EMBARGOED UNTIL 10AM EDTText as prepared for DeliveryJuly 21, 1999

Treasury Under Secretary Gary GenslerSubcommittee on Financial Institutions and Consumer CreditCommittee on Banking and Financial ServicesUnited States House of Representatives

Madam Chair, ranking Member Vento, and members of the Committee, I am pleased to have this opportunity to present the Administration's views on the protection of personal financial information. These issues are of great importance to the President and the entire Administration, and we look forward to working with Congress to provide American consumers the financial privacy protections that they deserve.

Privacy has been a cherished right to Americans since the founding of our nation. Originally, the idea was predominantly one of privacy from governmental interference: privacy in one's home and one's person. The citizenry's fear of governmental intrusions on privacy was rooted partly in American history -- our rejection of tyranny -- but also in practicality. Businesses had neither the means nor the incentive to invade one's privacy.

But over time, the notion of privacy has evolved. The right is no less cherished, but the threats to it are new. When, a century ago, Louis Brandeis famously enunciated privacy as a "right to be let alone," he was referring to privacy from the press.

Today many Americans increasingly feel their privacy threatened by those with whom they do business. In particular, financial institutions and others are able to consolidate information about spending and investing habits. Americans want the ability to earn, invest, and spend their money without having to expose their lives to those who process their transactions -- just as they would not expect a letter carrier to read their mail. Americans deserve that right, and financial services firms wishing to maintain their trust would benefit by embracing it.

For much of our history, consumers were justifiably confident about their financial privacy. Most of their day to day transactions were conducted in cash. They obtained financial services from local firms. Records were kept on paper ledgers rather than in computers. A small town banker, a local securities broker, or an insurance agent knew the customer's financial circumstances and tolerance for risk, to best anticipate the customer's financial needs. Yet customers were confident that the banker, broker or insurance agent would not share that information. Doing so would have been considered a breach of personal trust. That confidence is understandably on the wane today.

The first cracks in that confidence began to appear in the late 1960s, as unprecedented amounts of credit information were collected in new, national databases. Congressional hearings revealed that many credit files contained inaccurate and damaging information, and that consumers often had no way to correct errors that could lead to a denial of credit, employment, or insurance.

The resulting Fair Credit Reporting Act was the first federal law directed at financial privacy. The Act limited the purposes for which credit report information could be distributed, and granted individuals access to their credit histories and the ability to correct errors. Amendments to the Act in 1996 recognized that customers should have notice and the ability to opt out of certain information transfers. Taken together, these were significant privacy protections for their times.

Much has changed, however, since the Fair Credit Reporting Act was passed in response to the mainframe computers of the 1960s. We are in the midst of three important and significant changes in the financial services sector: a technological revolution, industry consolidation, and a move away from cash towards electronic transactions.

First, today's ordinary desktop computer is significantly more powerful than the mainframe of 30 years ago. Vast amounts of information can be stored, sorted, manipulated, and analyzed at lower and lower costs. Advances in telecommunications allow for this information to be sent virtually anywhere on the globe in a fraction of a second. Financial services firms are collectively spending billions of dollars per year to further enhance their technologies.

A second key change is the growing integration and consolidation of financial services providers. Interstate banking and branching has allowed banks to grow larger than ever before, and the removal of regulatory restraints has allowed banking organizations to offer more insurance and securities services. Even those smaller banks that have avoided consolidation often broaden their services by contracting with other financial services providers. At the same time, insurance companies are offering products that compete with bank products, and investment banks are in the lending business.

These developments have brought considerable benefits to consumers, in the form of operating efficiencies, new products, and better prices for customers. The desire of large, integrated financial services firms to profit from their scale and cross-sell their products, however, has created a powerful incentive to treat consumer data as a business asset. Consolidation and technology also have allowed the relationship between financial institutions and their customers to become increasingly impersonal. Fewer customers walk into branches to deal with a personal banker, as more customers drive up to ATMs or log onto the Internet.

Third, there is an increasing use of electronic means of payments and receipts. Americans increasing use of credit cards, debit cards and (more recently) electronic bill payment in lieu of cash now allows financial services companies to collect a far greater amount of information. Direct deposit now means that a bank knows not only what you spend but how much you earn, and from whom.

A generation ago, financial privacy meant keeping private your salary, your bank balances, and your net worth. Today, financial privacy means keeping secret your entire way of life. The typical credit report in 1970 would have shown only that a customer had received a total of, say, $5,000 of credit, and had repaid it on time. The credit card records of 1999, by contrast, can list each and every purchase ever made by that customer, sorted by date, location, and other details. Furthermore, if credit card companies work together with merchants, then the level of detail can become even more refined -- each dish ordered at a restaurant or each book title bought at a store.

Taken together, these three trends -- a technological revolution, industry consolidation, and the movement from a cash to electronic payment and receipt system -- are the means, motive, and opportunity for financial services firms to mine consumer information for profit. Our challenge, therefore, is to protect the privacy of consumers while preserving the benefits of competition and innovation.

On May 4, the President outlined the Administration's "Financial Privacy and Consumer Protection in the 21st Century" initiative. Protecting financial privacy led the list of key principles for consumer protection.

- First, the President recommended enactment of legislation to provide consumers notice and choice before their financial information is shared or sold -- the right to say "no." Central to this policy is the idea that control of the self-portrait painted by one's financial information belongs to the consumer, not the financial institution that processes the transactions.

- Second, the President stated that consumers should not have to worry that the results of their latest physical exam will be used to deny them a home mortgage or credit card. The President therefore recommended legislation that would impose special restrictions on sharing medical information within financial conglomerates and with third parties, consistent with the Administration's overall plan for protecting medical privacy. The President made clear in his State of the Union Address his intention to work with Congress to pass a strong, comprehensive medical record privacy bill this year. He has consistently encouraged legislation that would expand our authority to protect the privacy of medical information.
- Third, the President called for giving back to regulators authority to monitor compliance with privacy protections. Under the Fair Credit Reporting Act, for example, banking regulators were in 1996 prohibited from examining banks for compliance with this statute, as they do for other consumer protection statutes. Surely there is no compelling reason for treating privacy less seriously than other statutory consumer protections.

When the President announced this agenda in May, some may have viewed his proposals as ambitious. Only two months later, however, the policy of notice and choice is gaining momentum. Leadership by the President and members of this Committee and of the House has sparked a debate on this issue that has educated policy makers and produced dramatic results. Most recently, the House of Representatives passed with overwhelming bipartisan support a bill providing notice and choice before personal financial information can be shared with third parties. The House provided the enforcement mechanisms sought by the President. It also generally prohibited the use of so-called "pretext calling" -- albeit with an unwarranted exception that would allow investigators to commit fraud in child support cases, while a subpoena would be the best approach.

Acceptance of the idea of notice and choice is an important step in protecting financial privacy. Consumer choice over third party sharing, however, should be the floor, not the ceiling. We should move forward to consider how consumers can exercise choice over sharing of transaction and experience information within financial conglomerates -- especially conglomerates which, under H.R. 10 and S. 900, would be able to engage not just in financial activities, but also activities incidental and complementary to such financial activities. We should prevent exceptions from swallowing the rule by prohibiting re-use of shared data beyond the purpose for which it was shared. We should further ensure that any new federal legislation add to – as we believe H.R. 10 does, but should do so more clearly – rather than preempt existing protections in federal and state law. And we should consider how to make any privacy protection regime workable, all the while keeping in mind the significant economic benefits that information sharing can bring to consumers.

With that in mind, I will address five basic issues that we believe the Congress ought to consider as it moves forward with financial privacy legislation: what information such legislation should cover; what notice is appropriate; what choice is appropriate; what exceptions may be appropriate; and how any privacy regime is to be administered.

Madam Chair, you also requested that I discuss various privacy issues relating to the privacy practices of state governments and the federal government, and of the Treasury Department itself. I am attaching as an appendix a discussion of those issues not addressed in my testimony.

Scope

The first issue is what financial information should be protected. Under the Fair Credit Reporting Act, there are currently no limits on sharing information about consumers' transactions and experience. Thus, financial institutions currently are able to treat what a person buys with checks and credit cards as information belonging to the institution, and are free to sell it.

The Administration believes that this transaction and experience data must be protected, regardless of the type of financial institution at which it is held. Checks written on a checking account should share the same protections as checks written on a money market account. H.R. 10 adopts this sound approach.

We must consider, though, a future where financial information may be consolidated -- and potentially mined -- at non-financial firms. Many of us already provide a list of our assets to Internet web sites, where daily performance can be monitored. Consumers might be surprised if a list of stocks held at an Internet brokerage site were protected as confidential, but a list of stocks entered at another type of web site could be freely sold without notice or consent.

Eventually, we may wish to look beyond financial privacy. Like financial institutions, booksellers and other retailers can build considerable databases and can sell them without customer knowledge or consent. Your on-line bookseller may not only know what books you read, but what books you considered buying, where you vacation, what music you listen to. The Administration continues to support efforts at self-regulation. Industry efforts over the past year have been impressive, but they still have a long way to go. We will want to continue scrutiny of these non-financial areas.

Notice

Notice is fundamental to privacy protection. The Administration believes that every financial institution should establish and disclose a privacy policy that encompasses information sharing with both affiliates and third parties. Disclosure of an institution's information practices is a precondition to consumers choosing how their information will be used, or choosing to do business elsewhere.

The Administration believes that a meaningful notice should be provided before a customer opens an account and at least annually thereafter. The contents of the notice should be sufficient to inform the customer of the uses that will be made of their information and to whom it will be transferred.

That said, the exact contents of a notice may be best left to a rulemaking process where public comment can be solicited.

Choice

The next issue is that of choice -- under what circumstances customers should be able to restrict the uses a company makes of their data. The Administration believes that consumers should have the choice to opt out of -- that is, say "no" to -- the use of their data by both third parties and affiliates.

Although the uses of affiliate sharing generally tend to relate more to the consumer's original expectations than third-party sharing, this will not always be the case. Under both pending financial modernization bills, affiliates of banks will be permitted to engage in any financial activity, any activity incidental to financial activities, and to some extent in any activity complementary to such activities. Unless the language is clarified, commercial companies held pursuant to merchant banking and joint venturers -- perhaps even telemarketers -- could be considered affiliates. I would also note that restricting only third party sharing would tend to confer a competitive advantage on large banks, which have many affiliations, as opposed to small banks, which tend to use third parties to service customers.

