National Association
of Attorneys General

PRESIDENT
Marty Jackley
South Dakota Attorney General

PRESIDENT-ELECT
George Jepsen
Connecticut Attorney General

VICE PRESIDENT
Derek Schmidt
Kansas Attorney General

IMMEDIATE PAST PRESIDENT
Jim Hood
Mississippi Attorney General

EXECUTIVE DIRECTOR
James McPherson

2030 M Street, NW
Eighth Floor
Washington, DC 20036
Phone: (202) 326-6000
http://www.naag.org/

July 7, 2015

Honorable Mitch McConnell
Senate Majority Leader
317 Russell Senate Office Building
Washington, DC 20510

Honorable Harry Reid
Senate Minority Leader
522 Hart Senate Office Building
Washington, DC 20510

Honorable John Boehner
Speaker of the House
1011 Longworth House Office Building
Washington, DC 20515

Honorable Nancy Pelosi
House Minority Leader
233 Cannon House Office Building
Washington, DC 20515

Dear Congressional Leaders:

We, the undersigned Attorneys General, write to provide our perspective on the recent efforts in Congress to pass a national law on data breach notification and data security. As the chief consumer protection officials in our respective states, we have seen first-hand the harm that data breaches and identity theft cause consumers. There are numerous bills pending in congress that would create federal data breach notification and data security laws. However, any additional protections afforded consumers by a federal law must not diminish the important role states already play protecting consumers from data breaches and identity theft.

In 2005, forty-four state attorneys general wrote a similar letter to Congress calling for a national law on breach notification that did not preempt state enforcement or state law. The letter stated:

Do not preempt the power of states to enact and enforce state security breach notification...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.[1]

In the intervening decade since the prior letter, states have further proven these points, as offices of attorneys general have played critical roles investigating and enforcing data security lapses and responding to identity theft and consumer fraud on behalf of constituents. At the same time, state legislatures have continued to pass significant, innovative laws related to data security, identity theft, and privacy.

[1] Letter to Congressional Leaders from the National Association of Attorneys General (NAAG) (Oct. 27, 2005).

We write now to restate our concerns over the inclusion of a preemption provision in any national law on data security and data breach notification.

Data Breaches and Identity Theft Cause Significant Harm to Consumers

Since 2005, nearly 5,000 data breaches have compromised 815,842,526 records.[2] These records contain sensitive information about consumers – primarily financial account information, Social Security numbers or medical information. The breach of this information exposes consumers to identity theft. One study found that the breach of a Social Security number increases a consumer's risk of identity theft by 18 times.[3]

Our offices regularly receive complaints from consumers who have been victims of identity theft. At the federal level, identity theft has been the largest category of consumer complaints received by the Federal Trade Commission for fifteen consecutive years.[4] In 2013, unauthorized use of credit and debit cards resulted in $11 billion in fraud losses.[5] Full-blown identity theft involving the use of a Social Security number can cost a consumer $5,100 on average.[6]

States Play an Important Role Responding to Data Breaches and Identity Theft

States are the front line in helping consumers deal with the repercussions of a data breach. Our offices have helped tens of thousands of consumers remove fraudulent charges from their financial accounts and repair bad credit caused by identify theft. We also work to prevent the likelihood of identity theft by ensuring data collectors take the necessary steps to protect consumers' information. To do this, our offices regularly investigate the causes of data breaches to determine whether data collectors experiencing breaches used reasonable data security practices and notified consumers of the breaches according to the requirements of our state laws.

States began adopting data breach notification laws in 2003. These laws were designed to provide consumers with information about their compromised personal and financial information so they could take steps to protect themselves from identity theft. As of today, forty-seven states have passed laws requiring data collectors to notify consumers when their personal information

---

[2] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/data-breach, (accessed March 13, 2015).

[3] National Consumers League, The Consumer Data Insecurity Report: examining the Data Breach – Identity Fraud Paradigm in Four Major Metropolitan Areas, 14, (June 2014).

[4] Federal Trade Commission, *Press Release: Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014*, (Feb. 27, 2015).

[5] Javelin Strategy & Research, 2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends, 17, (Feb. 2014).

[6] Herb Weisbaum, *Data breaches cost consumers billions of dollars*, Today, (June 5, 2013).

has been compromised by a data breach.[7] A number of states have also passed laws affirmatively requiring companies to adopt reasonable data security practices.

In recent years, a number of states have reexamined and updated their data breach notification laws to ensure they continue to protect the sensitive information about consumers being collected. Some states now include notification requirements for compromised biometric data, login credentials for online accounts, and medical information. These categories reflect the significant increase in data collection that has occurred over the past ten years and respond to consumers' concerns about that increase.

Additionally, a number of states now require data collectors experiencing breaches to directly notify the attorneys general in states where the affected consumers reside. This requirement enables those offices to more quickly respond to breaches and accurately provide information to concerned consumers. The much-needed transparency over data breaches that has been achieved in recent years is largely attributable to these requirements at the state level.

