Gail Hillebrand
Senior Attorney
(415) 431-6747

Susanna Montezemolo
Policy Analyst
(202) 462-6262

June 16, 2005

SUMMARY

This statement is presented by Consumers Union,[1] the non-profit, independent publisher of Consumer Reports, on behalf of itself and the Privacy Rights Clearinghouse, a non-profit, non-partisan privacy education and advocacy organization. We believe that the recent security breaches by ChoicePoint, Lexis-Nexis, Bank of America, Citigroup and many others, which have put nearly 10 million Americans at heightened risk of identity theft, underscores the need for Congress and the states to act to protect consumers from identity theft.

Identity theft is a serious crime that has become more common in recent years as we have delved further into the "information age." According to the Federal Trade commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions $48 billion and consumers $5 billion. Victims pay an average of about $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports.[2] The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

And as ongoing scandals point to, American consumers cannot fully protect themselves against identity theft on their own. Even consumers who do "everything right," such as paying their bills on time and holding tight to personal information such as Social Security numbers and dates of birth, can become victim through no fault of their own because the companies who profit from this information have lax security standards.

Therefore, Congress and the states must enact new obligations grounded in Fair Information Practices[3] on those who hold, use, sell, or profit from private information about consumers. In this context, Fair Information Practices would reduce the collection of unnecessary information, restrict the use of information to the purpose for which it was initially provided, require that information be kept secure, require rigorous screening of the purposes asserted by persons attempting to gain access to that information, and provide for full access to and correction of information held.

---

[1] Consumers Union is a non-profit membership organization chartered in 1936 under the laws of the state of New York to provide consumers with information, education and counsel about goods, services, health and personal finance, and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of Consumer Reports, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, Consumer Reports with more than four million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

[2] Identity Theft Resource Center, *Identity Theft: The Aftermath 2003* (September 23, 2003).

[3] The Code of Fair Information Practices was developed by the Health, Education, and Welfare Advisory Committee on Automated Data Systems, in a report released two decades ago. The Electronic Privacy Information Center has described the Code as based on these five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Electronic Privacy Information Center, http://www.epic.org/privacy/consumer/code_fair_info.html.

We recommend that lawmakers do the following:

• **Give Americans the right to control their personal information through security freezes on their credit files.** Giving all consumers state and federal rights to "freeze" their credit files would allow them to block access to their credit reports, and the credit scores derived from those reports, until they affirmatively unlock the files. This would help prevent identity thieves from achieving their ultimate goal – opening up new credit accounts to accumulate debt in their victims' names.

• **Require notice of all security breaches:** Impose requirements on businesses, nonprofits, and government entities to notify consumers when an unauthorized person has gained access to sensitive information pertaining to them. We support S. 751, as introduced by Senator Dianne Feinstein, which would put these requirements in place. We also believe that S. 768, introduced by Senator Charles Schumer and Senator Bill Nelson, will make an excellent notice-of-breach law.

• **Require and monitor security:** Impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available. S. 768, as well as S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively, would direct the Federal Trade Commission to develop such standards and oversee compliance with them.

• **Give consumers access to and a right to correct information:** Give individuals rights to see, dispute, and correct information held by information brokers. This is also addressed in the Schumer/Nelson and Nelson/Markey bills.

• **Protect SSNs:** Restrict the sale, collection, use, sharing, posting, display, and secondary use of Social Security numbers.

• **Require more care from creditors:** Require creditors to take additional steps to verify the identity of an applicant when there is an indicator of possible ID theft.

• **Grant individuals control over their sensitive information:** Give individuals rights to control who collects – and who sees – sensitive information about them.

• **Restrict secondary use of sensitive information:** Restrict the use of sensitive personal information for purposes other than the purposes for which it was collected or other uses to which the consumer affirmatively consents.

• **Fix FACTA:** A consumer should be able to access more of his or her Fair and Accurate Credit Transactions Act (FACTA) rights, such as the extended fraud alert, before becoming an ID theft victim. Further, one of the key FACTA rights is tied to a police report, which victims still report difficulty in getting and using.

• **Create strong and broadly-based enforcement:** Authorize federal, state, local, and private enforcement of all of these obligations.

• **Recognize the role of states:** States have pioneered responses to new forms of identity crime and risks to personal privacy. Congress should not inhibit states from putting in place additional identity

theft and privacy safeguards.