Congress has embraced notice and choice -- for both affiliates and third parties -- in the Fair Credit Reporting Act. The FCRA has given consumers the right to notice and the opportunity to opt out before a company shares certain credit information with an affiliate. Financial firms have proven the practicality of notice and choice through the implementation of the FCRA. Most recently, U.S. Bancorp, in response to a suit brought by the Minnesota Attorney General, has agreed to notice and opt out before transaction and experience data can be shared with affiliates for direct marketing purposes and with unaffiliated third parties for purposes of marketing financial products or services of the unaffiliated third party. The settlement prohibits sharing information with third parties for purposes of marketing non-financial products.

Nonetheless, some have contended that customers need not have choice over information sharing because they possess the ultimate choice: the ability to take their business elsewhere. We believe that customers are less able to "vote with their feet" on financial privacy than may first appear. Changing one's bank or broker is not a simple matter. It requires a considerable investment of effort and time, as one checking account must be run off as another is created, as direct deposit orders must be reissued, as checks must be reprinted, as new codes must be memorized, as stocks must be transferred. It is a change that most of us make only when we are extremely dissatisfied with our current circumstances.

For that reason, the Administration believes that choice must be guaranteed by law. In most cases, we support the notice of "opt out" choice -- that the sharing may occur so long as the customer is given notice and the opportunity to object. In some cases, with particularly sensitive information such as medical information, an "opt in" may be appropriate. We also believe that these choices should not be circumvented by allowing a financial institution or an affiliate to do the marketing itself, on behalf of the third party.

Choice would allow consumers to make their own decisions as to the potential tradeoff between their financial privacy and the various marketing opportunities and other potential benefits of information sharing. This is a very personal decision which is most appropriately left to an individual.

Exceptions

While the Administration is firmly for choice, we also believe that there is a need for balance. There are some types of information sharing where customer choice may not be appropriate -- where allowing customers to opt out of information sharing is counterproductive or too costly. The most obvious case is sharing of information with appropriate law enforcement authorities. Another example is the sharing of information in order to facilitate the processing of individual transactions -- clearing checks, for example.

Other types of information sharing present difficult tradeoffs. In approaching any exceptions and the general policy of choice, we think three questions are appropriate:

· First, what is the consumer's reasonable expectation of privacy? This in turn largely depends on the type and sensitivity of the information. Most people expect that their checks will be processed efficiently -- even if by third parties -- but not that anyone processing the data will be able to learn how they live their lives. They also don't expect that information to be sold without their consent.

· Second, what is the purpose of the transfer? Does it directly benefit the consumer or mostly just the company? Is the company using the information to directly serve the customer, or is the company primarily using or sharing the customer's information for another purpose?

· Third, what are the costs of allowing choice? Does it significantly (i) disrupt the functioning of the enterprise, (ii) raise costs to consumers, or (iii) disrupt markets?

Any decision should be based on a balance of these factors. The Administration strongly believes that in most cases the balance counsels for choice, whether the sharing be with a third party or an affiliate. We also support strict limits on re-use of information shared pursuant to any exception, to the extent that such use exceeds the excepted use.

Perhaps the clearest case for choice is in the area of medical privacy. Although a company may have economic incentives to share medical information, no consumer expects that in consenting to a physical examination for an insurance policy, he or she is endangering an ability to obtain credit or employment. For that reason, the Administration favors strong restrictions on the ability of any company, including insurance companies, to share medical information. We strongly oppose, however, the medical privacy provisions of H.R. 10. These provisions contain significant exceptions that would, for example, allow re-use of medical information by companies with whom the information is shared, preempt state law, and allow an insurance company to ship information to other companies under the rubric of "marketing research" in circumstances that neither current practice nor future regulations would likely permit.

The provisions also would create uncertainty about the authority of the Department of Health and Human Services to establish stronger protections for customers of financial services companies. Notably, the provisions in H.R. 10 apply to "insurers," who are central to the functioning of the medical system. Such a broad scope would significantly undermine efforts to craft meaningful, comprehensive medical privacy legislation, and would erode existing protections. The Administration strongly urges that these provisions be stricken from the bill in conference.

The sale of marketing information to a third party -- or using such information on behalf of a third party -- also appears to be a clear case where no exception to notice and choice is appropriate. A consumer doing business with a financial institution would not expect the information generated through that relationship be sold for unrelated, especially non-financial, purposes. In such a case, the financial institution would be selling the information primarily for its own profit, not the customer's benefit. Due to advances in technology, maintenance of a "do not market" list has become more easily achievable.

In some cases, though, the case for an exception may be stronger. Financial services firms may wish to provide customers a consolidated account statement including accounts from different affiliates within the organization. Here, the case for an exception from "opt out" appears appropriate. Customers could reasonably expect to have their financial information presented to them in a comprehensive way; the consolidated statement is done for the convenience of the customer, who is able to correct any errors; and the cost of requiring separate mailings for each account could be considerable.

Other cases present more difficult tradeoffs. For example, with respect to risk management, one could conclude that a customer who has defaulted on one loan from a financial organization should not reasonably expect to be able to shield that information from an affiliate considering a second loan. Allowing the information to be shared protects the depository institution from loss, and should result in lower prices for creditworthy borrowers. The same also could be said of information on the timeliness of a customer's payments to the institution -- assuming that such an exception is implemented in a way that ensures that the customer receives notice that such information sharing is occurring and has access to and the ability to correct such information.

The idea that a sister bank could, however, deny a loan because a consumer's credit card reveals risk-taking *behavior* -- say, the recent purchase of a skate board or a sports car -- is far more troublesome. Thus, any information about where a consumer is spending money, or the purposes for which the consumer is obtaining credit, should remain subject to notice and opt out. How we live our lives, what we believe, the choices we make -- all of these very personal pieces of information should not be shared without our consent.

The Need for Regulatory Flexibility

Each of the issues we have just discussed is complicated, and the answers may well change as technology and business practices advance. The complexity and uncertainty of the task at hand suggest two further points.

First, we should allow many of the details to be worked out by the regulators that know the financial services industry best, after taking into account public comment. The agencies that examine financial services firms and follow industry trends should be responsible for writing and enforcing privacy rules applicable to the firms that they regulate.

Second, a transition period would be appropriate so that financial institutions can reprogram their systems to take account of customer choices.

Conclusion

Thank you for allowing me to appear today on an issue of such importance to the Administration. I welcome your questions.

Appendix to Testimony Before the Subcommittee on Financial Institutions and Consumer CreditThe Committee on Banking and Financial ServicesJuly 21, 1999

The following discussion of privacy policy issues complements the written testimony. It addresses federal government privacy policies and federal government web site privacy policies.

Government privacy policies:

The Privacy Act of 1974 establishes a set of fair information practices for the federal government's handling of personal information in systems of records. These principles include: written consent as the baseline for disclosure of personal information; notice of the specific purposes for which that information will be used; and access by individuals to their records and the ability to correct mistakes in those records. The Privacy Act does contain some exceptions, such as for certain law enforcement uses.

The Administration has no current proposals to update the Privacy Act, or the Right to Financial Privacy Act, which protects customer records maintained by certain financial institutions from improper disclosure to officials or agencies of the federal government.

This year the President established the position of the Chief Counselor for Privacy at OMB, underscoring the Administration's commitment to examining where progress can be made to improve federal government privacy policies while achieving other important government goals.

The Chief Counselor will be engaged in a "privacy dialogue" with state and local governments, as Vice President Gore announced last July 31. This dialogue will include considering the appropriate balance between the privacy of personal information collected by governments, the right of individuals to access public records, First Amendment values, and Department of Motor Vehicle information.

With respect to the IRS, the agency launched a major effort in late 1997 to eliminate unauthorized access and inspection of taxpayer records. Because the law requires the Service to terminate employees who are found to have engaged in unauthorized access, IRS focused its planning on deterring, preventing and detecting privacy violations, and on administering penalties for unauthorized access. This effort included an extensive training and education program aimed at establishing a single basic principle for all employees: do not look at, access, scan or otherwise gather information from any return or return information that you have no official need to see. IRS is constantly evaluating the success of these efforts and considering additional strategies as it learns from its experience.

Privacy on federal government web sites:

All federal agencies have web sites and every federal web site must comply with the Privacy Act. Federal agencies' web site privacy policies are diverse and are tailored to the information practices of each site. The Office of Management and Budget has provided guidance to agencies for developing their web sites. Jacob Lew, Director, Office of Management and Budget, issued a memorandum to agencies directing them to post privacy policies no later than September 1, 1999. OMB has also issued guidance on good practices for agency web sites. As of July 15, 1999, all Cabinet departments have privacy policies clearly posted on their home pages.

Treasury's web site privacy policy is conspicuously displayed as part of the home page (**www.Treas.gov**) . The Main Treasury web site does not use "cookies" (that is, a file placed on a visitor's hard drive that allows the web site to monitor the individual's use of the site) to collect information about citizens' visits to the web site. Treasury Bureaus have been notified that Main Treasury's web site should be used as a model. The Financial Management Service uses temporary cookies to maintain a connection with the user to insure the user receives a response, for example to comments, but the cookie is immediately deleted when the user leaves the site.

PERSONAL FINANCIAL INFORMATION:
DO CONSUMERS GET PRIVACY OR PIRACY?

Contents

WHAT'S WRONG WITH THE PRIVACY PROVISIONS IN H.R. 10 AND WHAT CONGRESS CAN DO TO FIX IT

Simply put, the House-passed privacy provisions in HR 10 fail to protect consumers' financial privacy. Consumers need the ability to control the sharing of their financial data – notice, access and at least the chance to say "no" to sharing financial information with *any* entity.

What's in HR 10?

- **Limited Notice Provisions:** HR 10 requires only that an institution notify consumers about their policies and practices related to "protecting" the information or disclosing to nonaffiliated third parties. There is no requirement to tell consumers about the types of information collected or the information sharing practices related to affiliates and any other entity or person.

- **Opt-Out to "Nonaffiliated Third Parties" Only**: The provision's limited third party opt-out does not apply at all to internal affiliate sharing—affiliates can still share and sell information and consumers have no ability to stop them.

