Testimony of

The Honorable William H. Sorrell

Attorney General
State of Vermont
April 13, 2005

I. INTRODUCTION

Mr. Chairman, Senator Leahy, and honorable members of the Committee, I am William H. Sorrell, Attorney General of the State of Vermont and President of the National Association of Attorneys General. I very much appreciate the opportunity to appear before you today to discuss security breaches relating to personal information of consumers and our recommendations for addressing some of the problems in this area.

The public has become aware of numerous incidences of security breaches in the past two months as a result of California's innovative security breach notification laws. The effect of these security breaches is to expose millions of consumers to potential identity theft, a serious and rapidly growing crime that now costs our nation $50 billion per year. We make the following recommendations to address the problems of security breaches:

? Enact a federal security breach notification law that doesn't preempt more protective state laws.
? Enact a unified federal program for regulation of data brokers that doesn't preempt more protective state laws.
? Strengthen the Gramm-Leach-Bliley "Safeguards Rules" to require definitive minimum standards for information security, and ensure that these rules cover data brokers.
? Recognize the important role of state legislative and law enforcement efforts, particularly in developing security freeze laws.

II. THE GROWTH OF SECURITY BREACHES

Over the past several months, consumers, law enforcement officials and policy makers have learned about a rising incidence of breaches at private companies and public institutions that exposed consumers' personal information to unauthorized third parties. Separately, these breaches involve the personal information of tens of thousands, hundreds of thousands, and even millions of records about consumers nationwide.

A. Numerous Serious Incidences of Security Breaches Have Occurred Since 2002.

Nine known incidences of serious security breaches have occurred in the past few years. It is instructive to examine each one in some detail.

? Ford Motor Credit: In 2002, three individuals were arrested for downloading credit reports on more than 30,000 consumers, and then selling the credit reports to street criminals who emptied the victims' bank accounts and opened credit cards in their names. The scheme centered on an employee of Teledata, a company that provides credit reports to banks and other lenders; the employee stole the passwords and codes of Teledata clients such as Ford Motor Company in order to download credit reports from the three major credit reporting agencies. Over a 10-month period, the password and code for Ford Motor Credit alone was used to download 13,000 credit reports from just one credit reporting agency, Experian. Losses were originally calculated at $2.7 million, but were expected to rise significantly in the weeks after the arrest.
? Acxiom: In 2003, the records of an unknown number of consumers were stolen from commercial data broker Acxiom, based in Little Rock, Arkansas. Hackers were able to download the passwords of 300 business accounts on Acxiom's system, costing the company $5.8 million in losses.
? ChoicePoint: In February 2005, ChoicePoint notified 144,000 consumers nationwide that their personal data may have been accessed by "unauthorized third parties" who were posing as small-business customers. ChoicePoint, an Atlanta-based data broker and specialty credit reporting agency with databases that contain 19 billion public records about consumers and businesses, reported that identity thieves created as many as 50 fake companies that posed as customers and gained access to consumer data.
? Bank of America: Also in February 2005, Bank of America announced that it lost computer backup tapes containing personal information, including names and SSNs, relating to 1.2 million federal workers. The tapes had been lost two