- **Provide resources and tools for law enforcement:** Provide funding for law enforcement to pursue multi-jurisdictional crimes promptly and effectively. Law enforcement also may need new tools to promote prompt cooperation from the Social Security Administration and private creditors in connection with identity theft investigations.

After a very brief discussion of the problem of identity theft, each recommendation is discussed.

THE PROBLEM OF IDENTITY THEFT IS LARGE AND GROWING

Current law simply has not protected consumers from identity theft. The numbers tell part of the story:

- According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the last five years, costing businesses and financial institutions $48 billion, plus another $5 billion in costs to consumers.
- The Privacy Rights Clearinghouse estimates that nearly 10 million people have had their personal data put at risk in security breaches between February 15 and June 6, 2005. See http://www.privacyrights.org/ar/ChronDataBreaches.htm.
- Based on a report to the FTC in 2003 that concluded that there were nearly 10 million identity theft victims each year, Consumers Union estimates that every minute 19 more Americans become victims of ID theft.

These numbers can't begin to describe the stress, financial uncertainty, lost work-time productivity and lost family time identity theft victims experience. Even financially responsible people who routinely pay their bills on time can find themselves in a land of debt collector calls, ruined credit, and lost opportunities for jobs, apartments, and prime credit. With more and more scandals coming out every week, the time has come for Congress to act to protect the security of our personal information.

RECOMMENDATIONS

Prevention of ID Theft Through Security Freezes:

Identity thieves are able to operate in large part because consumers don't control who has access to their credit files. That is, identity thieves who have stolen information about the consumer are able to apply for credit, and the creditor evaluating the fake application examines and relies on the real consumer's credit record to approve credit for the thief. This means that thieves can open accounts in their victims' names easily, and accumulate debt under their assumed identity, spoiling the real consumer's credit record. Eventually, both consumers and creditors pay the price for this –consumers have to spend an average of 600 hours and about $1400 to clear up their credit history, while creditors are left with uncollectible debts owed by impersonators.[4]

---

4 Identity Theft Resource Center, *Identity Theft: The Aftermath 2003* (September 23, 2003).

This could be easily prevented by giving all consumers the ability to decide whether to put a "freeze" on their credit files, which would allow consumers to block access to their credit reports, and the credit scores derived from those reports, until they affirmatively unlock the consumer credit files. Most businesses will not issue new credit or loans to people without first reviewing their credit report or credit score. If the credit file is frozen and an imposter applies for credit in the name of a consumer, a creditor would be very likely to deny the imposter's application, because the security freeze would prevent the prospective creditor from checking the consumer credit report or score. This would protect both the consumer and the business from being harmed by identity theft. Thus, giving Americans the right to place a security freeze on their credit files would help prevent identity thieves from achieving their ultimate goal – opening up new credit account to accumulate debt in their victims' names.

Americans want control over their personal information more than ever before. In a 2003 Harris Poll, 79 percent of surveyed adults reported that it is extremely important to control who can gain access to their personal information. The survey also revealed a growing distrust of the financial holding practices of businesses: A majority of Americans disagreed with the statement that "most businesses handle the personal information they collect about consumers in a proper and confidential way." This poll was conducted well over a year before the ChoicePoint scandal, which began the stream of data security breaches announced in recent months, occurred. Unfortunately, the tide of identity theft means that lack of such control can cost consumers in the time, money, and family stress of trying to remove bad information generated by a thief from the consumer credit file.

Giving consumers control of their personal information through security freezes is also in line with U.S. privacy policy over time. The U.S. has a tradition of protecting privacy rights through law, and the law must adapt to changes to ensure the fair and responsible collection and use of consumers' personal information. In the past, Congress has enacted laws to address privacy risks of the postal system and the telephone, and more recently video rentals and cable TV. Today, we face new challenges. Computers allow the unprecedented storage of our purchasing and financial histories, and data mining technologies programs facilitate the discovery of unanticipated patterns in these data. In addition, the recent creation of new corporate structures, such as financial holding companies that own a vast array of banks, insurance companies, investment firms, and other institutions, provides for the unprecedented sharing of consumers' personal information among affiliated companies. Consumers have little or no control over how a business that holds their personal data chooses to protect it, yet that data is the key that unlocks the consumer's financial life via his or her consumer credit file. The security freeze is an important mechanism to improve their own financial security by locking the door to their consumer credit files.