- **Marketing still Permitted with Nonaffiliated Third Parties**: Even if a consumer opts-out, information may still be shared with third parties *marketing* financial products on behalf the institution or pursuant to a "joint agreement" between two or more financial institutions to offer, endorse or sponsor a financial product. Therefore, with regard to *any* financial product, the consumer has no right to stop the disclosure of their information.

- **Loopholes Galore**: A number of loopholes exist in the bill that could allow financial institutions to share a customers information without notice to the customer or allowing that customer to have the ability to opt-out.

What Can Congress do to Provide *Real* Privacy Protection?

- **Notice about Information Sharing Practices with *All Entities*:** Require institutions to provide full disclosure of their information sharing policies with all entities, including the categories of information collected and categories of persons/entities to whom the information may be shared. Consumers need to be meaningfully and fully informed about the institution's information sharing and privacy practices.

- **Opt-Out of Information Sharing with *All Entities – Affiliates and All Third Parties – for All Purposes*:** Give consumers an across the board opt-out so they could say "no" to information sharing, for any purpose, with affiliates and third parties. This is the minimum protection consumers need – anything less is sanctioning widespread information sharing and violations of consumers' privacy. Even better, financial firms should not be permitted to share or sell a consumer's financial information with any entity, affiliate or third party, without the consumer's prior consent – an "opt-in."

- **Access to Information:** HR 10 does not provide any access to data for consumers. Consumers should have access to the information institutions hold on them to ensure the information is accurate and relevant and the ability to correct erroneous information. Consumers should also be able to hold institutions that violate their privacy accountable for the violations.

- **Security and Protection of Data**: The holders of data are in the best position to protect and secure the information on consumers. Banks and other financial firms should have a duty to protect the confidentiality of customers' financial and personal information and be held legally responsible when they violate the confidentiality standards.

Why is it Important for Consumers to have the Choice to Stop information Sharing with Affiliates?

- **Harm to Consumers from Affiliate Sharing is Great:** Financial firms are interested in sharing information with and selling the products of their affiliates. Financial institutions can use affiliates to sell or market any of their products. Rather than use third parties, they will simply bring everything into the affiliate structure.

  The most glaring example of the harm from unauthorized information sharing involves affiliate sharing -- the *NationsBank* case in which *NationsBank /Securities* settled securities laws violations by paying $7 million to the SEC and other agencies. The allegations included the bank sharing lists of customers with expiring CDs with NationsSecurities. The securities *affiliate* allegedly sold uninsured, risky products in a misleading manner that were not suitable to unsuspecting CD holders. Thousands of consumers were affected, losing portions of their life savings. <u>HR 10 as passed by the House does nothing to address this affiliate sharing problem but rather, gives its okay to widespread affiliate sharing without giving consumers any ability to stop such sharing.</u>

  As Representative Barton (R-TX), who co-sponsored with Rep. Markey the stronger privacy amendment that was denied a vote by the House Rules Committee, stated on the floor during the debate over HR 10 on July 1, 1999 --

  > *The question I ask this body and this country is: If we are concerned about the selling and sharing of information to third parties, should we not be just as concerned about the selling, sharing, transmitting, or accessing that information inside of these affiliates if there are going to be dozens or hundreds of these affiliates? ... **Until we solve the riddle of handling information within the affiliate structure, we do not have privacy. We do not have privacy.***

CONSUMERS CARE ABOUT PRIVACY PROTECTION AND CONTROLLING HOW THEIR PERSONAL INFORMATION IS USED

- 80% of those surveyed agreed that "Consumers have lost all control over how personal information is circulated and used by companies."

- 88% are concerned about threats to privacy. 55% are very concerned about those threats.

From a 1998 Poll by Lou Harris.

CONSUMERS LACK CONFIDENCE THAT EXISTING LAWS ARE ADEQUATE TO PROTECT PERSONAL INFORMATION AND A MAJORITY SAY NO TO AFFILIATE SHARING OF INFORMATION

- 92% surveyed say they would mind if a company they did business with sold information about them to another company.

- 78% did not agree that current federal and state laws are strong enough to protect personal privacy from businesses that collect information about consumers.

- 81% opposed the internal sharing of customer personal and financial information by corporate affiliates.

- Only 10% said they would support newly merged banks, insurance companies and investment firms sharing customer information about accounts or insurance policies and *the majority of these said that affiliated companies should be required to notify and obtain written permission from customers before sharing their personal information.*

From a 1998 AARP Survey.

The Washington Post

AN INDEPENDENT NEWSPAPER

Whose Financial Data?

CONGRESS HAS spent so many years trying to reform the laws regulating banks and other financial institutions that it would be rash to predict success in this session. It's true that the House and Senate now agree on what was for years the most contentious issue: repealing the Depression-era ban on cross-ownership among banks, insurance companies and securities houses.

But three areas of dispute continue to jeopardize final passage. The Treasury and the Fed still disagree about what corporate structure would best guarantee that federal insurance of bank deposits isn't unwittingly extended to nonbanking activities. Then there is disagreement about the Community Redevelopment Act, which has successfully encouraged banks to lend more to poor neighborhoods. The Senate version of the bill would weaken the CRA.

The biggest controversy in the House, though, has to do with privacy. The financial institutions want to retain ownership of all the information they collect about their customers. They can profitably sell such data; they also can use it, they argue, to offer improved services. But where the financial institutions see gains for consumers, some members of Congress see risk in the sharing of information across institutional divides. A bank could let its securities affiliate know when an elderly customer's certificate of deposit was expiring, setting the customer up for exploitation with a riskier financial product. Insurance companies with knowledge of a customer's poor health could warn a mortgage affiliate not to make a loan. And so on.

The House Commerce Committee approved, with bipartisan support, a compromise solution. Financial institutions would be able to sell most information, with the exception of medical data, and share such information among affiliates. But customers would be given the right to say no—to request that their information not be shared. This "opt-out" is less sweeping than what some self-styled consumer advocates wanted—that is, no sharing without express approval from each customer. But most industry lobbyists oppose even this modest measure, and the House leadership may keep the Commerce Committee version from coming to the floor. That would be a mistake; the House should be allowed to vote on a provision that would give consumers a bit of increased protection as financial institutions bulk up.

USA TODAY 6-10-99

Banking privacy laws stir legal debate

Minnesota case tackles sale of customer info

By Christine Dugas
USA TODAY

While Congress was considering whether to tighten bank privacy laws Wednesday, Minnesota's attorney general was suing a Minneapolis-based bank for illegally selling customer information to a telemarketing firm.

Attorney General Mike Hatch says that among other things U.S. Bank violated the federal Fair Credit Reporting Act by selling private customer information, such as Social Security numbers and account balances, to Member Works of Stamford, Conn.

Hatch says the bank received $4 million plus commissions for providing information on nearly 1 million customers across the Midwest and West.

Member Works, a publicly traded company, markets various membership programs that, for example, offer consumers travel and health care discounts.

Some of the nearly 50 consumers who complained to Hatch's office said bills had appeared on their credit card statements even though they never were contacted by Member Works. Others said money was debited from checking accounts without authorization.

"We are confident that our marketing standards operate well beyond current industry practices, as well as all state and federal regulations," said Member Works spokesman Wayne Gattinella.

U.S. Bank denied it has violated any laws. "In today's world, joint ventures and cooperative marketing programs are common practices in bringing benefits to customers," said Donn Waage, public relations director at U.S. Bancorp, the parent company.

The sale of customer information goes beyond U.S. Bank. Comptroller of the Currency John Hawke Jr., who regulates banks, says his office has received calls from attorneys general in other states about privacy issues.

"We are not sure how widespread such practices are," he said. "But we are collecting the information and will be looking into it further."

"Privacy shouldn't be for sale" says Ed Mierzwinski of U.S. Public Interest F :h Group. "It's outrageous and it's also outrageous that the financial lobby is lined up against reform."

Today the House Commerce Committee votes on a privacy amendment to the financial modernization bill. The ar ment, sponsored by Rep. Edward Markey, D-Mass., would give consumers the right to say no if they didn't want their bank to share information with affiliates, and it would require the bank to get a customer's consent to share information with anyone outside the company.

WASHINGTON POST 6-17-99

Edward Markey

Your Secrets For Sale

There are few things that people value more than their privacy, especially when it comes to their personal finances. A record of the checks you write, the charges you make on your credit card, the stocks you buy, your insurance claims—they tell as much or more about you than a personal diary.

Yet this personal diary is not kept under your bed or locked in your desk. It is held by a financial institution on terms that often do not coincide with its confidential, sensitive, personal character. In fact, financial institutions benefit from obsolete laws and rules that permit this information to be shared with people without your permission and even sold to others who are not even part of the bank or securities firm with which you were doing business. Some of this can be explained as necessary for "efficiency," but much of it can only be explained as unnecessary angling for competitive advantage at the expense of personal privacy.

Shouldn't you have a say if your bank or broker wants to share your personal information with another institution? Shouldn't you be the one to decide whether your personal profile is put up for sale?

It sounds reasonable enough, but the fact is that you have very little control over the distribution of your own financial records. Current law allows financial firms to share your personal financial information without your knowledge or consent.

Concerns about financial privacy are heightened by the increase in bank mergers with insurance companies and investment firms. Once they merge, financial institutions are under no restrictions on sharing customer information from division to division.

For instance, your life insurance records could be made available to the loan officer considering your mortgage application. Or a grieving spouse could become a target for investment pitches as the financial "holding company" looks for "synergies" by sharing her insurance information with a securities affiliate.

Congress is now considering a bill to modernize the financial services industry. This is the ideal vehicle for common-sense measures to protect consumers' privacy. But right now, the bill falls short. Consumer advocates and privacy experts agree that a strong financial privacy bill should:

(1) Give customers the right to say "no" to institutions sharing personal financial information with their affiliates and prohibit any transfer of personally identifiable information to third parties without the customers consent.

(2) Give customers the right to recover their losses when a financial firm violates their privacy.

(3) Allow customers to review their personal information for accuracy, and give them the right to correct erroneous information.

During consideration of the bill by the Commerce Committee, I succeeded in adding only the right to say "no." However, commercial interests oppose even this small gain so vehemently that they are threatening to kill the entire financial services bill if this provision is retained.

I support reforming our financial services laws for the sake of leveling the competitive playing field among financial service providers. But if the cost of such reform is that we fail to close the gaping privacy peepholes now riddling our financial system, the industry can sell your secrets to anyone. The special interests will have their cake and eat our privacy too.

