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

PRESIDENT
STEPHEN CARTER
Attorney General of Indiana

PRESIDENT-ELECT
THURBERT BAKER
Attorney General of Georgia

VICE PRESIDENT
LAWRENCE WASDEN
Attorney General of Idaho

IMMEDIATE PAST PRESIDENT
WILLIAM H. SORRELL
Attorney General of Vermont

October 27, 2005

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 your committee and others to consider 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 your committee 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

Gramm-Leach-Bliley Act, against entities that have not employed sufficient protections to safeguard consumers' personal information. However, consumers would suffer if Congress were to make the FTC the sole enforcer of new laws requiring security breach notification and security freezes. Indeed, State Attorneys General are currently involved in investigating security breaches and enforcing available state standards relating to use of adequate procedures and processes to protect consumers' personal information. Congress should ensure that State Attorneys General continue to play their important role in protecting consumers from practices that could lead to identity theft.

4. Do not preempt the power of states to enact and enforce state security breach notification and security freeze laws.

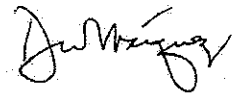
We urge Congress to not preempt the states in these two important consumer protection areas, or indeed in other areas. Preemption interferes with state legislatures' democratic role as laboratories of innovation. The states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government. Indeed, Congress would not be considering the issues of security breach notification and security freeze if it were not for earlier enactment of laws in these areas by innovative states.

In the event that Congress determines that it will consider preemption of the states in these areas, we urge Congress at a minimum to narrowly tailor preemption so that only those states laws that are "inconsistent" with the federal laws would be preempted, and then "only to the extent of the inconsistency." This is important because Congress may enact a security breach notification law or a security freeze law that does not cover all entities, and the states should be allowed to enact laws that cover those additional entities. While we oppose preemption in general, it is particularly important that if Congress does

adopt some degree of preemption, that preemption be limited to the timing, manner, and content of notices of security breach, and not interfere with other state laws addressing the subject of, or consequences of, a security breach.

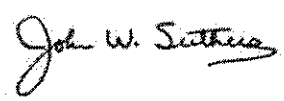
Thank you for considering our recommendations. We look forward to working with you on this important legislation in the coming weeks and months.

Sincerely,

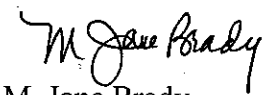


David W. Márquez
Attorney General of Alaska

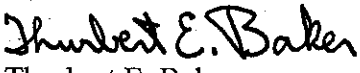
Mike Beebe
Attorney General of Arkansas



John Suthers
Attorney General of Colorado

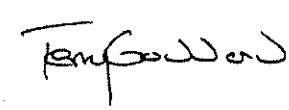


M. Jane Brady
Attorney General of Delaware

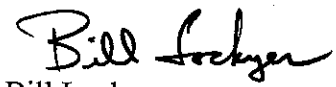


Thurbert E. Baker
Attorney General of Georgia

Stephen H. Levins, Executive Director
Hawaii Ofc. Consumer Protection

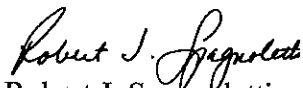


Terry Goddard
Attorney General of Arizona



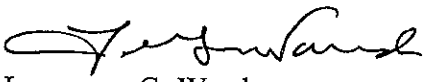
Bill Lockyer
Attorney General of California

Richard Blumenthal
Attorney General of Connecticut



Robert J. Spagnoletti
Attorney General of District of Columbia

Mark J. Bennett
Attorney General of Hawaii



Lawrence G. Wasden
Attorney General of Idaho

Lisa Madigan
Attorney General of Illinois

Tom Miller
Attorney General of Iowa

Gregory D. Stumbo
Attorney General of Kentucky

Charles Foti
Attorney General of Louisiana

G. Steven Rowe
Attorney General of Maine

J. Joseph Curran, Jr.
Attorney General of Maryland

Tom Reilly
Attorney General of Massachusetts

Mike Cox
Attorney General of Michigan

Mike Hatch
Attorney General of Minnesota

Jim Hood
Attorney General of Mississippi

Jay Nixon
Attorney General of Missouri

Mike McGrath
Attorney General of Montana

Jon Bruning
Attorney General of Nebraska

Brian Sandoval
Attorney General of Nevada

Kelly Ayotte
Attorney General of New Hampshire

Peter C. Harvey
Attorney General of New Jersey

Eliot Spitzer
Attorney General of New York

Roy Cooper
Attorney General of North Carolina

Wayne Stenehjem
Attorney General of North Dakota

Jim Petro
Attorney General of Ohio

Hardy Myers
Attorney General of Oregon

Roberto J. Sanchez-Ramos
Attorney General of Puerto Rico

Henry McMaster
Attorney General of South Carolina

Paul G. Summers
Attorney General of Tennessee

Mark Shurtleff
Attorney General of Utah

Rob McKenna
Attorney General of Washington

Pamela Brown
Attorney General of Northern Mariana Islands

W.A. Drew Edmondson
Attorney General of Oklahoma

Tom Corbett
Attorney General of Pennsylvania

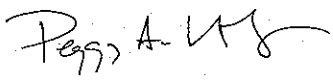
Patrick Lynch
Attorney General of Rhode Island

Larry Long
Attorney General of South Dakota

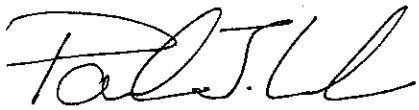
Greg Abbott
Attorney General of Texas

William H. Sorrell
Attorney General of Vermont

Darrell V. McGraw, Jr.
Attorney General of West Virginia



Peggy A. Lautenschlager
Attorney General of Wisconsin



Patrick J. Crank
Attorney General of Wyoming

cc: Chairman Shelby & Ranking Member Sarbanes
Senate Committee on Banking, Housing, and Urban Affairs

Chairman Stevens & Ranking Member Inouye
Senate Committee on Commerce, Science, & Transportation

Chairman Specter & Ranking Member Leahy
Senate Committee on the Judiciary

Chairman Barton & Ranking Member Dingell
House Committee on Energy & Commerce

Chairman Oxley & Ranking Member Frank
House Committee on Financial Services

Chairman Sensenbrenner & Ranking Member Conyers
House Committee on the Judiciary

I. Of the states listed, Hawaii is also represented by its Office of Consumer Protection, an agency which is not a part of the state Attorney General's Office, but which is statutorily authorized to represent the State of Hawaii in consumer protection actions. For the sake of simplicity, the entire group will be referred to as the "Attorneys General," and such designation as it pertains to Hawaii, refers to the Attorney General and Executive Director of the State of Hawaii Office of Consumer Protection.