months earlier, in December 2004. Bank of America received permission from its federal regulators to notify consumers about the security problem in mid-February.
? DSW Shoe Warehouse: On March 8, 2005, DSW Shoe Warehouse announced the theft of credit card information, including account numbers and customer names, relating to customers at more than 100 of its 175 stores. The theft took place over a three-month period, beginning in early December 2004. DSW is a subsidiary of Retail Ventures, Inc., based in Columbus Ohio.
? LexisNexis: On March 10, 2005, LexisNexis owner Reed Elsevier PLC announced that records of about 32,000 consumers were accessed and compromised when intruders used log-ins and passwords of a few legitimate customers to obtain access to a database of public records. The records included names, addresses, Social Security numbers (SSNs), and driver's license numbers. The breach occurred at Boca Raton, Florida-based Seisint, a data broker recently purchased by Reed Elsevier and integrated into LexisNexis. Seisint stores millions of personal records about consumers nationwide. On April 12, 2005, LexisNexis announced that an additional 280,000 consumers nationwide had been affected by other security breaches of Seisint data over the past two years.
? Boston College: In late March 2005, Boston College notified 106,000 alumni that a hacker had gained access to a computer database containing personal information about them. Officials of the college stated that they had to tell the affected alumni living in California about the theft due to California's notification law, and the officials therefore decided to tell alumni who live in other states, too, to help them limit their exposure to identity theft.
? University of California: On April 1, 2005, University of California-Berkeley officials announced that a laptop computer containing information about 98,000 students and alumni had been stolen a month earlier. The information, including names, SSNs, and in some instances birth dates and addresses, was unencrypted, although the laptop was password-protected. This breach follows another incident at UC-Berkeley in September 2004 in which a hacker obtained the names, SSNs and other identifying information belonging to 600,000 people.
? San Jose Medical Group: On April 8, 2005, the San Jose (California) Medical Group notified nearly 185,000 current and former patients that their financial and medical records might have been exposed following the theft of computers. The theft occurred after the group copied patient and financial information from its secure servers to two local PCs as part of a patient billing project and the group's year-end audit.
Several conclusions can be drawn from a review of these events. Hackers and identity thieves employ both high-tech means for stealing passwords and other log-in information to access consumers' personal information, as evidenced by the LexisNexis and Acxiom breaches, as well as low-tech techniques to breach information systems, as evidenced by the ChoicePoint incidence. In addition, although the pace of disclosures about these breaches has accelerated over the past few months, it is safe to presume that breaches have been occurring regularly over the past several years. What has changed is not the existence of the problem, but rather the public's awareness of it.
B. The Public Has Learned About These Breaches As a Result of California's Security Breach Notification Laws.

On July 1, 2003, California's security breach notification laws went into effect. These laws require businesses and California public institutions to notify the public about any breach of the security of their computer information system where unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. California's laws require that the notice be given without unreasonable delay, consistent with the legitimate needs of law enforcement, which can request a delay in notification if the notice would impede a criminal investigation of the incidence. "Personal Information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data element is not encrypted:
? Social Security number.
? Driver's license number or California Identification Card number.
? Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
The California law allows a business or public institution to satisfy the notice requirement in several ways: written notice through the mail; electronic notice in conformity with the Federal Electronic Signatures Act; substitute notice through email, website publication, and major statewide news media if more than 500,000 consumers are affected; or in conformity with the business' or institution's own notification system, if it meets the timeliness requirements of the California security breach notification laws.
California's unique and innovative laws in this area have ensured that we are aware of the growing problem of data leaks that are plaguing our nation's businesses and public institutions.
III. THE EFFECT OF SECURITY BREACHES
Identity theft, already a growing problem, is likely to grow even more rapidly as a result of security breaches. The effect of these data leaks is to expose consumers to the threat of identity theft by the criminals who gain access to consumers' personal information. MSNBC has noted that in the six-week period from mid-February through early

