumers with "clear and conspicuous notice" and an opportunity to opt out of the information-sharing.⁵ The Electronic Funds Transfer Act requires that financial institutions notify their customers about the circumstances under which those institutions, in the ordinary course of business, will disclose information about customer accounts to any other party, including affiliates.⁶ The Federal Trade Commission Act prohibits "unfair and deceptive practices in or affecting commerce"—including failing to abide by a stated privacy policy or other activities that violate privacy promises, contracts, and disclosures—by any business, specifically including banks.⁷ In sum, many of the legislative proposals to further strengthen the privacy protection afforded by the Gramm-Leach-Bliley Act duplicate or conflict with existing legal protections.

Another problem with many of the state proposals for additional legislation is that they are specifically preempted by the Fair Credit Reporting Act, which preempts any state law or regulation dealing with a number of subjects, including "with respect to the exchange of information among persons affiliated by common ownership or common corporate control."⁸ To the extent a state adopts any law or regulation affecting information-sharing among affiliates, it is preempted through January 1, 2004.

⁵15 U.S.C. §§ 1681-1681t (1999). The only exception is for information drawn from the affiliated companies' own "transactions and experiences" with the consumer. *Id.* § 1681a(d)(2)(A)(i).

⁶*Id.* § 1693c(a)(9); 12 C.F.R. § 205(b)(9).

⁷15 U.S.C. §§ 45(a), 57a(f).

⁸*Id.* § 1681t(b). The law excepts two provisions of Vermont law, Vermont Stat. Ann., tit. 9, §§ 2480e(a), 2840e(c)(1).

But the greatest problem posed by the flurry of pending bills that would prohibit financial institutions from using personal information without obtaining opt-in consent and that would extend that requirement or apply opt-out to information-sharing among affiliates, is that *those bills ignore the substantial value of information and the essential need for information-sharing*. For more than a century, the balance between open information flows and personal privacy has undergirded both lawmaking and judicial precedent concerning restricting information flows to protect privacy. As Robert Litan, Cabot Family Chairholder in Economics, Vice President, and Director of the Economic Studies Program at the Brookings Institution, has stressed: “A common theme that implicitly runs through both the federal and state laws” is that the governmental privacy protections are only permitted when they target “specific types of information and providers where a balancing test can be reasonably construed to warrant government intervention.”⁹

II. The Beneficial Uses of Personal Information by Financial Institutions

The importance of information-sharing in the modern American economy cannot be overstated. As Comptroller of the Currency John Hawke, Jr., testified before Congress in 1999, the whole financial services sector is an “information-driven industry. . . . Information exchanges thus serve a useful and critical market function that benefits consumers and financial institutions alike, in facilitating credit, investment, insurance and other financial transactions.”¹⁰ The rapid and reliable availability of accurate and complete personal information is essential to—it is no exaggeration to say that it is the very foundation of—virtually all financial services. The Federal Reserve Board reported to Congress in its report on personal information and financial fraud: “[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy.”¹¹

Financial institutions use this information in many different ways, depending upon the type of institution, transaction or activity, and information involved. While it would obviously be impossible to identify all of those uses and the benefits that flow from them, they may be summarized in ten broad, overlapping categories.

⁹Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, in Lucien Rapp and Fred H. Cate, eds., *European and U.S. Perspectives on Information Privacy* (forthcoming).

¹⁰Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of John D. Hawke, Jr.).

¹¹Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2* (1997).

A. Improving the Speed, Availability, and Affordability of Credit and Other Financial Services

The U.S. economic boom and the public's standard of living depend in large part on the availability of almost \$6 trillion in outstanding mortgages and other consumer loans. Consumer credit finances homes and cars, funds college educations, and provides the credit cards that consumers use everyday to purchase goods and services. *The "almost universal reporting" of personal information about consumers is, in the words of economist Walter Kitchenman, the "foundation" of consumer credit in the United States and a "secret ingredient of the U.S. economy's resilience."*¹² U.S. consumers have access to more credit, from a greater variety of sources, more quickly, and at lower cost than consumers anywhere else in the world. The same is true of many other financial services.

Information enhances the speed of credit, insurance, and other financial services decisions. The ability to make rapid and appropriate decisions about credit, investment opportunities, insurance, and a wide range of other financial services depends on ready access to information about consumers. Even very significant decisions about financing a college education or a new home or writing health or life insurance are often made in a matter of minutes or hours, instead of weeks or months as is the case in most other countries, because consumer information is readily accessible. Financial institutions collect information from many sources on myriad aspects of consumer activities to maintain the accurate, up-to-date files necessary to support rapid and accurate financial decisions.

¹²Walter F. Kitchenman, U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns 1 (The Tower Group 1999).

Information reduces the cost of financial services. Accessible information also significantly reduces the cost of many financial services. Reliable, centralized, and standardized consumer credit information makes it possible to pool consumer loans and then sell them to investors. This process—known as securitization—makes more capital available to consumers and greatly reduces the cost of credit. Today, more than 30 percent of consumer loans are securitized. As a result, Kitchenman calculates, mortgage rates in the United States are as much as two full percentage points lower than in Europe.¹³ With outstanding mortgage rates approaching \$4 trillion, *American consumers save as much as \$80 billion a year because of the efficiency and liquidity that information makes possible.* Similarly, standardized personal information makes possible a vibrant reinsurance market which allows more Americans to obtain insurance and at lower rates than would otherwise be possible. The cost of credit and other financial services in the United States is also lower because the information those decisions depend on is assembled routinely and efficiently, rather than at the time the consumer desires the service. This allows insurance companies to pay claims more quickly and reliably, thereby reducing the cost of consumers pay for insurance.