The writer is a Democratic representative from Massachusetts.

TOPEKA CAPITAL JOURNAL

July 25, 1999, Sunday

LENGTH: 856 words

HEADLINE: '**Jane Bryant Quinn:** Think your financial affairs private? Dont bank on it

BODY: NEW YORK -- You probably think that your bank keeps mum about your financial affairs. Think again. May be selling you down the river, to earn some extra money.

Many banks sell your confidential account information to telemarketing firms. Salespeople then call you, flogging discount dental plans, travel clubs and other products.

Monthly payments are deducted automatically from your bank account or charged to your credit card. The bank earns commissions on the sales.

Comptroller of the Currency John D. Hawke Jr. calls some of these practices "seamy, if not downright unfair and deceptive." You can try to get off the sales list (see below), but might not be able to.

When the telephone salespeople call you, what might they know? Plenty.

Besides your name, age, address and phone number, the bank might have disclosed your bank account number, Social Security number, current checking account balance, credit limit, credit score (showing how creditworthy you are), the number and type of credit cards you carry and what you owe on your credit card accounts.

A case recently brought by Minnesota Attorney General Mike Hatch against Minneapolis-based U.S. Bancorp charged that some customers had their bank accounts and credit cards debited, even though they didn't want the service.

U.S. Bancorp, which has 1,023 affiliated banks and branches, settled the case with no admission of wrongdoing. But it agreed to fines, restitution and charitable contributions of about $3 millionthe approximate amount it had earned on sales-commissions.

Theoretically, the Fair Credit Reporting Act (FCRA) limits the way some of your financial records can be used.

FCRA covers credit information, for example, your income, assets and employment history. Under the law, banks have to tell you that they might disclose this information, and give you a chance to take your name off the telemarketing lists. This is called "opting out."

Unfortunately, there is no effective way of enforcing FCRA, says Hawke, whose office regulates 2,400 national banks. The regulators don't know what the banks are doing, and few customers know they can opt out.

What's more, no federal law protects what's called "transaction and experience" information namely, the details of your bank and credit card accounts. They can be disclosed to telemarketers at will, says

Amy Friend, assistant chief counsel at the Office of the Comptroller of the Currency. So can your Social Security number. U.S. Bancorp had a deal with a telemarketer called Member Works in Stamford, Conn., which, says Hatch, has worked with 17 of the 25 largest banks. Hatch sued Member Works last week, charging deceptive practices. The company denies the charge.

As part of its settlement, U.S. Bancorp agreed to stop working with outside telemarketers selling nonfinancial products. Wells Fargo and Bank of America announced that they would do the same.

But they can still disclose your confidential account information to telemarketers selling financial products, for example, insurance and securities.

Chase Manhattan says it's revising its telemarketing policy. Bank One says it gives telemarketers only name, address and phone number.

A financial-restructuring bill in Congress would give you opt-out rights when banks sell your account information to third-party marketers who are peddling nonfinancial products, such as dental plans.

But industry lobbyists and the congressional leadership defeated attempts to give you even better protection. You'll still have no **privacy** rights, if your bank wants to give your confidential information to affiliated telemarketers or peddlers of financial products. If you don't want your account information disclosed to telemarketers, here's what to try:(1) Call your bank and get the name of the person in charge of customer relations. Write a letter, saying that you want to exercise your legal right, under FCRA, to keep your credit information from being disclosed.

Also say that you don't want your bank and credit-card account data disclosed to anyone selling financial or nonfinancial products, including the bank's own affiliates. Some banks might agree, although they don't have to. Ask the bank to acknowledge your letter.

(2) Write to the president of the bank, saying that you're shocked to learn that your bank and credit-card account information can be disclosed. The more top officials hear this, the better. Ask specifically whether the bank shares your account information with affiliated or nonaffiliated companies.

A mere **privacy** statement isn't enough. U.S. Bancorp's **privacy** statement read, "all personal information you supply to us will be considered confidential," but it sold your data just the same.

(3) Tell your senator and representative that you want an enforceable opt-out right for all telemarketers, including those affiliated with financial institutions. Unless Congress hears from the public, the industry's dollars will rule.

Jane Bryant Quinn welcomes letters on money issues and problems but cannot offer individual financial advice.

Washington Post Writers Group

LOAD-DATE: July 26, 1999

The **Dallas Morning News**

View Related Topics

June 28, 1999, Monday THIRD EDITION

SECTION: EDITORIALS; Pg. 12A; EDITORIALS

LENGTH: 448 words

HEADLINE: **Privacy** Issues;
How much customer information should be shared?

BODY:

Until recently, insurance, banking and brokerage interests pretty much have had their way on **privacy** issues in Congress' banking modernization debate.

The Senate's modernization measure that passed earlier this year didn't address whether a financial institution's banking, insurance and brokerage affiliates could share sensitive customer files. Similarly, the House Banking Committee's version tepidly mandated companies to disclose their **privacy** policies.

But the House Commerce Committee recently voted to allow customers to block companies from sharing sensitive, nonpublic financial customer information with affiliates or nonfinancial third parties for marketing purposes.

But even this provision, loudly opposed by financial institutions, has a big loophole that allows banks to use information as long as the customer hasn't instructed to the contrary. Requiring institutions to obtain prior customer approval, as is commonly the case in Europe, would offer better consumer protection.

At last, Congress has nabbed the industry's attention on **privacy,** an issue that until now had been on the edge of modernization deliberations. Mega banks and financial service firms amass a vast inventory of personal financial information that warrant more than industry promises of protection.

Customer **privacy** is no small matter, in part, because modern technology makes timely financial information extremely valuable. Many financial service companies already sell credit card and checking account information, birth dates, addresses and telephone numbers to outsiders.

Worried by the trend, Comptroller of the Currency John D. Hawke Jr. has repeatedly criticized the sale of customer information as "seamy" and legally questionable. In Minnesota, the state's attorney general is locked in a lawsuit with U.S. Bancorp, which it accuses of selling customer information to telemarketing firms in violation of the bank's own **privacy** policies. There are also allegations in the case that some telemarketers may have used credit card information to sign up customers for products and services they didn't order.

To its credit, Bank of America has promised to stop sharing certain customer information with telemarketers. Several other banks also are looking at their policies and procedures.

Reforms to end regulatory fire walls between banks, insurance companies and securities firms are long overdue. Financial institutions need additional flexibility and muscle to compete globally. Consumers, however, must regain some rights to determine how their financial histories are used, and must have reasonable assurances that confidential information will not be abused.

LANGUAGE: ENGLISH

LOAD-DATE: June 28, 1999

FOCUS™

Search: General News;Privacy, Dallas Morning News

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

Los Angeles Times

View Related Topics

June 14, 1999, Monday, Home Edition

SECTION: Metro; Part B; Page 4; No Desk

LENGTH: 493 words

HEADLINE: PRIVACY ABUSES BY BANKS

BODY:

Banks are no longer the friendly, discreet custodians of their depositors' money, judging by hundreds of thousands of consumer complaints to federal and state banking regulators. In fact, without public knowledge, banks are making millions peddling crucial information about their depositors. The abuse--especially by the large national banks--gives a new definition to bank robbery. Federal regulators have taken notice, and some states are hauling banks into court.

In California, Bank of America announced Friday that it will no longer sell customer information to third parties. Fine. But Wells Fargo and U.S. Bancorp say they will take only limited remedial steps. For the most part, other banks are silent on the issue. The best way to stop this abuse is through legislative protection of consumer **privacy.**

Financial **privacy** is under assault from all directions. The California Legislature, for instance, enacted a law to allow the state to sell personal income data, and only Gov. Gray Davis' last-minute intervention blocked its implementation. As objectionable as that law is, it at least gives taxpayers some say in the release of the information. Banks are not subject to such constraints.

In a practice that Comptroller of the Currency John D. Hawke Jr., the regulator of federally chartered banks, calls unfair and abusive, some banks regularly and without any legal restraint sell data about their customers to telemarketing companies in exchange for a commission. And it's not just names and phone numbers the banks sell. It's Social Security numbers, birth dates, credit card numbers and purchases, occupations, marital status, credit standing and account balances.

Some banks will even allow telemarketers to automatically charge the accounts of customers who express an interest in the telemarketers' products or services. Minnesota has filed a lawsuit against U.S. Bancorp over such practices, accusing the bank holding company of violating the Fair Credit Reporting Act.

The House Commerce Committee last Thursday adopted an amendment to force banks to disclose their **privacy** policies and allow consumers to block release of their personal and credit information. A much stronger provision to require banks to get their clients' consent prior to disclosure was defeated. It is essential that, if the House bill is enacted, the rules implementing it order banks to spell out their **privacy** policies clearly and conspicuously and make it as easy as possible for customers to opt out.

House enactment of an "opt-out" clause depends on whether Rep. David Dreier (R-San Dimas), chairman of the Rules Committee, will allow the Commerce Committee amendment, rather than a much weaker Banking Committee proposal, to be considered by the full House. Consumers should let Dreier know where they stand.

*

To Take Action: Rep. David Dreier, (202) 225-2305 or click on "Feedback" at the Web site http://www.house.gov/dreier.

LANGUAGE: English

LOAD-DATE: June 14, 1999

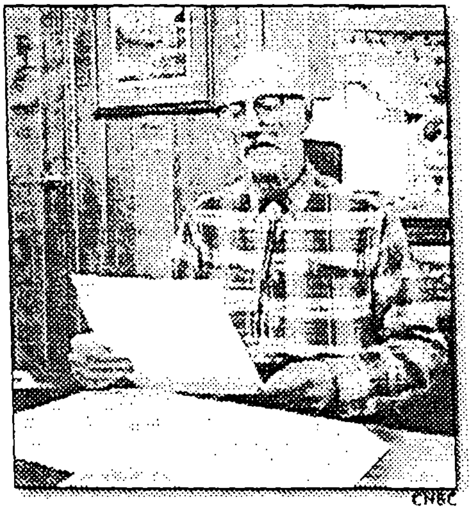
FOCUS™

Search: General News;Privacy, Los Angeles Times

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**


CNBC

Albert Newman, 79, couldn't figure out why he was getting mail from an insurance company for a policy he didn't want. But he traced it to his bank -- and is now suing for invasion of privacy.