The security freeze is a practical response to a real problem faced by consumers in today's complex financial world. It allows consumers an important individual protection. For this reason, it has already been enacted in California, Louisiana, Maine, Texas, Vermont, Washington, Colorado, and Nevada, and similar bills are awaiting action by Governors in additional states. This strong response from the states shows the power and importance of state legislative activity to protect their constituents, so it is important that Congress enact a security freeze for everyone but also allow states to provide this and other additional consumer protections for their residents.

Notification:

Notice of security breaches of information, whether held in computerized or paper form, are the beginning, not the end, of a series of steps needed to begin to resolve the fundamental conundrum of the U.S. information U.S. society: collecting information generates revenues or efficiencies for the holder of

the information but can pose a risk of harm to the persons whose economic and personal lives are described by that information.

The first principle of Fair Information Practices is that there be no collection of data about individuals whose very existence is a secret from those individuals. A corollary of this must be that when the security of a collection of data containing sensitive information about an individual is breached, that breach cannot be kept secret from the individual. Recognizing the breadth of the information that business, government, and others hold about individuals, we recommend a notice of breach requirement that is strong yet covers only "sensitive" personal information, including account numbers, numbers commonly used as identifiers for credit and similar purposes, biometric information, and similar information. This sensitive information could open the door to future identity theft, so it is vital that people know when this information has been breached.

We support a notice-of-breach law which does the following:

- Covers paper and computerized data
- Covers government and privately-held information
- Does not except encrypted data
- Does not except regulated entities
- Has no loopholes, sometimes called "safe harbors"
- Is triggered by the acquisition of information by an unauthorized person
- Requires that any law enforcement waiting period must be requested in writing and be based on a serious impediment to the investigation
- Gives consumers who receive a notice of breach access to the federal right to place an extended fraud alert.

We support S. 751, as introduced by Senator Feinstein, which contains these elements. S. 768 contains most, but not all, of these elements and in certain other respects provides additional protections.

Three of these elements are of special importance: covering all breaches without exceptions or special weaker rules for particular industries, covering data contained on paper as well as on computer, and covering data whether or not it is encrypted. First, a "one rule for all breaches" is the only way to ensure that the notice is sufficiently timely to be useful by the consumer for prevention of harm. "One rule for all" is also the only rule that can avoid a factual morass which could make it impossible to determine if a breach notice should have been given. By contrast, a weak notice recommendation such as the one contained in the guidance issued by the bank regulatory agencies[5] cannot create a strong marketplace incentive to invest the time, money, and top-level executive attention to reduce or eliminate, future breaches.

Second, unauthorized access to paper records, such as hospital charts or employee personnel files, are just as likely to expose an individual to a risk of identity theft as theft of computer files. Third, encryption doesn't protect information from insider theft, and the forms of encryption vary widely in

[5] That weak recommendation allows a financial institution to decide whether or not its customers need to know about a breach, and the explanatory material even states that it can reach a conclusion that notice is unnecessary without making a full investigation. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 CFR Part 30, 12 CFR Parts 208 and 225, 12 CFR Part 364, 12 CFR Parts 568 and 570. Other reasons why those guidelines are insufficient to substitute for a statutory requirement to give notice include that they do not apply to non-customers about whom the financial institution has sensitive data, that there is no direct or express penalty for violation of the guideline,, and that their case-by-case approach will make it extremely hard to determine in which circumstances the guidance actually recommends notice to consumers, complicating the process of showing that an obligation was unmet.

their effectiveness. Further, even the most effective form of encryption can quickly become worthless if it is not adapted to keep up with changes in technology and with new tools developed by criminals.