Information gives consumers real choices. Complete, reliable credit histories and the national sharing of personal financial information have greatly increased both the range and sources of financial services to which each consumer has access. As a result, the typical U.S. household has more than twelve retail banking products scattered across more than six different financial institutions. Upper-middle-class two-income families average 24 credit cards from a dozen different issuers, including retailers. The wealthy aren't the only people affected: All consumers benefit by the ability to “shop” for financial services based on price. As discussed in greater detail below, standardized, reliable personal information allows companies to provide insurance to Americans who were previously thought uninsurable, and to offer innovative, flexible investment opportunities to families who would otherwise not be able to afford them.

¹³Id. at 7.

Information facilitates consumer mobility. Another benefit to consumers of this information-based financial system is the ease of obtaining financial services when moving or doing business far from home. “Portable [credit] histories mean that both people and capital are more mobile, which is an important advantage in a more competitive global business environment.”¹⁴ The availability of that information, which facilitates both speedy and nationwide access to financial services, also helps U.S. consumers avoid or more rapidly overcome the dislocations that are the inevitable result of a more global economy, freer trade, and a rapidly changing job market.

Information “democratizes” opportunities. More complete, reliable, and widely available personal information, and the securitization and reinsurance that standardized information makes possible, have increased the number of Americans who now qualify for credit, insurance, and other financial services, and increased the confidence of serviced providers in meeting the needs of this previously underserved population. The result has been what has been called a “democratization” of financial opportunity: In the United States, you get credit, insurance, investment opportunities, in fact, a wide range of financial services, based on your record, not your name or how long you have known your banker or broker. Access to one company’s transaction records involving the consumer is not enough; standardized, centralized information that includes a complete picture of a consumer’s financial resources and activities is essential.

All of these benefits are lost or diminished if opt-in consent is required before personal information may be collected, used, or disclosed. The speed, efficiency, and lower cost that flow from information-sharing depend on information being shared *prior to* the time it is needed. If a bank must begin from scratch the process of collecting and verifying information about a customer who has applied for a mortgage, that process will take much longer than it does today, when most of that information is already available in the financial system, and the cost of that mortgage will necessarily be higher. Moreover, the standardization of consumer information that facilitates rapid information transfers, credit scoring, and securitization of loans, becomes impossible if information must be collected on an ad hoc basis, only after consent is obtained. In addition, precisely because consumers today have no legal right to control many forms of information collection about them (other than to ensure its accuracy), financial institutions can rely more completely and rationally on that information. After all, how many consumers, if given the choice, are going to consent to the reporting of negative information about their past financial activities?

In sum, the responsible sharing of personal information, subject to the existing requirements of the Fair Credit Reporting Act and other applicable laws, makes more financial services available to more people, faster, at lower cost, and with greater fairness and reliability than would otherwise be possible.

¹⁴Kitchenman, U.S. Credit Reporting, *supra*, at 1.

B. Providing Efficient, Reliable Service

The sharing of personal information is essential to the services that financial institutions provide to their customers. In fact, virtually every transaction performed today by financial institutions requires access to customer information across affiliates. There are many examples. Credit and debit card transactions—the very core of most consumers’ daily financial activities and key resources for customer convenience—necessitate extensive, responsible sharing of basic customer information. In 1998 the financial services industry handled 11 billion ATM and 5 billion credit card transactions, not to mention 28 billion checks. Consider the number of parties involved in a single transaction: the bank or retailer that accepts the debit or credit card, the financial network that processes the transaction, the information networks that transmit the information, the financial services institution that issued the card and verifies withdrawal or credit limits, the bank that deducts the funds from the customer’s account or applies the transaction to the customer’s approved credit-line, the operations that verify that the transaction has been completed, the internal and external auditors within every institution involved who review the transaction, and the customer service units within each entity who answer customer questions. *These transactions could not be completed without information-sharing.*

Information-sharing also allows for one-stop-shopping and service. Many financial services industry executives report that among the most frequent requests they hear from customers are for consolidated statements, simplified and unified reporting about their accounts, and single-number telephone access to all of their account information. As the *Wall Street Journal* editorialized this past fall, in opposition to additional protection for financial information, “*if a single cry goes up from modern man, it’s ‘Simplify my life.’*”¹⁵ To respond to this persistent demand requires that the diverse affiliates through which a single company offers insurance, brokerage, banking, and other services be able to communicate customer information with each other. “Otherwise, consumers would be forced to receive multiple statements, or to make multiple telephone calls, to deal separately with each type of account—a costly and inefficient result for consumers and financial institutions alike.”¹⁶

It is no answer to say that the financial institutions should offer all of its services and products through a single company. It is illegal under current federal and state law to do so. For example, the Gramm-Leach-Bliley Act, touted for knocking down regulatory barriers, still requires that insurance or annuity underwriting, insurance company portfolio investments, real estate development, and merchant banking be performed through a holding company affiliate, rather than a bank subsidiary.¹⁷ Moreover, the personnel, capital, and other resources necessary to

¹⁵Privately Held Concerns, *Wall Street Journal*, Oct. 22, 1999.

¹⁶Financial Privacy Hearings, *supra* (statement of L. Richard Fischer).

¹⁷See 12 U.S.C. § 1843(k)(4).

offer one financial service, for example, consumer loans, are often different from those necessary to offer another service, for example, insurance. Some activities are simply too incompatible to be offered through single entity.