Privacy advocates targeting banks

States eye tighter rules on how information is shared

By Sharon Epperson
CNBC

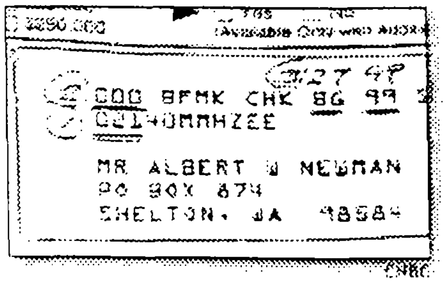
Aug. 3 — It's amazing how much personal information businesses require consumers to provide just to make a simple transaction, like rent a movie or order take out. But banks maintain a much deeper, richer trove of personal information on their customers — who probably assume it's all under lock and key. Don't bank on it.

COMPLETE STORY

'I think more onerous things kinds of things will occur in the future if we don't nip it in the bud now.'
— **CHRISTINE GREGOIRE**
Attorney General, Washington state

YOU MAY THINK your personal information is private. But banks know how much you make, what you spend it on, your Social Security number, your credit history. Things that even your friends and family don't know about, your bank does. And it may be sharing that knowledge with others.

"I was dumbfounded, disgusted, upset," said 79-year old Albert Newman, who, like many consumers, was unaware that his bank could give out his personal financial information. Five years ago, Newman started receiving mailings from an insurance company for a policy he didn't want. At first, he had no clue how the company got his name or address.



Newman used his cryptography experience to decode a mailing label -- and found it matched his checking account number.

But then Newman, a cryptographer in World War II, put those skills to work. He decoded the digits on the upper right hand corner of the insurance pitch — and discovered it was his checking account number.

"The cat was out of the bag," said Newman.

Newman is now suing Washington state's Heritage Bank for breach of contract, invasion of privacy and violation of the Consumer Protection Act. He says he wants the bank to "admit that they're doing something that the average individual doesn't understand or know about."

Heritage Bank officials denied selling any information to marketing firms but admit sharing "confidential and private information" with some financial service providers.

Right now, it is only illegal for a bank to sell someone's credit report to a third party like a direct marketer. But any other information can be fair game. Newman's attorney says until laws are changed, the scales of justice are tipped in the banks' favor.

"We have asked the attorney general's office to change the Consumer Protection Act to provide that disclosure of private financial information would be a per se violation," said public interest attorney Shawn Newman (who is no relation to his client).

Washington state Attorney General Christine Gregoire agrees that swift action needs to be taken.

"I think more onerous kinds of things will occur in the future if we don't nip it in the bud now," she said.

What you can do

Privacy experts says there are a few things you can do to keep private information private:

If you order a catalog or magazine, ask the company not to sell your name.

If your name has already been sold, ask for the list of businesses or charities that bought it and ask them to put you on their "do not mail" lists.

To remove your name from marketers' mailing lists, write to the Direct Marketing Association's Mail Preeference Service, Box 9008, Farmingdale, N.Y., 117835-9008

For phone lists, write to the DMA's Telephone Preference Service, PO Box 9014, Farmingdale, N.Y. 11785-9014

Write to credit reporting agencies and ask to "opt out" of the pre-approved credit lists they sell to companies Or call 888-567-8688.

A rash of consumer complaints compelled the Attorney General to create a new privacy task force.

"This is an issue that effects every single citizen of this country; the right for them to have their information protected," said Gregoire. "And the right for them not to allow someone to sell for commercial purposes their personal, private information without their consent."

Gregoire played a pivotal role in the recent successful fight of various state attorneys general against the tobacco industry. She says this battle is even bigger.

"This issue has a more far reaching potential problem for consumers and has caused much greater fear for consumers than any other case that I have dealt with," she said.

TAKING ACTION

The state of Washington is not alone in its fight to protect consumers' privacy. Government officials across the country are investigating banks' practices, and one state has already taken legal action.

U.S. Bancorp recently paid $3 million to settle a lawsuit waged by Minnesota's attorney general. The suit alleged that the bank released customer information to a telemarketing company for $4 million, plus commissions.

The bank said it would stop disclosing consumer information to most marketers, except those that sell financial products. Soon after, other banks, including Chase Manhattan and Wells Fargo, imposed similar restrictions.

The suit has heated up the debate at a time when Congress is divided over whether to add privacy provisions to banking legislation.

"What I have proposed is that we complete our hearings on privacy, do some in-depth study and write a financial privacy bill," said Sen. Phil Gramm (R-Texas).

BREAKING BARRIERS

But some fear that current proposals, like Gramm's financial modernization bill, will break down barriers between banks and other financial services firms — making it easier for them to share information.

Consumer advocates worry that in the era of mega-mergers like the Citibank-Travelers deal, a bank could, for example, deny a mortgage loan if it learned from its insurance affiliate that the customer was seriously ill.

But the banking industry maintains that such sharing of information can be an asset.

"Consumers actually benefit in the way of lower prices and greater convenience when limited information is shared about them within a bank's family," said Sonia Barbara, with the consumer's division of the American Bankers Association.

But if consumers don't see the benefit, the industry's trade group says they should let their bank know.

So that's what Albert Newman is doing. He has refused to settle his case; he wants his message heard loud and clear.

"There's no one with the temerity to say, 'Let's go get em.' I'll do that," he said.

Many banks claim customers can simply write to request their names be taken off any sales lists. But consumers groups suggest banks adopt "opt-in" provisions, in which customers would only receive outside materials if they opted to be included on these lists.

MORE LINKS
MSNBC not responsible for content of Internet links
INTERNET Direct Marketing Association

TOP BUSINESS NEWS

STORY Microsoft-AOL war heats up over plans for Internet access
STORY U.K. leaves rates at 22-year low
STORY Cardinal Health in $390 million deal
STORY Free PCs: a win-win or a win-lose?
STORY Just how low can Internet stocks go?

MSNBC VIEWER'S TOP 10

Would you recommend this story to other viewers?
not at all 1 - 2 - 3 - 4 - 5 - 6 - 7 highly

Cover | Quick News | News | Business | Sports | Local | Technology | Living & Travel | Health
TV News | Opinions | Weather | Shopping | MSN | Comics | Find | About MSNBC | Help | Index
Cool Tools | Jobs | Write Us | Advertising on MSNBC | Terms, Conditions, and Privacy

TOC: More Stories from this May 1999 issue

Latest Issue Online

Archives & Back Issues

Themes & Sections

Search Fast Company

"This is a Marketing Revolution"

by Charles Fishman
Photographs by Peter Ross

first appeared: Fast Company issue 24 page 204

Capital One is winning big in the cutthroat world of credit cards by changing the rules. Its mission: Deliver the right product, at the right price, to the right customer, at the right time. Its method: Never stop testing, learning, or innovating.

The telephones at Capital One Financial Corp. ring more than one million times a week. People call to ask about their MasterCard balance, or whether a recent payment was received, or why their interest rate has jumped. And more than 1 million times a week, here's what happens -- before a caller hears the first ring:

The instant the last digit is punched, high-speed computers swing into action. Loaded with background information on one in seven U.S. households and with exhaustive data about how the company's millions of customers behave, the computers identify who is calling and predict the reason for the call. After reviewing 50 options for whom to notify, the computers pick the best option for each situation. The computers also pull and pass along about two dozen pieces of information about the person who is calling. They even predict what the caller might want to buy -- even though he or she isn't calling to buy anything -- and then they prepare the customer-service rep to sell that item, once the original reason for the call has been addressed.

All of these steps -- the incoming call, the data review, the analysis, the routing, and the recommending -- happen in just 100 milliseconds. That's one-tenth of a second, or one-eighth of the time that elapses between beats of a human heart.

Make no mistake: Capital One has some wicked-fast computers. And its growth rate has been nearly as fast. The company took shape in 1994, when it began as a spin-off of Signet Banking Corp. It now ranks among the 10 largest issuers of credit cards in the United States, with 16.7 million customers (it added 5 million new accounts last year alone) and total balances of $17.4 billion. Its stock chart looks more like that of an Internet startup than like that of a bank. Stock in the company, which was first offered at $16 per share, has traded as high as $140. The company, with 11,000 employees, has a market value of more than $7.8 billion.

Capital One's cofounders -- a pair of buddies with no previous hands-on experience in the banking industry -- had rocked the credit-card world while they were at Signet, where they had invented the "teaser rate" card and the "balance transfer" option. Those two innovations sucked millions of customers away from established companies, and the two men brought them over to their own company. The real secret of Capital One's success, though, has been its commitment to endless innovation. Lots of companies claim that they compete on knowledge. Capital One has enough information on consumers to fill the hard drives of more than 200,000 personal computers. It uses that information much as a physicist uses a particle accelerator: Cap One analysts and product managers come up with an idea for a product, bounce the data a bit, test it, tweak it, and launch it as fast as possible. In other words, they use the scientific method to design credit cards.

"Credit cards aren't banking -- they're information," declares Rich Fairbank, 48, chairman and CEO, whose father is a physicist. "When we started this company, we saw two revolutionary opportunities: We could use scientific methodology to help us make decisions, and we could use information technology to help us provide mass customization."

Says Nigel Morris, 40, Cap One's president and Fairbank's alter ego: "Very few companies have the ability to test and learn." But those twin capabilities -- testing and learning -- form the foundation on which Capital One is built. The company tests every product offering, every procedural change, every job applicant. It keeps records on every customer interaction and on every card purchase, and, with the patience and persistence of a good scientist, it runs experiment after experiment. "For every action we've taken," says Jim Donehey, 50, Capital One's chief information officer, "we know what the reaction has been. If we sent out a blue envelope and a white envelope, we know which envelope went to which customer -- and we've recorded what the reaction was in each case."

For example, Capital One started selling things (insurance, long-distance service, buying-club memberships) to customers who called -- after tests showed that people prefer to buy things when they call Capital One, rather than when Capital One calls them. Today half of all new Cap One customers buy something (other than a credit card) within their first year as a customer.

Last year, the company performed 28,000 experiments -- 28,000 tests of new products, new advertising approaches, new markets, new business models. As a result, it can deliver the right product, at the right price, to the right customer, at the right time. It offers 6,000 kinds of credit cards, each with slightly different terms, requirements, and benefits, and each requiring a slightly different monthly statement. Some credit-card holders have a no-fee Mercedes-Benz affinity card with a credit line of $20,000. Others pay $29 a year for a card with just $200 worth of credit. Some have a credit card with a Canadian moose on it. Others have a card with a map of Japan and an image of Mt. Fuji on it. One reason why Cap One has attracted millions of customers is that it's able to present itself a little differently to each of those customers.