Recognizing the need to work together at the state level, forty states participate in the Privacy Working group. This group discusses and jointly investigates data breaches and other privacy matters. When a breach impacts consumers in multiple states, the working group coordinates its resources and works together to determine whether consumers' information was unnecessarily at risk and whether the breached data collector took proper steps to notify consumers.

Data Security Vulnerabilities Are Too Common

Our offices have seen numerous cases in which companies failed to adequately protect the sensitive data entrusted to them by consumers. One of the earliest large-scale retailer data breaches occurred when intruders gained access to consumers' financial information through the retailer's unsecured wireless network. While many companies have become more sophisticated over time in their security practices, we still frequently encounter situations in which companies do not comply with their own security policies, ignore security warnings, neglect to apply critical software patches, and fail to take other measures to safeguard consumers' information. The

---

[7] Alaska Stat. § 45.48.010, *et seq.*; Ariz. Rev. Stat. § 44-7501; Ark. Code § 4-110-101, *et seq.*; Cal. Civ. Code §§ 1798.29, 1789.80, *et seq.*; Colo. Rev. Stat. § 6-1-716; Conn. Gen Stat. 36a-701(b); Del. Code tit. 6, § 12B-101, *et seq.*; Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i), Ga. Code §§ 10-1-910, -911, -912; § 46-5-214; Haw. Rev. Stat. § 487N-1, *et seq.*; Idaho Stat. §§ 28-51-104 to -107; 815 Ill. Comp. Stat. 530/1 to 530/25; Ind. Code §§ 24-4.9, *et seq.*, 4-1-11, *et seq.*; Iowa Code § 715C.1, 715C.2; Kan. Stat. 50-7a01, *et seq.*; KRS § 365.732, KRS §§ 61.931 to 61.934; La. Rev. Stat. §§ 51:3071, *et seq.*, 40:1300.111 to .116; Me. Rev. Stat. tit. 10 § 1347, *et seq.*; Md. Code, Com. Law § 14-3501, *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308; Mass. Gen. Laws § 93H-1, *et seq.*; Mich. Comp. Laws §§ 445.63, 445.72; Minn. Stat. §§ 325E.61, 325E.64; Miss. Code § 75-24-29; Mo. Rev. Stat. § 407.1500; Mont. Code §§ 2-6-504, 30-14-1704,, *et seq.*; Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807; Nev. Rev. Stat. 603A.010, *et seq.*, 242.183; N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21; N.J. Stat. 56:8-161, -163; N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208; N.C. Gen. Stat §§ 75-61,75-65; N.D. Cent. Code § 51-30-01, *et seq.*; Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192; Okla. Stat. §§ 74-3113.1, 24-161 to -166; OR. Rev. Stat. § 646A.600 to .628; 73 Pa. Stat. § 2301, *et seq.*; R.I. Gen. Laws § 11-49.2-1, *et seq.*; S.C. Code § 39-1-90, 2013 H.B. 3248; Tenn. Code § 47-18-2107; Tex. Bus. & Com. Code §§ 521.002, 521.053, Tex. Ed. Code § 37.007(b)(5); Utah Code §§ 13-44-101, *et seq.*; Vt. Stat. tit. 9 § 2430, 2435; Va. Code § 18.2-186.6, § 32.1-127.1:05; Wash. Rev. Code § 19.255.010, 42.56.590; W.V. Code §§ 46A-2A-101, *et seq.*; Wis. Stat. § 134.98; Wyo. Stat. § 40-12-501, *et seq.*; D.C. Code § 28- 3851, *et seq.*; Guam Code Am. § 48-10, *et seq.*; P.R. Laws Am. Tit. 10, § 4051, *et seq.*; V.I. Code tit. 14, § 2208; *see* State Security Breach Notification Laws, Nat'l Conference Of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Jan. 12, 2015).

weaknesses generated by companies' poor security practices are inevitably exploited by cybercriminals, putting consumers' personal information at risk.

It is also important to remember that not all data breaches are the result of third-party hacks. According to Experian, the nation's largest credit reporting agency, "[e]mployees and negligence are the leading cause of security incidents."[8] Similarly, a 2013 Ponemon Institute study found that "[e]mployee or contractor negligence and system error or malfunctions are the two primary types of data and security breach incidents experienced by organizations," whereas "[m]alicious insiders and external attacks (exfiltration) are less prevalent."[9]

These findings mirror our own observations. Our offices regularly receive reports that companies have improperly disposed of consumers' information, lost files, or disclosed data through inadvertence or carelessness. For example, a recent data breach at a large multinational bank occurred because the company misplaced two unencrypted computer server backup tapes, potentially exposing consumers' most personal information, including names, addresses, Social Security numbers, and account numbers. The Attorney General of North Carolina reports that as of April 7, 2015, of the 2,583 data breaches reported to his office,[10] the most cited reason for a breach occurring was the accidental release or display of personal information. Many of these types of breaches could have been easily prevented if the businesses had taken reasonable steps to secure consumers' data.