It is also no answer to rely on affirmative consumer consent. Many of the most common consumer transactions—for example, cash withdrawals at ATMs, purchases with credit cards, and payments by check—involve many businesses that few customers ever see. Today there are two national and 43 regional point-of-sale and ATM networks, linking over 15,000 financial institutions and over 500 million cardholder accounts with more than 4 million merchants. How are these essential parties to obtain or verify consent from customers they will never encounter? Moreover, debit and credit card and check-cashing networks depend upon the instantaneous availability of standardized, reliable data. Other highly valued services, such as consolidated statements and customer service, could not exist if consumers were given the choice about the sharing of information about their accounts, because few financial institutions could realistically provide both consolidated and nonconsolidated services. To do so would require one 800-number manned by one set of customer representatives using one information system for customers who consented to affiliate-sharing, and a panoply of additional 800-numbers manned by teams of other customer representatives using a variety of other information systems each covering only a single aspect of a customer's portfolio for those customers who did not consent. This is an area where there is no room for consumer choice—opt-in or opt-out: Service must either be provided on a consolidated basis for all (which is the overwhelming choice of most consumers) or for none (in which cases all customers must endure the added cost and inconvenience of separate statements and service centers).

Before computer networks made centralized data management possible and affordable, financial institutions provided customers access to information about their accounts, each maintained by a separate affiliate, through a bewildering array of hundreds or, in some cases, thousands of 800-numbers. Today, information-sharing allows these companies to offer their customers access to all of their financial information through a single 800-number, answered 24-hours a day because of the economies of scale made possible through routine data-sharing among affiliates. *New restrictions on affiliate-sharing or requirements that companies first obtain consumer consent before sharing data about them would make it impossible for the financial services industry to provide customers with the type of convenient, efficient service they have come to expect.*

C. Identifying and Meeting Customer Needs

The sharing of personal information empowers the financial services industry to identify and meet customer needs rapidly and effectively. According to Federal Reserve Board Chairman Alan Greenspan:

[I]nformation technologies have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even five years ago. . . . Prior to the advent of what has become a veritable avalanche of IT innovations, most of twentieth century business decisionmaking had been hampered by limited information. . . . [T]he recent years' remarkable surge in the availability of real-time information has enabled business management to remove large swaths of inventory safety stocks and worker redundancies, and has armed workers with detailed data to fine tune product specifications to most individual customer needs.¹⁸

Federal Reserve Board Governor Edward Gramlich echoed this theme in testimony before Congress in July 1999: "*Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy.*" The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences."¹⁹

Information-sharing allows financial institutions to ascertain customer needs accurately and rapidly. By examining patterns of customer transactions across affiliates, comparing customer comments shared with different affiliates, and using information to better understand customer objectives, financial institutions can anticipate customer needs and measure likely demand for potential products and services. As Chairman Greenspan wrote to Congressman Ed Markey (D-Mass.) in 1998: "Detailed data obtained from consumers as they seek credit or make product choices help engender the whole set of sensitive price signals that are so essential to the functioning of an advanced information based economy such as ours."²⁰ Restraints on information-sharing significantly impede that process, skew the data collected, and diminish its usefulness.

Information-sharing also allows financial institutions to "deliver the right products and services to the right customers, at the right time, more effectively and at lower cost," Fred Smith, founder and President of the Competitive Enterprise Institute, has written.²¹ The use of personal information to recognize and respond to individual customer needs is the definition of good

¹⁸Remarks by Alan Greenspan at the Conference on Bank Structure and Competition of the Federal Reserve Bank of Chicago, Chicago, IL (May 6, 1999).

¹⁹Financial Privacy Hearings, *supra* (statement of Edward M. Gramlich).

²⁰Letter from Alan Greenspan to Edward J. Markey, July 28, 1998.

²¹Fred L. Smith, Jr., Better to Share Information, *Desert News* (Salt Lake City, UT), Oct. 14, 1999, at A22.

banking service, epitomized by George Bailey, small-town banker played by Jimmy Stewart in the movie, “It’s a Wonderful Life.” Bailey not only knew his customers by name, but also knew their account balances and payment habits. This knowledge is what defined an effective banker because it empowered him to meet, and even anticipate, their needs. The same is true of other financial services industry sectors, where laws or professional standards require that the institution know enough about their customers to make appropriate recommendations for insurance, stocks, or other investments.

Today, the financial services industry relies not just on individual memory, but also on a vast network of computers to know their customers and offer them products and services that are appropriate for them. To be sure, the industry hopes that through the sale of appropriate services and products it too will profit, but it only profits in the long run if it meets customer needs and expectations. As a result, many banks today notify customers who maintain high balances in checking accounts or on-demand savings accounts of the availability of higher return investments. The *Los Angeles Times* reported in December 1999 about customers who are understandably “irritated if the bank fails to inform them that they could save money by switching to a different type of checking account.” But, of course, as the newspaper noted, “to reach such a conclusion, the bank must analyze the customer’s transactions”²²

Insurance companies and brokerage firms analyze customer data to ensure that customers have the appropriate investments and insurance and are not borrowing money to make inappropriately risky investments. Financial institutions offer customers with high or recurring credit card balances home equity loans, thereby reducing the consumer’s interest rate and monthly payment, but only if the lender is allowed to determine that the customer owns a home. Customers are not automatically switched from one product or service to another: To do so violates the law and leads to stiff financial penalties. Nor are customers compelled to follow the professional advice they are offered. Rather, these uses of data allow the institution to provide its customers with opportunities likely to be appropriate for them based on their demonstrated behavior.

In testimony before Congress last summer, Washington attorney L. Richard Fischer highlighted one of the fastest-growing trends, and most valued services, in the banking industry today: “relationship banking.” “The ability to share information also allows a financial institution to offer reduced rates and fees to a customer of the institution’s affiliate, permitting consumers and institutions to benefit from the inherent efficiencies of so-called ‘relationship banking.’”²³ By having a complete picture of its customers’ financial situations, banks can offer them bundled services at a single lower price than if provided on an a la carte basis. Customers win in two ways: First, they are offered a range of diversified services that are most appropriate for their individual financial situations. Second, they get those services at a lower price.