A requirement to give notice of a security breach elevates the issue of information security inside a company. A requirement for swift, no-exemption notice of security breaches should create reputational and other marketplace incentives for those who hold sensitive consumer information to improve their internal security practices. For example, California's security breach law has led to improved data security in at least two cases. According to news reports, after giving its third notice of security breach in fifteen months, Wells Fargo Bank ordered a comprehensive review of all its information handling practices. The column quoted a memo from Wells Fargo's CEO stating in part: "The results have been enlightening and demonstrate a need for additional study, remediation and oversight….Approximately 70 percent of our remote data has some measure of security exposure as stored and managed today." [6]

In another example, UC Berkeley Chancellor Robert Bigeneau announced plans to hire an outside auditor to examine data gathering, retention, and security, telling employees: "I insist that we safeguard the personal information we are given as if it were our own."[7] This announcement followed the second announced breach of the security of data held by the University in six months, this one involving 100,000 people.[8]

In the Sarbanes-Oxley Act, Congress recognized the importance of the "tone at the top," and for that reason took steps to require the corporate boards and CEOs work to improve the quality and accuracy of audited financial statements. A strong, clear notice of security breach law, without exceptions, could similarly focus the attention of top management on information security—creating an incentive for a "tone at the top" to take steps to minimize or eliminate security breaches.

Security:

We support S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively. These measures would direct the Federal Trade Commission (FTC) to promulgate strong standards for information security and a strong obligation to screen customers, both initially and with respect to how those customers further protect the information from unauthorized use. They also provide for ongoing compliance monitoring by the FTC. S. 768, the Schumer/Nelson bill, contains similar provisions.

If Congress wanted to take even stronger steps with respect to information brokers, it could require information brokers to undergo annual audits, paid for by the broker and performed by an independent auditor retained by the FTC, with specific authority in the FTC to require corrective action for security and customer screening weaknesses identified in the audit, as well as allowing the FTC to specify particular aspects of information security that should be included in each such audit.

Any federal information broker law must require strong protections in specific aspects of information security, as well as imposing a broad requirement that security in fact be effective and be monitored for ongoing effectiveness. Congress must determine the balance between the public interest in the protection of data and the business interest in the business of information brokering. Security breaches and the effects on consumers of the ongoing maintenance of files on most Americans by

---

[6] D. Lazarus, "Wells Boss Frets Over Security," S.F. Chronicle, Feb. 23, 2005. http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/02/23/BUGBHBFCR11.DTL

[7] "Cal Laptop Security Put Under Microscope," April 6, 2005, Inside Bay Area, http://www.insidebayarea.com/searchresults/ci_2642564

[8] Opinion Page, Oakland Tribune, April 5, 2005.

information brokers are issues too important to be delegated in full to any regulatory agency.

Access and Correction:

Two of the basic Fair Information Practices are the right to see and the right to correct information held about the consumer. S. 768, S. 500, and H.R. 1080 all address these issues. While the Fair Credit Reporting Act (FCRA) allows consumers to see and correct their credit reports, as defined by FCRA, consumers currently have no legal right to see the whole file held on them by an information broker such as ChoicePoint and Lexis-Nexis, even though the information in that file may have a profound effect on the consumer. There is also lack of clarity about what a consumer will be able to see even under the FCRA if the information broker has not yet made a report to a potential employer or landlord about that consumer.[9]

Because the uses of information held by data brokers continue to grow and change, affecting consumers in myriad ways, consumers must be given the legal right to see all of the information data brokers hold on them, and to seek and win prompt correction of that information if it is in error.

Protection for SSNs:

The Social Security number (SSN) has become a de facto national identifier in a number of U.S. industries dealing with consumers. Some proposals for reform have emphasized consent to the use, sale, sharing or posting of Social Security numbers. We believe that a consent approach will be less effective than a set of rules designed to reduce the collection and use of sensitive consumer information.

Take, for example, an analogy from the recycling mantra: "Reduce, reuse, recycle." Just as public policy to promote recycling first starts with "reducing" the use of materials that could end up in a landfill, so protection of sensitive personal information should begin with reduction in the collection and use of such information. Restrictions on the use of the Social Security number must begin with restricting the initial collection of this number to only those transactions where the Social Security number is not only necessary, but also essential to facilitating the transaction requested by the consumer. The same is true for other identifying numbers or information that may be called upon as Social Security numbers are relied upon less.

