

Testimony

Of

Assistant Attorney General Julie Brill
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609-1001
Tel: 802-828-3658

Email: jbrill@atg.state.vt.us

before the

Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
United States House of Representatives

Hearing on H.R. 3997, the Financial Data Protection Act

November 9, 2005

Good morning, Chairman Bachus, Ranking Member Sanders, and distinguished members of the Subcommittee on Financial Institutions and Consumer Credit. Thank you for inviting me to speak with you today on the important issue of security breaches and protection of personal information. My name is Julie Brill, and I am an Assistant Attorney General for the State of Vermont. I have been working in the consumer protection arena in Vermont for 14 years, specializing in privacy and data security issues, among other things. In addition, I am chair of the National Association of Attorneys General Working Group on Privacy, and chair of the National Association of Attorneys General Working Group on Credit Reporting. In these capacities, I have worked with the National Association of Attorneys General on numerous national issues relating to privacy, security breaches and data security, including comments to Congress and various federal agencies. I testify this morning on behalf of the National Association of Attorneys General as well as Vermont Attorney General William H. Sorrell.

There have been reports of over 118 data leaks this year, which taken together have affected 57 million consumers in the United States.¹ The security breaches have exposed millions of consumers to potential identity theft, a serious and rapidly growing crime that now costs our nation over \$50 billion per year. Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by theft of personal information. As a result of California's innovative state law, now adopted by 21 additional states, the public has become aware of these numerous

¹ See Choicepoint's 2005 Disclosures of US Data Incidents, available at <http://www.privacyatchoicepoint.com/common/pdfs/Datadislosures2005.pdf>.

data leaks.² State security breach notification laws have provided consumers with vital information about unauthorized access to their personal information, so that the affected consumers can take precautions to ensure that they do not become victims of identity theft, or that any harm they experience as a victim of identity theft is minimized.

The National Association of Attorneys General is gratified that this Committee is considering legislation to create a federal security breach notification law modeled on state laws. The issue is of such importance that just two weeks ago, 48 State Attorneys General set forth their views on the appropriate contours of any federal law in a letter to the Congressional leadership.³ The letter is attached to my written testimony and dated November 7, 2005, to reflect all signatories to date.

In their letter, the Attorneys General call on Congress to enact a strong federal security breach notification law that provides meaningful information about data leaks to consumers. If Congress is unable to enact a strong notice law, then the Attorneys General suggest that Congress leave the issue to the states, which have responded rapidly and strongly to the problems presented by security breaches.

The Attorneys General believe an effective federal security breach notification law would contain the following elements.

² The following states have enacted security breach notification laws: Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Rhode Island, Tennessee, Texas, and Washington.

³ The original letter, dated October 27, 2005, was signed by the Attorneys General of Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Hawaii, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Northern Mariana Islands, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, Wisconsin, and Wyoming. The Attorney General of New Mexico joined the letter a few days after it was originally sent. The letter is now dated November 7, 2005.

- The federal law should broadly define “security breach” as unauthorized acquisition of or access to computerized, paper or other data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. There should be no additional requirement that the breach entail actual harm or a measure of risk of harm.
- In the event that Congress decides to consider the concept of harm in addition to the unauthorized acquisition of personal information before notice would be required, the “harm” element should be an exception, not a trigger, in order to make it plain that a notice must be given in the absence of sufficient information. Security breach notices should be provided to consumers ***unless there is no risk of harm or misuse of personal information*** resulting from the breach.
- The breached entity should be required to consult with law enforcement and receive an affirmative response that there is no risk of harm or misuse of personal information from the breach before the “harm” exception would apply.
- All entities, including financial institutions governed under the Gramm-Leach-Bliley, should be covered.
- There should be no “fraud monitoring” exception, especially with respect to compromised information relating to debit card, bank account and other non-credit card account information.

The Attorneys General believe that Congress should ensure that the federal security breach notification law can be enforced by the State Attorneys General in state or federal court. Federal regulators like the Federal Trade Commission require assistance from local law enforcement in many areas affecting consumers, including telemarketing, credit reporting, and general unfair and deceptive practices. State Attorneys General are currently involved in investigating security breaches, and Congress should ensure that the Attorneys General continue to protect consumers in this important area.