²²Edmund Sanders, *Your Bank Wants to Know You*, *Los Angeles Times*, Dec. 23, 1999, at A1.

²³Financial Privacy Hearings, *supra* (statement of L. Richard Fischer).

So, for example, a consumer may choose to link her mortgage loan with a checking or savings account at the lender's affiliate, and thereby avoid minimum balance requirements for the checking or savings account, and enjoy the convenience of being able to arrange for direct deductions from a bank account to make the monthly mortgage payment. A financial services institution can aggregate all of a customer's accounts to satisfy minimum balance requirements. It can make an instant decision whether to increase a credit line, based on its total relationship with the customer. "Information sharing also enables financial institutions to offer consumers popular products such as 'affinity' or 'co-brand' credit card accounts. Such programs provide frequent flyer miles, grocery or gasoline rebates and other benefits to credit cardholders. Other such programs permit universities and other not-for-profit organizations to benefit from cardholder use of their accounts."²⁴

To provide all of these and other opportunities, access to data is essential. Laws restricting affiliate-sharing or requiring ad hoc opt-in consent make the provision of these services untenable. How could an affinity program work if the card issuer and unaffiliated partner could not share customer data? How could a lender accurately and rapidly judge the risk of increasing a customer's credit line if it could not look at all of her accounts with affiliated companies? How would a financial services institution identify appropriate candidates for debt consolidation, if it couldn't examine both the range of outstanding debts and home ownership or other relevant criteria?

Again, it is no answer to say that the financial service industry may have access to that information after obtaining consent, because it is too costly to build and operate the systems that compare data in literally millions of accounts on an ad hoc basis. Moreover, how would a company know whose consent to seek, if it could not first determine who was an appropriate candidate for the product or service?

As a practical matter, opt-in consent both burdens and confuses customers. One major U.S. bank reported that its customers who participated in a test of various privacy policies were annoyed at the very idea of being contacted by the bank to obtain permission to contact them again in the future to offer selected opportunities. Customers expected that the bank would use information to offer them appropriate offers. The last thing they wanted was another phone call or letter asking permission to do what they perceived to be the very foundation of the banking relationship.

Moreover, individual consent is often impractical—both to obtain and use. Consider the experience of U.S. West, one of the few U.S. companies to test an opt-in system. In obtaining permission to utilize information about its customer's calling patterns (*e.g.*, volume of calls, time and duration of calls, etc.), the company found that an opt-in system was expensive to administer, costing almost \$30 per customer contacted. To gain permission to use such information for

²⁴Id.

marketing, U.S. West determined that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West *never reached the customer*, despite repeated attempts. Consequently, many U.S. West customers received more calls, and one-third of their customers were denied opportunities to receive information about valuable new products and services.²⁵

D. Informing Consumers of New Opportunities

Financial institutions use their own information, as well as data from public records and other sources, to inform consumers of new opportunities. Known as “target marketing” or “direct marketing,” this use of data allows a business to send an offer to a customer specifically identified as likely to be interested, as opposed to marketing randomly, contacting everyone in an entire geographic community, or relying solely on mass media advertising to reach likely customers. *Target marketing dramatically reduces costs to consumers by reducing the cost of soliciting customers, improves the likelihood that a customer will in fact be interested in the service or product (thereby reducing marketing costs and enhancing customer satisfaction) , and reduces the impact on the environment.*

For reasons that are not entirely clear, target marketing has provoked a public outcry. This is anomalous, for a number of reasons. First, more than two-thirds of U.S. consumers—132 million adults—took advantage of direct marketing opportunities in 1998, accounting for more than \$1.3 trillion in sales of goods and services.

²⁵Brief for Petitioner and Intervenors at 15-16, U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

Second, target marketing has been the subject of some of this country's longest-standing privacy protections applicable to the private sector. Since 1971, for example, the Direct Marketing Association has operated the Mail Preference Service (and, more recently, the Telephone Preference Service and now the E-Mail Preference Service). With a single request to each it is possible to be removed from most DMA-member company mailing, telephone, and e-mail solicitation lists. However, the DMA reports that the service is used by only three percent of the U.S. adult population.²⁶ Under the federal Telephone Consumer Protection Act, consumers can stop telemarketers from calling again simply by instructing them not to.²⁷ That Act also prohibits all telephone solicitations to residential telephone numbers before 8 a.m. and after 9 p.m. local time at the recipient's location. Under the Fair Credit Reporting Act, credit reporting agencies that furnish consumer credit information to be used for marketing credit or insurance opportunities to consumers must establish and publish a toll-free telephone number that consumers can call to have their names removed from lists provided for such direct marketing purposes.²⁸ Persons who acquire such information from credit reporting agencies for marketing credit and insurance services (*i.e.*, "prescreening") must inform consumers that credit information was used, identify the credit agency from which the data were obtained, and provide information about consumers' legal rights, including the right to opt out of future prescreening.²⁹ For all of the public angst expressed about target marketing, evidence indicates that very few consumers take advantage of their opt-out rights.

Finally, the preoccupation with target marketing is difficult to fathom because of the lack of significant harm that could result. Consumers who receive offers for products or services they don't want can discard them: it is their choice. Without target marketing, consumers would have less meaningful choice, face more mail and telephone calls, and pay higher prices. Given the high percentage of Americans who shop via direct marketing, it seems clear that the vast majority of the public value the opportunities, convenience, and lower prices that target marketing provides, and does not believe that such marketing poses a demonstrable harm. For this reason, when its demonstrated benefits are weighed against its negligible risk of harm, regulation would seem patently unjustified. Brookings' Robert Litan, a former Deputy Assistant Attorney General in the

²⁶Financial Privacy Hearings, *supra* (statement of Richard A. Barton). See also http://www.the-dma.org/home_pages/consumer/dmasahic.html#removal.