We endorse these basic principles for an approach to Social Security numbers:

- Ban collection and use of SSNs by private entities or by government except where necessary to a transaction and there is no alternative identifier which will suffice.
- Ban sale, posting, or display of SSNs, including no sale of credit header information containing SSNs. There is no legitimate reason to post or display individuals' Social Security numbers to the public.
- Ban sharing of SSNs, including between affiliates.
- Ban secondary use of SSNs, including within the company which collected them.
- Out of the envelope: ban printing or encoding of SSNs on government and private checks, statements, and the like
- Out of the wallet: ban use of the SSN for government or private identifier, except for Social Security purposes. This includes banning the use of the SSN, or a variation or part of it, for government and private programs such as Medicare, health insurance, driver's licenses or driver's records, and military, student, or employee identification. Any provision banning the printing of SSNs on identifying cards

[9] Testimony of Evan Hendricks, Editor/Publisher, Privacy Times before the Senate Banking Committee, March 15, 2005, http://banking.senate.gov/files/hendricks.pdf .

should also prohibit encoding the same information on the card.
- Public records containing SSNs must be redacted before posting.
- There should be no exceptions for regulated entities.
- There should be No exception for business-to-business use of SSNs.

Congress should also consider whether to impose the same type of "responsibility requirements" on the collection, sale, use, sharing, display and posting of other information that could easily evolve into a substitute "national identifier," including drivers license number, state non-driver information number, biometric information and cell phone numbers.

Creditor identity theft prevention obligations:

Information is stolen because it is valuable. A key part of that value is the ability to use the information to gain credit in someone else's name. That value exists only because credit granting institutions do not check the identity of applicants carefully enough to discover identity thieves before credit is granted.

Financial institutions and other users of consumer credit reports and credit scores should be obligated to take affirmative steps to establish contact with the consumer before giving credit or allowing access to an account when there is an indicator of possible false application, account takeover or unauthorized use. The news reports of the credit card issued to Clifford J. Dawg, while humorous, illustrate a real problem—creditor eagerness to issue credit spurs inadequate review of the identity of the applicant.[10] When the applicant is a dog, this might seem funny, but when the applicant is a thief, there are serious consequences for the integrity of the credit reporting system and for the consumer whose good name is being ruined.

As new identifiers evolve, criminals will seek to gain access to and use those new identifiers. Thus, any approach to attacking identity theft must also impose obligations on those who make that theft possible – those who grant credit, goods, or services to imposters without taking careful steps to determine with whom they are dealing.

At minimum, creditors should be required to actually contact the applicant to verify that he or she is the true source of an application for credit when certain triggering events occur. The triggering events should include any of the following circumstances:

- Incomplete match on Social Security number
- Address mismatch between application and credit file
- Erroneous or missing date of birth in application
- Misspellings of name or other material information in application
- Other indicators as practices change

Under FACTA, the FTC and the federal financial institution regulators are charged with developing a set of red flag "guidelines" to "identify possible risks" to customers or to the financial institution. However, FACTA stops with the identification of risks. It does not require that financial institutions do anything to address those risks once identified through the not-yet-released guidelines.

---

[10] Both the news stories about Clifford J. Dawg and a thoughtful analysis of the larger problem of too lax identification standards applied by creditors is found in C. Hoofnagle, Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors, in Securing Privacy in the Information Age (forthcoming from Stanford University Press), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=650162.

The presence of a factor identified in the guidelines does not trigger a statutory obligation to take more care in determining the true identity of the applicant before granting credit. Congress should impose a plain, enforceable obligation for creditors to contact the consumer to verify that he or she has in fact sought credit when certain indicators of potential identity theft are present.

Control for consumers over affiliate-sharing, use of information, use of credit reports and credit scores:

Consumers are caught between the growth in the collection and secondary use of information about them on the one hand and the increasing sophistication of criminals in exploiting weaknesses in how that information is stored, transported, sold by brokers, shared between affiliates, and used to access credit files and credit scores.

Identity theft has been fueled in part by information-sharing between and within companies, the existence of databases that consumers don't know about and can't stop their information from being part of, the secondary use of information, and the granting of credit based on a check of the consumer credit file or credit score without efforts to verify the identity of the applicant.[11] We have consistently supported federal and state efforts to give consumers the legal right to stop the sharing of their sensitive personal information among affiliates. Finally, it is essential to stopping the spread of numbers that serve as consumer identifiers that Congress and the states impose strong restrictions on the use of sensitive personal information for purposes other than the purpose for which the consumer originally provided that information.

Fix FACTA:

FACTA has made some things more difficult for identity theft victims, according to information provided to Consumers Union by nonprofits and professionals who assist identity theft victims. Moreover, FACTA gives only limited rights to those who have not yet become victims of identity theft, and FACTA fails to offer a pure prevention tool for all consumers. A consumer who asserts in good faith that he or she is about to become a victim of identity theft gets one right under FACTA—the right to place, or renew, a 90 day fraud alert. However, this type of alert places lower obligations on the potential creditor than the extended alert, which is restricted only to identity theft victims.