April, the rash of data heists has exposed more than two million U.S. consumers to possible identity theft.
Current estimates of the incidence of identity theft in the United States are disturbingly high. According to a survey released in January 2005 by Javelin Strategy & Research, about 9.3 million U.S. adults were victims of identity theft between October 2003 and September 2004.
Even though the vast majority of victims of identity theft do not report the crime to law enforcement authorities or credit bureaus, the reported incidence of identity theft has grown dramatically. The Federal Trade Commission reported in February 2005 that the number of identity theft complaints submitted to its Consumer Sentinel database has grown from 161,896 in 2002 to 246,570 in 2004, representing a growth rate of more than 50% in two years. Victims' information is misused to perpetrate financial fraud in the vast majority of cases: fraud involving credit cards, checking and savings accounts, and electronic funds transfers represented 46% of the complaints in 2004. Members of this Committee represent states that contain areas suffering the most from the growing incidence of identity theft. Out of the 50 Metropolitan Statistical Areas that have generated the greatest number of complaints relative to population, six are in California, four are in Texas, three are in each of New York, Ohio, Pennsylvania, and Wisconsin, and two are in Illinois. Arizona victims of identity theft have filed the largest number of complaints relative to population, followed by Nevada, California, Texas, Colorado, Florida, New York, Washington, Oregon, and Illinois.
Identity theft has a deeply negative impact on our nation's economy. According to a survey published by the Federal Trade Commission in September 2003, the total cost of identity theft approaches $50 billion per year, with victims bearing about $5 billion of the losses, and businesses bearing the remaining $45 billion. The average loss from the misuse of a victim's personal information is $4,800, but for victims who had new credit card and other accounts opened in their name, the average loss is $10,200. Overall, victims spent almost 300 million hours resolving problems relating to identity theft in one year, with almost two-thirds of this time - 194 million hours - spent by victims who had new credit card and other accounts opened in their name.
IV. CONSUMERS' AND STATE OFFICIALS' CONCERNS ABOUT SECURITY BREACHES

The recent rash of information heists have had several important effects on the state and local level. Consumers have expressed concerns about their current level of knowledge of security breaches and what they realistically can do in the event they become a victim. State Attorneys General and other state and local officials have taken action in a number of areas to resolve these concerns.
? Consumers Across the Nation Want to Receive Notice of Security Breaches.
The citizens of California have received notice of security breaches as a result of that state's innovative law. Consumers in the remaining 49 states, the District of Columbia and the territories want the same right to receive notice when their personal information is accessed in an unauthorized manner. Unfortunately, in the absence of other state laws or a federal minimum standard, consumers in the other states have not consistently received notices in the recent spate of incidences. LexisNexis sent notices on a voluntary basis to affected consumers nationwide. ChoicePoint originally sent notices only to California residents; only after receiving letters from the Attorneys General of numerous states did ChoicePoint expand its notification process to include potentially affected consumers in all states.

In addition to haphazard notification, the paucity of regulation in this area has led to another problem. The notices that were actually received by consumers came in envelopes from "ChoicePoint." Consumers have no idea who ChoicePoint is because consumers typically have no business relationship with ChoicePoint. We learned of instances where consumers tossed out the notification letters without opening them, on the assumption that the letters were another unsolicited offer for a credit card or some other piece of junk mail.
Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by identity theft. The Federal Trade Commission reports that the overall cost of an incident of identity theft, as well as the harm to the victims, are significantly smaller if the misuse of the victim's personal information is discovered quickly. For example, when the misuse was discovered within five months of its onset, the value of the damage was less than $5,000 in 82% of the cases. When victims did not discover the misuse for six months or more, the thief obtained $5,000 or more in 44% of the cases. In addition, new accounts were opened in less than ten percent of the cases when it took victims less than a month to discover that their information was being misused, while new accounts were opened in 45 percent of cases when six months or more elapsed before the misuse was discovered.

To ensure that citizens across the nation receive adequate notice about security breaches, twenty-eight states are currently considering legislation modeled on California's law.
? After Learning About a Breach of Their Personal Information, Consumers Want to Review Their Credit Reports to Determine if They Are Victims of Identity Theft.

The 2003 amendments to the federal Fair Credit Reporting Act gave consumers the right to receive a free copy of their credit report once every 12 months, following the example previously set by seven states that require credit reporting agencies to provide free reports to their citizens. However, because the FTC allowed the nationwide credit reporting agencies to stagger the implementation of the national free credit report, consumers in the Southern states -- Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, Oklahoma, South Carolina, Tennessee, and Texas -- are not able to order their free reports under federal law until June 1, 2005. And consumers in the Eastern states -- Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Rhode Island, Vermont, Virginia, and West Virginia, as well as the District of Columbia, Puerto Rico, and all U.S. territories -- are not able to order their free reports under federal law until September 1, 2005. As a result, many citizens have been unable to see their credit report for free during this time of heightened anxiety over possible
identity theft, causing great frustration in the Eastern and Southern states.
In addition, in those Eastern and Southern states - like Vermont - that already require credit reporting agencies to provide free credit reports under state law, consumers have been confused and frustrated because the credit reporting agencies have not adequately adjusted their systems to enable consumers in these states to easily access their free report under state law. Many consumers in Vermont attempted to obtain their free report under Vermont law after learning about the ChoicePoint and other security breaches, only to be told - incorrectly - by the credit bureaus' voice-mail systems that they were not eligible for a free credit report.
? Consumers Want to Control Access to Their Credit Reports so that Identity Theft Does Not Occur.