²⁷47 C.F.R. § 64.1200(e)(2). Telephone Consumer Protection Act, 47 U.S.C. § 221, is implemented through regulations promulgated by the Federal Communications Commission. 47 C.F.R. § 64.1200.

²⁸15 U.S.C. § 1681b(c)(5).

²⁹*Id.* § 1681m(d).

Antitrust Division of the U.S. Department of Justice and a former Associate Director of the Office of Management and Budget, writes:

The worst that might happen is that some consumers would receive unwelcome mail or telephone solicitations (which by law they can stop), while others would be denied that opportunity (and thus conceivably miss out on a particular “good deal” that they otherwise might enjoy). Against these potential harms is balanced the potential benefit to third parties of being able to use the database (perhaps with some errors) to finely tune its marketing campaign and thus reduce its marketing costs, a result that benefits both marketers and consumers alike. Thus, the fact that current law does not require affirmative customer consent to the sale of such data also seems appropriate.³⁰

Finally, target marketing is a key resource for new and smaller businesses—the foundation of economic growth and new jobs—by allowing them to communicate with consumers likely to be interested in their services or products. Requiring opt-in for target marketing hurts both consumers, who miss out on opportunities, and businesses, who face higher costs to reach consumers, but such a requirement imposes an especially heavy burden on small companies, which cannot afford mass market advertising and lack the extensive customer lists of their well-established competitors. Open access to third-party information and the responsible use of that information for target marketing is essential to leveling the playing field for new market entrants. Just look at the marketing practices of Internet-related companies like America Online, which gained its dominant position largely by mailing free copies of its software to people likely to be interested in Internet access. Prohibiting that activity would have denied consumers information about an opportunity that many of them obviously value and AOL access to a market it wished to serve. Requiring affirmative consumer consent before the software could have been sent would have had a similar effect, while *increasing* the number of contacts with the consumer that AOL would have been required to make. All to avoid what—an unsolicited piece of mail? Such a regulatory structure seems difficult to justify.

E. Preventing and Detecting Fraud

One key use of personal information by the financial services industry is to prevent and detect fraud. In 1998, more than 1.2 million worthless checks were entered into the U.S. banking system every day, accounting for \$12.6 billion in losses. Losses to banks alone due to check fraud—what the FBI calls the banking industry’s biggest crime problem—in 1997 reached \$512 million. Banks detected and stopped an almost equal number of fraudulent checks. Credit card issuers lost \$668 million in 1998 due to fraud. The insurance industry paid \$20 billion last year for fraudulent property and casualty claims. The Secret Service placed the cost of identity fraud in 1997—the last year for which figures are available—at \$745 million, up from \$450 million the

³⁰Litan, *Balancing Costs and Benefits of New Privacy Mandates*, *supra*.

previous year. Across the economy, it is estimated that business losses due to all forms of document fraud and counterfeiting exceed \$400 billion per year.

These losses hurt consumers, businesses, and the economy as a whole, but they create a disproportionate impact on the financial services industry which bears the greatest share of the financial loss. In the case of credit cards, for example, the law shifts the loss from consumers to card issuers, by specifying that consumers cannot be liable for more than \$50 if their cards are used fraudulently.³¹ But even then, the financial services industry usually covers even the \$50 that consumers could be required to pay. Fraud also costs the industry because of the time and resources it spends trying to prevent and detect it. And fraud hurts every consumer, even those who did not suffer a direct financial loss, through higher prices and because of the anxiety, emotional strain, and lost time that individuals experience both as the victims of fraud and in fighting against fraud.

Personal information is one of the most effective tools for stemming these losses. That information is used every day to identify consumers cashing checks and seeking access to accounts. Not only does that information help identify the purveyors of financial fraud, it also gives retailers and check-cashing services the ability and the confidence to accept checks, especially from out-of-state accounts. Close monitoring of account activity also allows financial institutions to recognize unusual behavior that may indicate that a credit card or debit card has been stolen or is otherwise being used without authorization. A credit card transaction in which a customer, who does not normally do so, buys \$2 worth of gasoline, for example, may suggest experimental use of a stolen credit card, researchers at Wharton Business School have noted.³² Moreover, because of information-sharing, a customer who reports a lost or stolen credit or debit card knows that the information will automatically be shared with all of the financial services institution's affiliates. Similarly, affiliates share information about fraud schemes and unauthorized account activity so that they can guard against such schemes system-wide. These uses of information not only offer consumers convenience, they also dramatically increase the chance of preventing further losses and of apprehending the thief.

Personal information is also a key resource used by the financial services industry to deter and detect fraudulent activity by customers and to apprehend the perpetrators. For example, insurance companies often compare information provided by applicants for health or life insurance policies with data provided by the Medical Information Bureau. By providing general, standardized information, the MIB helps insurers detect when an applicant has failed to disclose relevant information about chronic health conditions or significant past medical treatments. Similarly, if a customer defaults on a mortgage loan, that information will be shared with other financial institution affiliates, such as those that issue credit cards. If a customer engages in

³¹ 14 C.F.R. § 226.12(b).

³² Mining Data for Nuggets of Knowledge, Wharton Executive Education.

fraudulent activity, for example, check-kiting, affecting one affiliate, that information will be shared with other affiliates to prevent the customer from perpetrating a similar scheme there. And if a borrower cannot be located or has stolen institutional resources, personal information will be used to attempt to locate him, collect the debt owed, and prosecute criminally if appropriate. These uses of information help reduce the prices that other customers must pay for financial services by reducing both institutional losses and the cost of recovering institutional assets.