"What we've done," says Fairbank, "is to create an innovation machine." That machine has just begun to kick into gear. "This is not just a credit-card strategy," Fairbank insists. "This is a marketing revolution that can be applied to many businesses."

For Fairbank and Morris, the credit-card business has been a grand experiment in using information technology to figure out what people want to buy and how Capital One can sell it to them. Says Jory Berson, 28, vice president of marketing and analysis at Cap One: "I want us to become the place where people go to find anything they want to buy."

"We can answer your question before you ask it."

Joe from Florida is a tough call -- a confused older man, the holder of a MasterCard with a $100 credit limit. He informs his phone rep, Tim Gorman, 29, that he knows what happened the last time he called Capital One: "I've got it written on the wall right next to the phone," he says.

Nancy from North Carolina is easier. A moment after her voice materializes in Gorman's earpiece, information about her credit card pops up on his computer. Nancy is a desirable customer: She has a $6,500 credit limit on her Visa, she's been a Capital One customer for four years, she pays no annual fee, and she hasn't paid late in the past 12 months.

Her opening line: "I want to close my account."

Gorman is used to that greeting. He works as a Capital One "retention specialist," and all of the calls routed to him are from people who say they want to close their account.

Gorman knows better. Most of them just want a better deal.

"I just got a card with a 9.9% interest rate," says Nancy, "and that's a lot lower than my current rate."

Nancy's current rate is 16.9%. Gorman's computer displays three counteroffers that he can make in an effort to keep her business. Those offers have different interest rates -- starting with 12.9% and ramping down to 9.9%.

"Well, ma'am, I could lower your rate to 12.9% . . ."

Nancy grabs the first deal that Gorman offers, and Gorman scores a "save." Is he concerned that Nancy didn't get the best deal available? Not really. "Who's to say she really was offered a 9.9% card?" he says. "Maybe that was just something that she saw or something that came in the mail." Nancy is happy, Capital One is happy, and Gorman has earned incentive pay for keeping her -- plus a little extra for getting her to take a deal that preserves much of Capital One's revenue.

Superficially, Gorman's exchange with Nancy sounds like what happens at credit-card companies everywhere. It's standard these days for account information to pop up when a call comes in (computers identify the account by linking it to a phone number), and many companies bargain over interest rates and fees. But at Capital One, that's where the interaction begins, not where it ends. The history of "intelligent call routing" (a term that Capital One coined) -- with its tiers of computer-enabled decision making -- is a case study in how a culture of innovation can take small problems or modest ideas and turn them into breakthroughs.

In this case, the problem had to do with the phone bill. Two years ago, calls from Capital One customers were taking too long to handle, and an analysis showed that customers were not to blame. Callers simply weren't getting to the right place at the right moment: People with a lost card or a fraud problem ended up reaching an ordinary rep; people who just wanted to know their balance stayed on hold to talk to a live rep; people unhappy with their interest rate called the "lost card" number on the back of their card and had to be transferred to customer service.

"All that time -- to take a call, to bridge the call to the right person -- that pisses off the customer," says Greg Gannon, 44, a technology manager who was brought in to look at the problem. "You wait for an agent, you wait for a transfer, you wait again for an agent."

Plus, says Jim Donehey, "All that time, we're paying for the call." Companies pay by the second, and at a place like Capital One, which takes 2.5 million live calls a month, even one extra second per call adds up to real money. "The real question was, How can we minimize all that?" says Donehey.

The company tried lots of options. For example, it discovered that some people called much more often than the average of five times a year. "We sent out a letter at one point that said, in effect, 'Please don't call so much,' " says Donehey. That test yielded this result: If you want people to call you, send them a letter telling them not to. "That was what I call 'a Homer Simpson moment.' "

The ultimate solution -- suggested by the technology folks -- had less to do with an animated character than with artificial intelligence: Why not predict the reason for each call and then send that call to the agent who is best able to handle it? In fact, a company like Capital One, with 3,000 people answering calls, knows plenty about why customers reach for the phone: Ninety percent of all calls fall into 1 of 10 categories. Raise your customers' interest rate, and they call. Put an automatic fraud stop on their card, and they call. Send out a new card that needs to be activated, and they call. Some people call once a month to find out their balance; some people call three times a month.

It took months to analyze these calling patterns, to figure out which events in a customer's credit-card life would predict a call. Decision-tree software had to be written, equipment had to be bought, phone switches and computers had to be taught to talk to each other. Along the way, people working on the project arrived at some powerful insights. For example, customers who call each month to check their balance or to see whether their payment has arrived could be identified and routed to an automated system that answers the phone this way: "The amount now due on your account is $364.27. If you have a billing question, press 1. . . . " Or: "Your last payment was received on February 9. If you need to speak with a customer-service representative, press 1. . . . " The genius of this system, says Donehey, is that "we can answer your question before you ask it." A phone call that might have taken 20 or 30 seconds, or even a minute, now lasts just 10 seconds. Everyone wins.

A routine problem in search of a quick solution led to a new way of doing business. Today customers get where they are going immediately, and they get the information that they need quickly. Customer-service reps handle those calls that need to be handled by people, and they don't waste any time passing calls to colleagues. For example, customers who have received prototype products are automatically routed to staffers who know about those products.

This calling system has become a competitive advantage for Capital One, making possible both lower costs and better service, and the company is understandably reluctant to share specific performance data about it. But a few round figures are available: The system went into effect last June, and, says Donehey, "Within a few months, it was right 40% of the time." Gannon says the prediction-success rate is now at 60% to 70%.

And the system just keeps getting smarter. Do you routinely call from your boyfriend's phone -- the number for which is not on file at Capital One? Eventually the computer will figure out that his number should be associated with your account. If you call to close your account, you'll encounter a subtle measure of what Cap One thinks of your business -- because the system will do a real-time analysis of your value as a customer. People worth keeping are routed to a live agent like Tim Gorman. People whom Capital One is not unhappy to be rid of are routed to a voice-response unit and allowed to close their account using their Touch-Tone phone. Meanwhile, more capabilities are in development. For example: The system will learn what language each customer prefers to do business in and then route calls accordingly.

"This started as such a simple problem," says Donehey, "but IT enabled us to go back to the business side with a solution that went beyond solving that problem. The flow of information between IT and the business side and the customer is constant. A lot of the stuff that really makes our technology work has nothing to do with technology -- it has to do with attitude."

"Every interaction is a selling opportunity."

Larry from Pennsylvania is on the line, baffled by his new Capital One "Silver" Visa, with its $1,000 limit and its $59 annual fee. The card comes with coupons offering discounts on hotels and rental cars, but Larry can't figure out how they work.

Barbara Brannon, 57, a veteran customer-service rep and one of Cap One's telephone stars, talks to Larry as if she has nothing else to do. She concedes that the Silver Visa carries a fee that's $20 higher than that of Larry's former card, a regular Visa. But, she says, "you can get that back with a single discount at a single hotel."

Once Brannon has helped Larry understand his new card, she says, "Sir, do you do any catalog shopping?"

"No."

"Are you interested in any kind of interior-design shopping?"

"Catalogs?" Larry asks.

"It's like the Silver Visa," says Brannon. "It's a service that we offer -- Capital One Interiors. It's a catalog with a lot of coupons. If you order it, you'll pay for it by the second or third time you use it."

"Thanks just the same," says a suddenly lucid Larry. "I get enough junk mail already."

Brannon is a star -- not just because she understands how to handle routine credit-card confusion, but because she is an unerring saleswoman as well. After all, why not try to sell a guy who is confused about coupons more coupons?

On a typical day, Brannon sells something to roughly 15% of the customers who are routed to her. Using an analysis of each customer's buying habits and demographics, her computer terminal automatically tells her which products to offer. Whether Brannon makes an offer on a particular call is up to her. With customers who are particularly upset or who are being transferred to another department, she doesn't. On this winter evening, though, she's scoring a sale with one out of every three callers. "I don't shove it down their throats," says Brannon. "I throw it out if it's something that I think they might like."

A woman from Miami, who has called to find out if she has to pay her $39 annual fee every year, cheerfully signs up to pay $59.95 a year for Privacy Guard, a service that helps you check your credit report. "That's called a sale!" says Brannon. "That's called fattening your paycheck. Give me more calls!"

Esther from Connecticut, who had called to check her current interest rate, signs up to pay $59.99 for Capital One Edge, a program in which you receive a catalog of discounted merchandise as often as 12 times a year.

Carolyn from Illinois, whose credit history has won her a Visa with a $200 limit and a $59 annual fee, calls to find out how to get a cash advance. After answering that question, Brannon warns Carolyn that her Visa has less than $100 of credit available. Then she offers Privacy Guard to Carolyn. The cost: $59.95. "If you want to get your credit report, this is the way to do it," Brannon says. "This is what you need." (Actually, if your Visa has a $200 limit and a $59 annual fee, you don't really need a credit report.) Says Carolyn: "Yes, I would like to try that."

No one at Capital One can recall whose idea it was to sell things to customers when they call the company, rather than the other way around. Most credit-card companies, including Capital One, have long tried to "cross-sell" their customers -- often by using inserts in monthly statements to tout everything from calculators to cruises.

The idea to add a new twist came, naturally, through data analysis. "It happened three or four years ago," says Nigel Morris. "We were doing outbound telemarketing, calling at dinner time, and we looked at the statistics on who bought things, who told us to get lost, and who bought things that they never used. We thought, 'This isn't working that well. What if we talk to people when they call us?' "

For Morris, a transplanted Brit who vibrates with energy and who has a mischievously contrarian streak, it seemed like a natural: "Gosh, if you call me and I'm trying to sell you something, then I'm going to treat you very nicely. That's going to promote better service. But people said, 'Service people are not salespeople. The systems don't exist to do this -- to service people and sell them at the same time. And anyway, even if you could do it,' they said, 'you would never sell enough to make the longer phone calls worthwhile.' People said it couldn't be done. That's all the motivation we needed."