The 2003 amendments to the federal Fair Credit Reporting Act also gave consumers the right to place a "fraud alert" on their credit reports for at least 90 days, with extended alerts lasting for up to seven years in cases where identity theft occurs. Yet many states are considering enacting stronger measures to assist consumers in combating the rapidly escalating outbreak of security breaches. Two states, California and Texas, allow consumers to place a "security freeze" on their credit report. A security freeze allows consumers to control who will receive a copy of their credit report, thus making it nearly impossible for criminals to use stolen information to open an account in the consumers' name. Security freeze provisions will become effective on July 1, 2005, in two additional states, Louisiana and Vermont. Although the credit bureaus argue that security freezes are overkill, and cause consumers more harm than good, many members of the business community in Vermont supported implementation of our security freeze law, enacted last year. Overall, consumer advocates and many State Attorneys General believe that security freeze laws are one of the most effective tools available to stop the harm that can result from data heists. Twenty states are currently considering security freeze bills.
V. RECOMMENDATIONS ON ADDRESSING THE PROBLEM OF SECURITY BREACHES

We recommend that this Committee take several actions to address the security breach problem, with its concomitant potential effect on the increased incidence of identity theft. The recommendations center on enactment of better federal laws to address the problem, while allowing the states to continue to perform their vital functions in assisting consumers and creating additional innovative solutions.
1. Enact a Federal Security Breach Notification Law: Enact a federal law requiring notice of security breaches in appropriate circumstances. Allow states to enact laws that are more protective of consumers, thus ensuring that states can continue devising additional innovative solutions to this issue.
2. Enact a Federal Program for Regulation of Data Brokers: Enact a federal law to regulate data brokers in a manner similar to regulation of credit reporting agencies. Currently, the regulation of data brokers comes under a scattered mixture of federal laws, including the federal Fair Credit Reporting Act, the Gramm-Leach-Bliley Act (GLBA), and a few other laws, and arguably these laws do not cover all the practices of data brokers. In developing a unified federal regulatory scheme for data brokers, only preempt state laws to the extent that they are less protective of consumers.
3. Strengthen the "Safeguards Rules": Enact a federal law that will strengthen the GLBA Safeguards Rules issued by the federal financial regulators and the Federal Trade Commission. Currently, these rules require the covered institutions to develop a written information security plan that describes their programs to protect customer information, and to maintain reasonable security for customer information. The rules were intended to provide flexibility to account for each covered institution's size, complexity, scope of activities, and sensitivity of information handled. However, in light of the recent wave of security breaches, we believe that more definitive minimum standards of information security should be required, and that the Safeguards Rules should be expanded to more clearly cover data brokers.
4. Recognize the Important Role Of State Legislative and Investigative Efforts: States are providing key additional protections for consumers. California's security breach notification law, and the security freeze laws in California, Louisiana, Texas, and Vermont, are important examples of the critical role played by states in developing innovative

solutions to the complex problems presented by data breaches. In addition, State Attorneys General and local law enforcement are playing critical roles in the investigations surrounding security breaches that have been disclosed to date. State and local law enforcement officials are cooperating with their federal counterparts to investigate and prosecute the perpetrators, and to determine if there were defects in security systems that may have allowed the breaches to occur. Congress should recognize these vital functions provided by state and local authorities, and ensure that these functions are not preempted.

Thank you for giving me the opportunity to testify on this important subject.