The financial services industry's ability to monitor personal information to detect and prevent fraud and other criminal activity has long been understood—and, in fact, required—by federal law enforcement authorities. Banks in particular are subject to a number of reporting requirements relating to the prevention of fraud and related activities, including the requirement that financial institutions notify government officials of high-value current transactions and file “suspicious activity reports.” Last year, banks met their legal obligations by filing 124,000 of these reports—called SARs—more than double the 50,000 reports filed in 1996, the first year that banks were subject to the SAR filing requirement. Recognizing the exceptional value of these uses of information to detect fraud, money laundering, and other crimes, federal regulations prohibit banks from even telling customers when they are the subject of an SAR.³³ *Responsible information monitoring deters fraudulent and criminal activity.*

³³12 C.F.R. §§ 21.11, 208.62, 353.1, 563.180, 748.1.

Requiring consent for any of these uses undermines that effectiveness in preventing and detecting fraud. “Indeed,” as Litan writes, “individuals who are most likely to defraud a third party are strong candidates for opting out or refusing to opt in to information sharing by the bank.”³⁴ Moreover, as with centralized customer service centers, they must work for all consumers or none. It is unthinkable that an individual seeking to cash a check at a supermarket could decline to provide picture identification because he had opted out of such data collection when he opened his checking account. Similarly, it is unreasonable for federal law to saddle banks with the losses resulting from credit card fraud and then not permit those banks to monitor transaction patterns in an effort to reduce fraudulent use. There is also something fundamentally unfair about prohibiting financial institutions from using for the common benefit of their customers and themselves information that they have spent millions of dollars collecting and in which they have a legally recognized property interest.³⁵ To do so not only threatens the solvency of the financial services industry, but also inevitably leads to higher prices for consumers.

F. Facilitating Solvency and Safety

Access to customer information helps ensure the solvency of the U.S. financial services industry, for all of the reasons outlined above. That information helps companies innovate, it allows them to attract customers with new services and products, to help them control costs, it permits them to target market, it gives them a key tool for preventing and detecting fraud, thereby reducing the losses caused by fraud, it helps them make better decisions about loans and credit opportunities and avoid delinquencies and bad debts. In short, *as Chairman Greenspan has noted, access to personal information makes individual financial institutions “more creditworthy and efficient,” and the U.S. financial services sector “more transparent and stronger in general.”*³⁶

Another important benefit to consumers and to U.S. markets more broadly of responsible information-sharing is the use of that information by institutions, auditors, self-regulatory organizations, and state and federal regulators. The financial services industry is subject to wide-ranging regulatory requirements designed to protect individual investors, borrowers, and depositors; guarantee institutional solvency; protect against inappropriate risk; ensure compliance with anti-discrimination laws; and promote investment in local communities. Compliance with these regulatory obligations is accomplished in large part by using personal information across all affiliates.

There are many examples. Banks’ obligation to file SARs has already been noted. Another example is regulators’ and auditors’ use of standardized data to identify unusual transactions and accounts easily, evaluate the risk associated with different portfolios, and compare institutions and

³⁴Litan, *Balancing Costs and Benefits of New Privacy Mandates*, *supra*.

³⁵In *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court characterized documents relating to a customer’s account as “the business records of banks” to which the customer “can assert neither ownership nor possession.”

³⁶*Id.*

portfolios nationwide. Internally, many financial institutions centralize their compliance activities in a central unit, responsible directly to the CEO or President of the corporation. This helps ensure effective oversight across all affiliates and guarantee the independence of institution officials responsible for compliance.

But this widely recognized “best practice” for ensuring compliance with applicable laws and regulations, like other internal and external audit functions, is untenable if information cannot be transferred across affiliates or if individual customers can block access to their data. *Effective regulatory oversight, and virtually all other measures designed to ensure the safety and security of customer funds and information, depends upon routine access to standardized, reliable customer information.*

G. Improving Efficiency and Lowering Costs

Financial institutions rely on their ability to use and share information responsibly to operate more efficiently, thereby providing their customers with desired services, more quickly, and at lower cost than would otherwise be possible. For example, because affiliated companies are permitted to combine their data systems and operations, they can acquire information systems on a more cost-effective basis, avoid the costs of maintaining separate, redundant systems, and employ fewer technicians than separate systems would require. Those integrated data systems offer enhanced services, customer convenience, and lower costs.

Information-sharing also allows financial institutions to outsource many basic business operations—such as customer account servicing, records administration, auditing, check-printing, and certain compliance functions—to third parties, who perform these operations on behalf of financial institutions. Insurance companies increasingly outsource underwriting determinations and claim administration to third parties that specialize in these activities and maintain the infrastructure necessary to perform them efficiently and accurately. As Richard Fischer, author of *The Law of Financial Privacy*, has noted, “[t]hese third-party specialists typically perform such services more efficiently, and at a lower cost, than the institution itself might, serving consumers in the most cost-effective and efficient way possible.”³⁷ Moreover, and as discussed in greater detail below, outsourcing enables smaller institutions to offer products and services to consumers that the institution otherwise simply would not have the capacity or resources to offer. “[T]he ability to share information and outsource banking operations heightens efficiency and promotes competition in the financial services sector, to the ultimate benefit of consumers.”³⁸

Of course, such outsourcing is subject to legal and contractual restraints that protect the confidentiality of personal and proprietary information and prevent it from redisclosure or use for any purpose unrelated to the outsourced function. Laws or regulations allowing consumers to opt-out of outsourcing, or prohibiting outsourcing without customers’ affirmative opt-in consent,

³⁷Financial Privacy Hearings, *supra* (statement of L. Richard Fischer).