A consumer should be able to access more of his or her FACTA rights, such as the extended fraud alert, before becoming an identity theft victim. One key FACTA right is tied to a police report, which victims still report difficulty in getting and using.

Here are some key ways to make FACTA work for victims:

- Initial fraud alert should be one year, not 90 days
- Extended alert and other victims' rights, other than blocking of information, should be available to all identity theft victims who fill out the FTC ID theft affidavit under penalty of perjury
- Business records should be available to any consumer who fills out the FTC ID theft affidavit under penalty of perjury
- Consumers who receive a notice of security breach should be entitled to place an extended fraud alert

[11] Secondary use is use for a purpose other than the purpose for which the consumer gave the information.

• Consumers who place a fraud alert have the right under FACTA to a free credit report, but this should be made automatic.

There is also work to do outside of FACTA, including work to develop a police report that could be given to victims that is sufficiently similar, if not uniform, across jurisdictions, so that the victim does not find creditors or businesses in another jurisdiction refusing to accept a police report from the victim's home jurisdiction.

Congress must encourage the states to continue to pioneer prompt responses to identity crime:

Virtually every idea on the table today in the national debate about stemming identity theft and protecting consumer privacy comes from legislation already enacted by a state. Congress must not cut off this source of progress and innovation. Instead, any identity theft and consumer privacy legislation in Congress should expressly permit states to continue to enact new rights, obligations, and remedies in connection with identity theft and consumer privacy to the full extent that the state requirements are not inconsistent with the specific requirements of federal law.

Criminals will always be more fast-acting, and fast-adapting, than the federal government. An important response to this reality is to permit, and indeed encourage, state legislatures to continue to act in the areas of identity theft and consumer privacy. Fast-acting states can respond to emerging practices that can harm consumers while those practices are still regional, before they spread nationwide. For example, California enacted its notice of security breach law and other significant identity theft protections because identity theft was a significant problem in California well before it became, or at least was recognized as, a national crime wave.

Identity theft illustrates how much quicker states act on consumer issues than Congress. According to numbers released by the FTC, there were 9.9 million annual U.S. victims of identity theft in the year before Congress adopted the relatively modest rights for identity theft victims found in FACTA. The identity theft provisions adopted by Congress in FACTA were modeled on laws already enacted in states such as California, Connecticut, Louisiana, Texas, and Virginia.[12]

Strong and broadly-based enforcement:

Consumers need effective enforcement of those obligations and restrictions Congress imposes in response to the increasing threats to consumer privacy, and of the growth of identity theft. A diversity of approaches strengthens enforcement. Each statutory obligation imposed by Congress should be enforceable by federal agencies, the federal law enforcement structure with the Attorney General and U.S. Attorneys, and State Attorneys General. Where a state is structured so that part of the job of protecting the public devolves to a local entity, such as a District Attorney or City Attorney, those local entities also should be empowered to enforce anti-identity theft and privacy measures in local civil or, where

---

[12] See California Civil Code §§ 1785.11.1, 1785.11.2, 1785,16.1; Conn. SB 688 §9(d), (e), Conn. Gen. Stats. § 36a-699; IL Re. Stat. Ch. 505 § 2MM; LA Rev. Stat. §§ 9:3568B.1, 9:3568C, 9:3568D, 9:3571.1 (H)-(L); Tex. Bus. & Comm. Code §§ 20.01(7), 20.031, 20.034-039, 20.04; VA Code §§ 18.2-186.31:E.

The role of the states has also been important in financial issues unrelated to identity theft. Here are two examples. In 1986, California required that specific information be included in credit card solicitations with enactment of the then-titled Areias-Robbins Credit Card Full Disclosure Act of 1986. That statute required that every credit card solicitation to contain a chart showing the interest rate, grace period, and annual fee. 1986 Cal. Stats., Ch. 1397, codified at California Civil Code § 1748.11. Two years later, Congress chose to adopt the same concept in the Federal Fair Credit and Charge Card Disclosure Act (FCCCDA), setting standards for credit card solicitations, applications and renewals. P. L. 100-583, 102 Stat. 2960 (Nov. 1, 1988), codified in part at 15 U.S.C. §§ 1637(c) and 1610(e). The implementing changes to federal Regulation Z included a model form for the federal disclosure box which is quite similar to the form required under the pioneering California statute. 54 Fed. Reg. 13855, Appendix G.

appropriate, criminal courts.