Lastly, but most importantly, the Attorneys General urge Congress not to preempt state security breach notification laws. In the event that Congress considers preemption of state laws in this area, such preemption should be narrowly tailored so that only state laws that are "inconsistent" with the federal law are affected, and then "only to the extent of the inconsistency". The federal law may govern the timing, manner and content of security breach notification laws, but should not interfere with state laws addressing notices to be provided by entities not covered by the federal law or the consequences of security breaches.

Thank you for giving me this opportunity to testify on this important subject. I will be happy to answer questions.

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

750 FIRST STREET NE SUITE 1100

WASHINGTON, D.C. 20002

(202) 326-6018

(202) 408-6998

<http://www.naag.org>

LYNNE M. ROSS
Executive Director

November 7, 2005

PRESIDENT
STEPHEN CARTER
Attorney General of Indiana

PRESIDENT-ELECT
THURBERT BAKER
Attorney General of Georgia

VICE PRESIDENT
LAWRENCE WARDEN
Attorney General of Idaho

IMMEDIATE PAST PRESIDENT
WILLIAM H. SORRELL
Attorney General of Vermont

Honorable Bill Frist
Senate Majority Leader
509 Senate Hart Office Building
Washington, D.C. 20510-4205

Honorable Harry M. Reid
Senate Minority Leader
528 Senate Hart Office Building
Washington, D.C. 20510-3903

Honorable J. Dennis Hastert
Speaker of the House
235 Cannon House Office Building
Washington, D.C. 20515-1314

Honorable Nancy Pelosi
House Minority Leader
2371 Rayburn House Office Building
Washington, D.C. 20515-0508

Dear Congressional Leaders:

We, the undersigned Attorneys General, applaud the efforts of the various committees in Congress which are considering enactment of a national security breach notification and security freeze law. Over the past year, the public has become aware of numerous incidences of security breaches, exposing millions of consumers to harm, including potential identity theft, a serious and rapidly growing crime that now costs our nation over \$50 billion per year. The issues under consideration by you and your members could provide critical assistance to identity theft victims in our states and throughout the nation.

To assist your efforts, we offer the following comments, representing our views on certain critical issues relating to your consideration of security breach notification and

security freeze legislation.

1. Enact a strong security breach notification law

We call on Congress to enact a national security breach notification law that will provide meaningful information to consumers. If Congress is not able to enact a strong notice law, it should leave the issue to state law, which is responding strongly. Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by theft of personal information. The Federal Trade Commission (FTC) reports that the overall cost of an incident of identity theft, as well as the harm to the victims, is 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 value of the damage was \$5,000 or more in 44% of the cases. In addition, new accounts were opened in fewer than 10% 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% of cases when six months or more elapsed before the misuse was discovered.

The public has become aware of the numerous incidences of security breaches over the past year as a result of California's security breach notification laws, which went into effect on July 1, 2003. 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.

The public has become so concerned about security breaches and their potential

role in the increased incidence of identity theft that 21 additional states have enacted security breach notification laws over the past year: Arkansas, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Rhode Island, Tennessee, Texas, and Washington.

We urge your committee to enact a meaningful federal security breach notification provision that is at least as protective of consumers as California law. A meaningful federal security breach notification law would, in our view, broadly define what constitutes a security breach and the notice requirements in order to give consumers a greater level of protection. For example, "security breach" should be broadly defined as "unauthorized acquisition of or access to computerized or other data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." We also believe that the standard for notification should be tied to whether personal information, whether in electronic or paper form, was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, rather than a standard that includes an additional requirement that the breach entail actual harm or a measure of risk of harm. Standards that require additional proof by a tie to harm or to a risk of harm place the bar too high. It is extremely difficult in most cases for a breached entity to know if personal data that has been acquired from it by an unauthorized person will be used to commit identity theft or other forms of fraud. It is certain, however, that creating an additional trigger requirement relating to proof of risk will result in fewer notices than consumers now receive under many state laws. We note that the majority of states that have enacted security breach notification laws – California, Georgia, Illinois, Indiana,

Maine, Minnesota, Nevada, New York, North Dakota, Ohio, Rhode Island, Tennessee, and Texas – do not require any additional trigger requirement before notice about a breach is required to be given to affected consumers.