In the case of inbound cross-selling, the first test product was easy and sweet. New customers must call an automated line to activate their card. "We thought, 'That's the perfect time to sell them something,' " says Jory Berson, who is in charge of cross-sell opportunities at Capital One. "The first thing we sold was a balance transfer: 'Now that you've got our card, is there any debt that you want to transfer to us?' " While customers waited on the line for a computer to verify and activate their card, they could sign up to move balances from other cards onto their new account.

Customers loved it. Or, at least, they bought it.

The response was so enthusiastic, relative to Cap One's effort, that Berson began looking for other products that Capital One could sell in this way. "I don't have a big desire to sell you groceries, because once I have to ship stuff, I can't save you any money," he says. "But auto insurance -- I can sell that cheaper. Mortgages, long-distance service, auto loans, cellular service -- same thing."

Berson sat down with his partners -- Eric Nelson, 30, Cap One's IT director, and Marge Connelly, 37, who runs all of the company's call centers. At their first meeting, in the wake of the balance-transfer experiment, "the brainstorming was less about 'Is this a good idea?' than about 'How do we do it as quickly as possible?' We weren't trying to pretend that this is rocket science," says Berson.

Indeed, the biggest hurdles were human. "At first blush," says Connelly, "folks look at the idea of selling to someone who's calling, and they say, 'There's a conflict between servicing and selling.' Some associates said, 'I don't feel good about making this offer to customers.' We were listening, trying to appreciate that feeling."

The solution, says Connelly, was "to elevate this beyond the immediate transaction level. If I'm a phone associate, my mission is to meet my customer's needs. And people have a pretty wide range of needs. If I've got this great product, it might save a customer some money, or it might create convenience. If I'm committed to service, there's no way I'm not going to consider offering that product."

Within three months of that first brainstorming session, live reps started fielding calls during which they both serviced and sold. Today Cap One does almost every cross-selling effort in partnership with another company. It makes a deal to market a product: The Hartford provides the insurance, MCI provides the long-distance service, Damark International provides the catalog clubs.

"The creativity comes in how we do that," says Rich Fairbank. "We do three things that other companies in the industry don't do. First. every interaction is a selling opportunity -- although I don't want to give the impression that we can't wait to get through your problem before we try to sell you something. Second. it's done in an information-based way: What's sold and how it's sold are decided statistically, according to information that we have. And third, we are totally committed to selling products that are of very high value. I say this with passion, because it's easy for companies to trap themselves into selling low-value things."

(For his part, Jory Berson says that he "feels better" about the auto-insurance offering, the mortgage deal, and the long-distance service than he does about Privacy Guard or about the catalog memberships. But even the latter. he says, "are presented fairly, at a fair price -- usually a lower price than other issuers offer.")

What ultimately kicked Cap One's cross-selling into high gear was Greg Gannon's intelligent call-routing system. It was a perfect fit: The same computer that predicts why you're calling can also predict what product you might want to buy. In fact, where your call gets sent often has as much to do with what Cap One wants to sell you as it does with how you will get your question answered.

Customers who are judged most likely to buy are sent by the computer to Cap One's most skilled sellers -- to Barbara Brannon's group. Every one of the three dozen non-credit-card products that Capital One offers has a statistical model behind it that outlines which kinds of customers will find it most appealing, and under what circumstances. A specific "product offer" comes to a customer-service rep in the same data burst as a caller's account information. So the decision about what to offer is made the instant someone calls. "It's got to be real-time," says Berson. "If normally I'd sell you long distance, but you're calling because you lost your card, I'd be a fool not to sell you credit-card registration."

Capital One doesn't reveal how much of its revenue or profit comes from non-credit-card sources. "It's a huge part of our business," says Berson. "We now make more than 1 million sales in a year through customer-service marketing -- not including inserts, or telemarketing, or automated calls." Those sales occur during the 30 million live calls that Capital One handles each year. In 1998, for the first time, half of all new Cap One customers bought another product from the company within 12 months of signing up for their credit card. "That's amazing penetration," says Berson, "and it leads to tremendous profitability."

"A cell-phone is just a credit card with an antenna."

When is a credit-card company not a credit-card company? That's the question now facing Capital One. If the company can serve its customers faster and smarter than its competitors can, if it can sell products unrelated to credit cards, then why continue to think of itself as a credit-card company at all?

According to cofounders Fairbank and Morris, Capital One's real capital resides in the hundreds of terabytes of data that the company has collected on the behavior of current and potential customers, and in the vast testing experience of its analysts, who know how to figure out what really matters to (and about) those customers. The company's knowledge base positions Capital One to tackle all kinds of other information-rich businesses.

Already, a Capital One subsidiary, America One, is selling cell-phone service in much the same way that the mother company offers credit cards -- by offering a slightly different deal to each type of customer. (Quips Morris: "A cell-phone is just a credit card with an antenna.") Cap One doesn't confuse its customers with choices. Instead, it tries to figure out what its customers will want. "Our secret," says Fairbank, "is that we are trying to deliver very simple solutions to the customer."

Fairbank claims that within two or three years, most people will know Capital One for reasons other than its credit-card business. "Fifty percent of what we're marketing now did not exist at this company six months ago," he says. "And 95% of what we're marketing today didn't exist two years ago. I'm proud of that fact -- until I reflect on its implications. It means that 50% of what we'll be selling six months from now doesn't exist yet."

Says Jory Berson: "We're becoming a company that people can turn to for just about anything. When you get ready to buy a car, the first thing I want to go through your mind is, What kind of deal can Capital One get me on an auto loan or on auto insurance?"

What about the car itself? "Oh, sure," he says. "A car-buying service is on my list."

Sidebar: What's the Hard Part? Innovation Never Ends

Capital One scored some early victories in the credit-card game by changing the rules. Its founders invented the "teaser rate" -- the banking equivalent of a cheap mortgage that gets adjusted up after a certain period. The teaser attracted millions of customers, and eventually competitors began to mimic the idea. The result was a merry-go-round of so-called teaser hoppers. People would move their balance to a low-introductory-rate card; as soon as the rate expired, they would switch to another card. Over time, Cap One was being eaten alive because of customer attrition.

The lesson: Companies that thrive on change can never rest. Competitors are quick to copy good ideas. The way to compete on innovation is to keep innovating.

That's the hard part. And that's why Capital One is so obsessed with making its own innovations obsolete. Consider the teaser rate. "Customers have gotten smarter about this game," says Dan Friedman, 29, a credit-card product manager. "But customers don't want to play it." What do they want? People want a simple card with a good rate, says Friedman. So, for two and a half years, Friedman's team offered prototype no-fee, fixed-rate cards to a wide spectrum of Americans. The cards had slightly different rates, slightly different credit limits, slightly different terms: "We were doing at least a dozen tests each quarter."

The team absorbed data about which rates appealed to which kinds of customers, about how customers used the new cards, and about which set of factors produced the most profitable card. "We found a rate at which we got good loyalty and low attrition," says Friedman. "That's what we wanted." There was just one problem: The card wasn't profitable.

"That is where smart people come into play," says Friedman. Two of Friedman's analysts concluded that they needed to attract customers who were better credit risks -- in other words, people who defaulted less often. "They suggested different underwriting standards. As soon as we had that hypothesis, we could test it with data that we already had."

The result of all this experimentation: Early in 1998, Capital One began offering a permanent, fixed-rate card to a select group of customers. The card has a fixed annual rate of 9.9% and no annual fee. The company that changed the game with the teaser rate is changing it again. Today, in fact, Cap One doesn't even offer a teaser-rate card to new customers.

Sidebar: Testing, Testing

At Capital One, the essence of innovation is experimentation. Every idea for a new product starts with a test, or a series of tests. If a test succeeds, the company ramps up fast.

Each test offer is handled by a small group of reps, whose opinions about the products are also taken into account. Cap One tracks not only whether people buy something but also whether they use it. The company has shelved products that customers didn't buy or didn't use. Selling software didn't work. Neither did selling mutual funds (although plans are under way to launch another mutual-funds sales program). Behind every test is a three-person team: someone from marketing, someone from operations, someone from IT. There are no silos at Capital One. Each business unit has a "business information officer" who is responsible for making technology work in that unit.

Testing doesn't apply only to products. Cap One hired more than 100 people a week in 1998, but it doesn't conduct anything resembling routine job interviews. Instead, applicants take tests, sit through guided interviews, and do role-playing exercises. In the case of customer-service reps, supervisors never even meet candidates; they meet only the people who get hired. "We found out that interviews by line managers didn't predict job performance at all," says Dennis Liberson, 43, the company's HR chief. That discovery was made, of course, through follow-up testing -- through comparing actual performance of employees with what their supervisors had predicted when they were first hired.

This year, 1,000 of Capital One's 11,000 employees will sit down to take tests. HR has developed 10 new pre-employment tests, and it wants to see how good they are. It will administer those tests to selected current employees, who will in turn have their job performance evaluated. Test results will then be anonymously correlated with how well those employees do their work. "We think these tests will predict certain competencies," says Liberson. "But before we start using them, we want to make sure."

In other words, the testers have a new test that they need to test. The company's testing culture is so deeply intricate, so wound around itself, that a senior executive recently pointed to an M.C. Escher print in his office -- a print of people climbing or descending a series of interlocking staircases -- and laughed: "That's our organizational chart."

Capital One sometimes thinks so hard about what it does -- and tests its ideas so thoroughly -- that the whole system can make an outsider's head hurt. But most people at Capital One will tell you that testing does not give them a headache: Rather, it opens their minds to new ideas. "Testing," declares Wendy Alexander, 29, international product manager, "liberates you from conventional thinking."

Charles Fishman (cnfish@mindspring.com), a Fast Company contributing editor, is based in Raleigh, North Carolina. He scored 40 out of 40 on Capital One's management-screening test. Even so, the company rejected his application for a no-fee, 9.9% MasterCard. Visit Capital One Financial Corp. on the Web (http://www.capitalone.com).