There is also a role for a private right of action. It is an unfortunate reality in identity theft is that law enforcement resources are slim relative to the size of the problem. This makes it particularly important that individuals be given a private right of action to enforce the obligations owed to them by others who hold their information. A private right of action is an important part of any enforcement matrix.

Money and tools for law enforcement:

Even if all the recommended steps are taken, U.S. consumers will still need vigorous, well-funded law enforcement. At a meeting convened by Senator Feinstein which included some twenty representatives of law enforcement, including police departments, sheriffs, and District Attorneys, law enforcement uniformly proposed that they be given tools to more effectively investigate identity theft. Law enforcement costs money, and the law enforcers noted that the multi-jurisdictional nature of identify theft increases the costs and time, it takes to investigate these crimes.

Law enforcers in California and Oregon have noted a strong link between identity theft crime and methamphetamine. The Riverside County Sheriff noted at a March 29, 2005 event that when drug officers close a methamphetamine lab, they often find boxes of fake identification ready for use in identity theft. The drug team has closed the lab; without funding for training and ongoing officer time, there may be no investigation of those boxes of identities.

To prove a charge of attempted identity theft, a prosecutor may need to prove that the real person holding a particular driver's license number, credit or debit card number, or Social Security number is different from the holder of the fake ID. Doing this may require the cooperation of a state Department of Motor Vehicles, a financial institution, or the Social Security Administration. The public meetings of the California High Tech Crimes Advisory Committee have including discussion of the difficulties and time delays law enforcement investigators encounter in trying to obtain this cooperation. Congress should work with law enforcement and groups representing interest in civil liberties to craft a solution to verifying victim identity that will facilitate investigation of identity theft without infringing on the individual privacy of identity theft victims and other individuals.

Law enforcement may have more specific proposals to enhance their effectiveness in fighting identity theft. We generally support:

- Funding for regional identity theft law enforcement task forces in highest areas of concentration of victims, and of identity thieves
- Funding for investigation and prosecution
- An obligation on creditors, financial institutions, and the Social Security Administration to provide information about suspected theft-related accounts or numbers to local, state, and federal law enforcement after a simple, well designed, request process

We believe that the time has come for both Congress and state legislatures to act to stem identity theft through strong and meaningful requirements to tell consumers of security breaches; strong and detailed security standards and oversight for information brokers, reining in the use of Social Security numbers, increased control for consumers over the uses of their information, and obligations on creditors to end their role in facilitating identity theft through lack of care in credit granting. This should be done without infringing on the role of the states, with attention to the need to fund law enforcement to fight identity theft, and with attention to the need for private enforcement by consumers. We look forward to

working with the Chair and members of the Committee, and others in Congress, to accomplish these changes for U.S. consumers. These recommendations have been informed by the work of victim assistance groups, privacy advocates, and others.[13]

[13] Many law enforcers, victim assistance workers, and consumer and privacy advocates were engaged in the issue of identity theft prevention long before the most recent ChoicePoint security breach came to light. Consumers Union has worked closely for many years on efforts to fight identity theft and protect consumer financial privacy with other national groups, and with consumer privacy and anti-identity theft advocates and victim assistance groups based in California. Our views and recommendations are strongly informed by the experiences of consumers reported to us by the nonprofit Privacy Rights Clearinghouse, the nonprofit Identity Theft Resource Center, and others who work directly with identity theft victims. These groups have worked to develop the state laws that are the basis for many of the proposals now being introduced in Congress. Consumers Union is grateful for the leadership of the Privacy Rights Clearinghouse in consumer privacy policy work, the work of the state PIRGs and U.S.PIRG on consumer identity theft rights which includes the preparation of a model state identity theft statute in cooperation with Consumers Union, for the work for consumers on the accuracy of consumer credit reporting issues done over the past decade by the Consumer Federation of America and U.S. PIRG, and for the contributions to the policy debate of organizations such as the Electronic Privacy Information Center, Privacy Times, and others too numerous to mention.