³⁸*Id.*

would make the efficiencies, enhanced services, and lower costs impossible to achieve. No financial institution can reasonably transfer some, but not all, of a specific type of record for processing: The simple reality of the market is that it must be all or nothing.

H. Serving the Underserved

The many services that financial institutions use information to provide are important to all consumers, but they are especially significant for middle- and lower-income Americans. The wealthy are frankly better able to absorb higher prices for financial services, to engage private bankers and investment advisors, to invest in other countries, and the like. It is the middle class and previously unserved or underserved populations that benefit most directly from lower financial services prices, the dramatic expansion of credit, 24-hour online banking, reduced transaction costs of stock purchases and other investments, consolidated statements and service centers, affordable insurance, universally accepted credit and debit cards, instant credit, and the creation and marketing of new investment products for wage-earners.

Many of these benefits extend far beyond mere customer convenience or financial gain. Without information-sharing, many people would effectively be uninsurable. Market-wide information sharing allows for a vibrant reinsurance market, which permits broader sharing of previously unacceptable risk. As a result, many Americans who would otherwise could not afford insurance, today can obtain reasonably priced policies. There are many similar examples, where information-sharing has allowed the financial services industry to literally transform people's lives.

If the impact of privacy regulation is to raise the price of financial services, to reduce the availability of credit, to slow the development of low-cost investment opportunities, or to stop insurance companies from seeking reinsurance, it will be a very high cost indeed and one that will be borne disproportionately by those Americans least able to afford it.

I. Promoting Competition and Helping Small Companies

One major benefit of information-sharing is that it allows new businesses to break into the market for financial services, and smaller financial institutions—such as community banks, independent insurance agents, and Internet brokerage services—to compete more effectively with larger companies.

There are many examples, some of which have already been noted. Targeted marketing, based on personal information obtained from public records and private companies, allows companies without extensive customer lists of their own or the resources to engage in mass marketing, to reach customers likely to be interested in their products or services. The ability to outsource information processing and marketing tasks permits companies to manage data effectively without investing in expensive information systems and personnel. In fact, with the increased use of technology, smaller companies increasingly cannot compete unless they can outsource their technology needs to gain the benefits of economies of scale. Data-sharing allows

new companies to emerge that specialize in providing only one aspect of financial services products or services, for example, servicing loans, processing payments, or printing checks. Similarly, data-sharing is a prerequisite for *independent* agents and brokers, who offer their clients a wide range of products of services offered by many different companies.

The effect of enhanced competition is to increase opportunities provided to customers and to reduce prices. Yet these benefits are compromised if consumers can prohibit the sharing of their data. For example, many banks contract with other companies to process loan payments. If a customer opts out of allowing data about her loan to be shared with the payment processing company, what is the bank to do? It is impractical for the bank to provide a separate address and processing system for that one customer's loan payments. The only alternative is to deny that customer a loan in the first place. An opt-in system merely magnifies this problem. As Robert Litan has written, switching from an opt-out system to an opt-in system would inevitably "raise barriers to entry by smaller, and often more innovative, firms and organizations"³⁹

There is another benefit that results from the competitive market for financial services: The development and marketing of corporate privacy standards. As Marcia Sullivan, Vice President and Director of Government Relations at the Consumer Bankers Association has noted:

The electronic marketplace today provides a remarkable forum for the efficient, effective interaction of consumers, government and industry with regard to consumer privacy protection. Businesses and banks in particular increasingly regard privacy as a separate basis on which to compete for customers; and consumers increasingly shop for privacy as they would any desirable product or service. The American public is quite sensitive and vocal on privacy issues, and the marketplace is quick to respond to public privacy concerns.⁴⁰

³⁹Litan, *Balancing Costs and Benefits of New Privacy Mandates*, supra.

⁴⁰Hearing before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 105th Cong., 1st Sess. (Sept. 18, 1997) (statement of Marcia Z. Sullivan).

J. Facilitating E-Commerce and Innovation

One of great strengths of the United States' current system of responsible information-sharing is that it facilitates innovation in services and products and the ways in which they are provided to customers. Many of the innovations that customers take for granted are the result of advances in information technologies and the ability to aggregate and share information. As Federal Reserve Board Chairman Alan Greenspan has stressed:

Today, the marketplace for financial services is intensely competitive, innovative, and global. Banks and nonbanks, domestic and foreign, now compete aggressively across a broad range of on- and off-balance-sheet financial activities. It is noteworthy that, for the most part, this transformation has not been propelled by sweeping legislative reforms. Rather, the primary driving forces have been advances in computing, telecommunications, and theoretical finance that, taken together, have eroded economic and regulatory barriers to competition, *de facto*. Technology has fundamentally reshaped how financial products are created and how these products are delivered, received, and employed by end-users.⁴¹

Today, if a financial institution determines a better way to service an insurance policy, clear a check, or process a payment, it is free to do so, consistent with its legal and professional obligations to its customers. In an opt-in world, that institution would first have to contact every customer affected and seek their permission to handle information about them differently. Few customers care about these back-office operations, but if a single customer objected or if a single customer could not be reached to obtain her consent, the financial institution would have to either manage those customers' accounts separately from all others, or not deploy the innovative system or method. Given the impossibility of contacting, much less obtaining consent from, all customers, and the financial impracticality of maintaining separate processing systems, the end result is to restrain innovation. Moreover, the sheer cost of seeking consent—even if it could reliably be obtained—would act as a dramatic disincentive to investing in innovation.

Put bluntly, opt-in inevitably acts as a restraint on innovation, for at least three reasons. First, opt-in fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them. Second, opt-in resolves all cases of ambiguity against the prospective information use. Third, opt-in is not merely costly to administer, since it requires contacting every consumer to obtain permission for every intended use or category of use of information, it is impossible to administer effectively, because of the inherent difficulty of businesses contacting consumers, as opposed to consumers contacting business (which typically maintain regular hours, fixed addresses, and provide 800-numbers).