Privacy Policy of Top Ten Banks (by assets) posted on Web Site

Privacy 🔒 or **Piracy** ☠ **?**

	Opt-Out: Companies *can* disclose unless Consumers say *No*			Opt-In: Companies *cannot* Disclose unless Consumers say *Yes*	
	Affiliate Sharing		Third Party Sharing	Affiliate Sharing	Third party Sharing
	Only Credit Report Information (FCRA required)**	All Financial Data			
NationsBank	🔒	☠	🔒✓	☠	☠
Citibank	☠	☠	🔒✓	☠	☠
Chase Manhattan	☠	☠	☠	☠	☠
Bank of America	🔒	☠	🔒✓	☠	☠
First Union	🔒	☠	☠	☠	☠
Morgan Guaranty Trust	No Privacy Policy Available				
Bankers Trust	No Privacy Policy Available				
Wells Fargo	🔒	☠	🔒✓	☠	☠
Fleet	☠	☠	☠	☠	☠
First Nat'l Bank of Chicago (BankOne)	☠	☠	☠	☠	☠

KEY:

🔒 Provides privacy policy listed

🔒✓ Limited privacy policy, e.g., only opt-out on marketing lists

☠ Does not disclose or provide privacy policy listed on web site; may, however, have additional policy in mailings to customers

** Opt-out for credit information is consistent with that required under the Fair Credit Reporting Act

Consumers Union & US Public Interest Research Group (US PIRG) – June 1999

Use and Sharing of Information outside Our Affiliated Family of Banks and Companies

We maintain procedures designed to protect confidential information about you (and your products and services with us). Other than under the limited exceptions explained in this brochure, it is our practice not to share confidential customer information outside our affiliated family of banks and companies. You do not need to request this confidentiality – it is our standard practice.

The limited exceptions under which we share confidential customer information with parties outside our affiliated family of banks and companies apply only when we are *legally required* to share this information or when we are *legally permitted* to share this information to serve your interests or to address legitimate business concerns. (See Question and Answer #6 below.)

QUESTIONS AND ANSWERS ABOUT OUR USE OF INFORMATION

OUR INFORMATION ABOUT YOU

Question #1: *Why do you want to know about me?*

Answer #1: One of the main reasons we gather information about you is to protect you. We need to be able to identify you and your products and services to prevent access to personal and financial information by unauthorized persons.

We also gather information to help us understand your financial needs and provide you with quality products and services. For example, if we know you own your home, we know that a home equity loan may be a better alternative than an installment loan to finance your next purchase – because of possible tax benefits.

In some cases, we also gather information to help us design or improve our products and services. For example, information obtained from customers can tell us whether to develop a new type of home mortgage or checking account. This type of information enables us to identify the needs of customers and provide services to meet those needs.

Finally, we also gather information to comply with laws and regulations that govern the financial services industries. For example, federal regulations require that we obtain a social security number or tax identification number for many types of accounts, such as bank deposit accounts that pay interest.

WELLS FARGO

USE AND SHARING OF INFORMATION WITHIN OUR AFFILIATED FAMILY OF BANKS AND COMPANIES

Question #2: *How do I benefit when you share information about me and my products and services with you within your affiliated family of banks and companies?*

Answer #2: We provide products and services to customers through a number of separate banks and companies. By allowing our affiliated banks and companies to share information about you and your products and services with each other, you enable us to serve your total financial needs. You may receive our combined bank/company account statements, easier access to certain account features, new or enhanced products, special promotional offers, and certain discounts that you might not otherwise know about or be eligible to receive.

Question #3: *If I request to be excluded from affiliate sharing of information as explained in the front cover, will all of your affiliated banks and companies honor this request?*

Answer #3: When we process your request, all of our affiliated banks and companies will honor your request, although certain information about you and your products and services with us still may be shared (as explained in Questions and Answers #4 and #5 below). You cannot selectively request to be excluded on a company-by-company basis or product-by-product basis.

Question #4: *If I request to be excluded from affiliate sharing of information, what information about me and my products and services with you will and will not be shared within your affiliated family of banks and companies?*

Answer #4: This is a complex question because the Fair Credit Reporting Act and certain other laws permit you to direct us not to share *certain* information within our affiliated family – but these laws also permit us to share certain *other* information within our affiliated family. Even if you "request to be excluded from affiliate sharing of information," we will share this *other* information about you and your products and services with each other to the extent permitted by law, as discussed below.

Fair Credit Reporting Act

The Fair Credit Reporting Act is the primary law that covers information sharing within our affiliated family of banks and companies. This Act permits our affiliated banks and companies to share with each other the following types of information: identification information about you; information about your transactions with any of our affiliated banks and companies; and information about the experiences of any of our affiliated banks and companies with you.

Except for this identification, transactional, and experiential information, when you request to be excluded from affiliate sharing of information in accordance with the procedures set out in the front cover of this Use of Information brochure, we cannot share information about you and your products and services with us from your applications or agreements, from credit reporting agencies, or from other sources when the communication of this information would be classified as a "consumer report" under the Fair Credit Reporting Act. The Fair Credit Reporting Act, however, does not prohibit us from sharing this information within our affiliated family of banks and companies in other circumstances.

Other Restrictive Laws

Other laws and rulings also regulate our ability to share *certain* information within our affiliated family of banks and companies in particular circumstances or to offer you products and services in particular cases. Some laws, for example, prohibit us from sharing certain information within our affiliated family of banks and companies without your express written or oral consent or, in a few cases, under any circumstances. Whether or not you have provided us with a "request to be excluded from affiliate sharing of information," of course, we abide by these laws.

Question #5: *Can you provide me with a few examples of information that still may be shared within your affiliated family of banks and companies if I request to be excluded from affiliate sharing of information?*

Answer #5: In virtually all cases, we can share identification information about you, such as your name and address. In most cases, we also can share information about your transactions or experiences with any of our affiliated banks and companies, such as your loan repayment or checking account history, as permitted under the Fair Credit Reporting Act.

When we service your accounts, we can share a great deal of additional information solely for that purpose. Some of our affiliated banks and companies, for example, share or receive information to provide technical or operational support services – such as to prepare your account statements or provide data processing services for other affiliated banks and companies.

USE AND SHARING OF INFORMATION OUTSIDE OUR AFFILIATED FAMILY OF BANKS AND COMPANIES

Question #6: *Under what circumstances do you provide information to parties outside your affiliated banks and companies?*

Answer #6: Although we are committed to protecting our confidential information about you and your products and services with us, occasionally it is necessary to provide some of this information to parties outside our affiliated banks and companies.

We are required, for example, to share information about you and your products and services with us with parties named in a lawsuit or administrative action when we are served with a subpoena or court order. We also are required to share this information with federal or state regulatory authorities, such as banking examiners or the Internal Revenue Service, as authorized by federal or state law. Consistent with the practice of other banks and financial services companies, we also share certain information about you and your products and services with us with reputable credit reporting agencies as authorized by federal law and with others who may receive certain information from us under particular circumstances – *but only as lawfully permitted or required.*

From time to time, we contract with parties outside our affiliated banks and companies in order to make available to you certain services or products. For example, we may contract with insurance companies to make available to you various insurance products. We also sometimes contract with outside agents or service providers to prepare your account statements, enter or calculate transactions and balances, or provide other materials or services on our behalf. These agents, service providers, and third party product providers agree to safeguard our information about you and your products and services with us and must abide by applicable law.

We also occasionally decide to sell business assets or a business line, such as mortgage servicing rights. In these cases, we may transfer to the purchaser the related customer information.

The "Deposit Account Agreement" or the "Customer Disclosure Agreement" for our affiliated banks tells when the bank will disclose account information to third parties. Our affiliated companies, while not required to provide this same disclosure, follow similar rules and provide information to such third parties only in appropriate circumstances.

Question #7: *Do you provide special treatment of information that your affiliated trust company or bank holds as my trustee or disclosed fiduciary, since I am particularly concerned about preserving the confidentiality of this information?*

Answer #7: Yes, any information about you within our trust division, along with your trust or agency accounts, is subject to special protection – even within our affiliated family of banks and companies. This information is considered extremely confidential.

OTHER QUESTIONS ABOUT THE USE AND SHARING OF INFORMATION

Question #8: *Is it possible that one of your affiliated banks or companies may solicit me for a product or service based on information received from an outside source?*

Answer #8: Like other financial services organizations, our affiliated banks and companies sometimes purchase mailing or other lists from outside agencies or companies that are in the business of compiling lists for purchase by others for their independent use. These lists are compiled by such agencies and companies primarily from public sources of information.

Question #9: *How can I remove my name from lists created by outside agencies and companies that are in the business of compiling lists for purchase?*

Answer #9: If you wish to have your name removed from the lists created by outside agencies and companies in the business of compiling lists, send a written request with your name, address and social security number (if issued) to the organizations listed below. These organizations are responsible for notifying the agencies and companies that are in the business of compiling lists that you wish to have your name removed from the lists they sell. Be sure to include all versions of your name that appear in mailings or in calls you receive. You must register your own name and address directly with each organization listed below since they cannot process any requests from us

Mail Preference Service
c/o Direct Marketing Association
P.O. Box 9008
Farmingdale, NY 11735 9008

Telephone Preference Service
c/o Direct Marketing Association
P.O. Box 9014
Farmingdale, NY 11735 9014

The Direct Marketing Association will include your name in its consumer exclusion files so that your name may be removed from lists compiled or maintained by the agencies and companies that are members of that organization. Your name remains in the file for five years.

We hope that the provisions and explanations in this Use of Information brochure answer most of the questions that you have about our use and sharing of information about you. It is an important part of our continuing commitment to provide superior service to you, our customer.

NC 11251 MAT 110 98 2308273

NORWEST

WELLS FARGO

USE OF INFORMATION

Use and Sharing of Information within Our Affiliated Family of Banks and Companies

To provide you with superior service and inform you of product opportunities and for other business purposes, the banks and companies affiliated with Wells Fargo & Company (which include Norwest banks and companies and Wells Fargo banks and companies) share information about you and your products and services among themselves. (See Questions and Answers #1 and #2 inside.) If you send us a written request that contains your name, address, social security number (if issued), your primary accounts or services with us, and your direction, such as "I request to be excluded from affiliate sharing of information," we will not share information about you among our affiliated banks and companies to the extent you may opt out of sharing under the federal Fair Credit Reporting Act and other applicable law. (See Question and Answer #4 inside.) Your written request needs to be mailed to Operations Center (M.S. 6058), P.O. Box 5110, Sioux Falls, SD 57117.

The provisions and explanations in this Use of Information brochure apply only to individuals. These provisions and explanations supersede all previous notices or statements with respect to the subject matter described in this Use of Information brochure. We reserve the right to change the provisions and explanations in this Use of Information brochure at any time. If you previously have informed Norwest or Wells Fargo of your request to be excluded from such affiliate sharing of information, you need not submit another request.