In the event that Congress decides to consider the concept of harm in addition to the unauthorized acquisition of personal information in the context of security breach notification, we urge Congress to cast this element as an exception, not a trigger, in order to make it plain that notice must be given in the absence of sufficient information. Such an exception could contain the following provisions: (1) security breach notices must be provided to consumers unless there is “no risk of harm or misuse of personal information” – not “no risk of identity theft” – resulting from the breach; (2) security breach notices must be provided to consumers in the event that it cannot be determined whether or not there will be a risk of harm or misuse of personal information; (3) the breached entity should be required to consult with law enforcement and receive an affirmative written response with respect to the determination that there is no risk of harm resulting from the breach; and (4) any determination by law enforcement that there is “no risk of harm or misuse of personal information” should be made in writing and filed with both the FTC and with the State Attorney General from the state in which the breach occurred.

In addition to an acquisition-based notification standard, we believe that an effective federal security breach notification law should have the following additional provisions:

- Coverage of all entities, including financial institutions governed by the Gramm-Leach-Bliley Act. Financial institutions, which may hold very sensitive data

about consumers, should not be subject to a lesser standard for giving notice under their regulatory guidelines than other entities are held to by statute.

- Inclusion of the following as “personal information” that, if acquired or accessed by an unauthorized person, would trigger notification: an individual's first name or first initial and last name, or the name of a business, 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 government-issued identification number.
 - Account number, credit or debit card number, alone or in combination with any required security code, access code, or password that would permit access to an individual's financial account.
 - A unique electronic identification number, email address, or routing code alone or in combination with any required security code, access code, or password.
 - Unique biometric data such as fingerprint, voice print, a retina or iris image, or other unique physical representation.
 - Home address or telephone number.
 - Mother's maiden name.
 - Month and year of birth.
 - Such other information as the FTC may add by regulation.
- Notification provisions that would, at a minimum, provide the following notices to consumers: individual notice by mail or by email if the consumer has

consented to email in a manner consistent with the requirements of the Electronic Signatures in Global and National Commerce Act; substitute notice, if permitted at all, could be an option only when more than 500,000 consumers are affected and should require publication on a website and in major statewide or national news media.

- No “fraud monitoring” exemptions, especially when the compromised information relates to a debit card, bank account, or other non-credit account.

2. **Enact a strong federal security freeze law.**

We also call on Congress to enact a strong federal security freeze law. The 2003 amendments to the federal Fair Credit Reporting Act 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. Several states have enacted stronger measures to assist consumers in combating the rapidly escalating outbreak of security breaches. Five states – California, Louisiana, Texas, Vermont, and Washington – already allow consumers to place a “security freeze” on their credit report. A security freeze allows a consumer to control who will receive a copy of his or her credit report, thus making it nearly impossible for criminals to use stolen information to open an account in the consumer’s name. Security freeze provisions will become effective in the next several months in the following additional seven states: Colorado, Connecticut, Illinois, Maine, Nevada, New Jersey, and North Carolina.

We believe that security freeze laws that give all consumers the right to use a freeze as a prevention tool are one of the most effective tools available to stop the harm that can result from data heists. If Congress is inclined to create a federal security freeze

law, we urge Congress to make such a law meaningful by modeling it on the best provisions in comparable state laws, including:

- Creating a security freeze that is available to all consumers at no fee or a low-capped fee.
- Banning fees for victims of identity theft who have a police report or FTC affidavit, seniors, veterans, and persons who receive a notice of security breach.
- Allowing consumers who choose to implement a freeze to also have the ability to selectively or temporarily lift the freeze, again at no charge to victims of identity theft, seniors, veterans, and persons who receive a notice of security breach, and to other consumers at a modest, capped fee.
- Ensuring that the security freeze provisions apply to all entities who may examine a credit file in connection with new accounts, including accounts for goods and services, such as cell phones, utilities, rental agreements, and the like.
- Allowing consumers who choose to implement a freeze with all three major national consumer reporting agencies to be able to do so by contacting one of them, rather than all three individually.

3. Allow the State Attorneys General to enforce the new federal security breach notification and security freeze laws in state or federal court.

We further call on Congress to ensure that State Attorneys General can enforce any new federal security breach notification and security freeze laws. The FTC continues to do a commendable job in enforcing its current laws, including the FTC Act and the