⁴¹Remarks by Chairman Alan Greenspan at the Conference on Bank Structure and Competition of the Federal Reserve Bank of Chicago, Chicago, IL (May 1, 1997).

The irony is that opt-in provides consumers with no more privacy protection than opt-out: Under either system, it is the customer alone who makes the final and binding determination about data use. In fact, opt-in virtually ensures greater customer annoyance, since under opt-in businesses must contact consumers to obtain permission to make the most innocuous use of nonsensitive information. It is hard to imagine that consumers will appreciate the additional flood of telephone calls and mail that compliance with an opt-in system will require.

The threat to innovation posed by opt-in and limits on affiliate-sharing would have a significant effect on the financial services industry at any time, but in the face of rapid technological growth and the rapid expansion of e-commerce, the impact could be crippling for both consumers and the financial services industry. As a result, Chairman Greenspan has cautioned against adopting laws or regulation that inhibit the industry's ability to innovate to meet customer needs: "Given the high degree of uncertainty inherent in the development of new products and processes, policymakers should be cautious when attempting to anticipate the future path of innovation, or the effects new regulations may have on innovation. . . ." This argues against the adoption of rules, like opt-in, that restrain innovation and are contrary to the interests of both consumers and business. "Incentive-compatible regulation, flexibly constructed and applied, is the logical alternative to an increasingly complex system of rigid rules and regulations that inevitably have unintended consequences, including possible deleterious effects on the innovation process."⁴²

One of the largest components of electronic commerce in the United States today is in the field of financial services, where, for example, Online stock trades account for more than one-fourth of all trades executed. Executing those trades, providing Online banking services, and effectively all e-commerce activities require sharing information. Many financial institutions have created separate e-commerce affiliates, which operate Web portals and provide online services. But those affiliates must still have access to customer account information in order to complete transactions and protect against fraud or deception. Moreover, e-commerce is never limited to a single institution; other service providers are always necessarily involved. A ban on affiliate-sharing or adoption of an opt-in system would seriously impede these innovative and valuable services. The entire function and focus of digital systems is the transmission and aggregation of information. Laws or regulations that create barriers in the operation of those system inevitably restrict the development and deployment of new customer services.

⁴²Id.

III. The Threat of New Limits on Information Flows

The most valuable resource held by any financial institution is public trust. Earning and maintaining that trust is the key to the financial services industry's long-term solvency and profitability. According to Hjalma Johnson, President of the American Bankers Association, "Privacy is the cornerstone of banking, the heart of our relationship with customers. My message to bankers this year is 'embrace technology, preserve trust,' And nowhere do these two goals come together more clearly than in protecting our customers' financial information."⁴³ The same can be said with equal force about other segments of the financial services industry.

Historically, the focus of the financial services industry's trust relationship with customers has been on the responsible handling of information. In the context of that relationship, "responsible" means, to be sure, protecting against unnecessary disclosure or fraudulent use and ensuring the accuracy and security of that information, but it also means using information productively—so that the customer benefits. Few customers commit their personal information to financial institutions without the expectation of personal gain: interest on a savings account or annuity, money to buy a house or car and insurance to protect it, gains in the stock market to provide for a comfortable retirement.

This does not mean that privacy is unimportant or unprotected, but rather that it must be balanced—as consumers do everyday—with the benefits that flow from the responsible use of personal information.

⁴³Remarks by Hjalma Johnson, President, American Bankers Association, before the ABA Community Bankers Council, Washington, D.C., November 15, 1999.

When she was acting Comptroller of the Currency, Julie Williams testified before Congress that “[t]he financial services industry has had longstanding experience in handling and safeguarding sensitive customer information and protecting consumer privacy. *Access to and use of financial information is the lifeblood of the financial services industry—ensuring that institutions make appropriate credit determinations, provide proper investment guidance, extend insurance wisely, as well as identify new market opportunities.*”⁴⁴

She could not be more correct. And she might have added that few customers would want to do business with an institution that ignored either the privacy or the profitability of personal information. A financial institution that never shared customer information would be privacy protective indeed, but it would have few customers, because it could not provide them with a range of services at a reasonable price without using information about them to do so. In sum, the goal of most financial services companies is not merely to protect customers’ privacy, it is “to bring value to our customers,” according to Gail Magnuson, former Vice President of Customer Information Policy at Bank of America.⁴⁵

The responsible use of information to serve customer needs is the very definition of the trust relationship that financial institutions have such a long history of achieving. Interestingly, despite the congressional and press outcry over privacy, Federal Reserve Board Governor Edward Gramlich testified before Congress last July that “[a]lthough we believe that information sharing between banks and third parties is fairly common, to date we have received relatively few complaints and have not found the need to initiate any enforcement actions on privacy grounds.”⁴⁶

This should not come as a surprise. The responsible use of information to serve the needs of customers is exactly what most people expect of the financial services industry. And it is the balance between respect for personal information and its responsible, productive use that has yielded exceptional benefits for consumers and contributed to the longest sustained economic growth in modern history. Opt-in legislation and limits on affiliate-sharing threaten to destroy that balance, and with it the many benefits that have resulted from responsible information use and the economic prosperity to which that use has contributed.

⁴⁴Hearing to Review the Use of Deceptive Practices to Gain Access to Personal Financial Information before the Comm. on Banking and Financial Services, House of Representatives, 105th Cong., 2d Sess. (July 28, 1998) (statement of Julie L. Williams).

⁴⁵Edmund Sanders, *Your Bank Wants to Know You*, *supra*.

⁴⁶Financial Privacy Hearings, *supra* (statement of Edward M. Gramlich).