Federal Law Should Not Preempt State Law

State attorneys general are on the front lines responding to data breaches. Our offices hear directly from affected consumers, and we regularly respond directly to their complaints and calls. For example, the Office of the Illinois Attorney General has helped over 38,000 Illinois residents remove more than $27 million in unauthorized charges from their accounts. Any federal legislation on data breach notification and data security should recognize this important role and not hinder states that are helping their residents. Preempting state law would make consumers less protected than they are right now. Our constituents are continually asking for greater protection. If states are limited by federal legislation, we will be unable to respond to their concerns.

Toward that end, it is important that any federal legislation ensure that states can continue to enforce breach notification requirements under their own state laws. States should also be assured continued flexibility to adapt their state laws to respond to changes in technology and data collection. As we have seen over the past decade, states are better equipped to quickly adjust to the challenges presented by a data-driven economy. States have been able to amend their laws and focus their enforcement efforts on those areas most affecting consumers.

---

[8] Experian Data Breach Resolution, 2015 Second Annual Data Breach Industry Forecast, 6, http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182.

[9] Ponemon Institute, The Post Breach Boom, 2, (Feb. 2013).

[10] Does not represent all breaches because some may not be reported to Attorney General's Office; also, does not include numbers affected by some breaches where that information has not been provided.

Placing enforcement authority and regulatory authority with the federal government would hamper the effectiveness of the federal law, especially with respect to data breach notification and data security. Too many breaches occur for any one agency to respond effectively to all of them. Some breaches will be too small to be a priority at the federal level, yet such breaches could have a large impact in a particular state or region. State attorneys general must have the authority to investigate such breaches, and they should be able to continue to require notification to their offices. A federal agency cannot be tasked with receiving notification for every breach that occurs in the country. While such notification at the federal level may work for large breaches that affect consumers nationwide, it does not work for breaches that affect one state or one region. Many breaches are significant, but not nationwide in their scope. A better solution to the problem is for state attorneys general to also be given timely notification of breaches, as many state laws already require.

States should also be able to maintain their ability to place requirements on data collectors that go beyond those required at the federal level. With the increasing speed rate of technological developments, states are in a better position to respond when needed, just as they have done over the past decade.

Conclusion

To ensure that any federal data breach notification law is effective and consumers are afforded the best protection, it is crucial that state attorneys general maintain their enforcement authority under their states' laws, and that any legislation be tailored to ensure complementary enforcement authority. As you and your colleagues debate these issues, we hope you take into consideration the comments we have provided here. Through our work on data breach investigations we understand the complexity of these issues and want to ensure that the progress made at the state level is not lost.

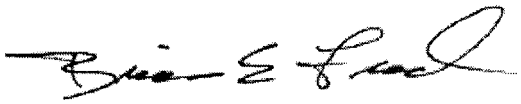
Sincerely,

Leslie Rutledge
Arkansas Attorney General

George Jepsen
Connecticut Attorney General

Lisa Madigan
Illinois Attorney General

Greg Zoeller
Indiana Attorney General



Brian Frosh
Maryland Attorney General

Maura Healey
Massachusetts Attorney General

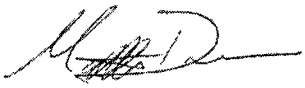
Douglas Peterson
Nebraska Attorney General

Luther Strange
Alabama Attorney General

Craig W. Richards
Alaska Attorney General

Mark Brnovich
Arizona Attorney General

Kamala Harris
California Attorney General



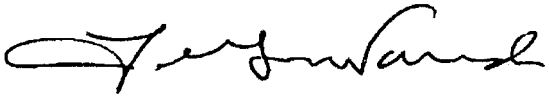
Matthew Denn
Delaware Attorney General

Karl A. Racine
District of Columbia Attorney General

Pamela Jo Bondi
Florida Attorney General

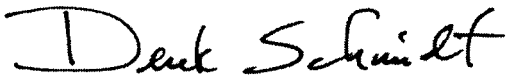
Samuel S. Olens
Georgia Attorney General

Doug Chin
Hawaii Attorney General

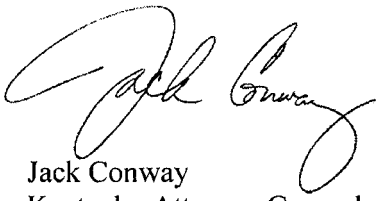


Lawrence Wasden
Idaho Attorney General

Tom Miller
Iowa Attorney General

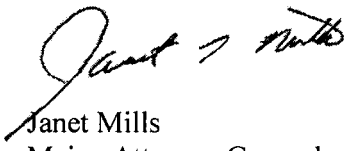


Derek Schmidt
Kansas Attorney General



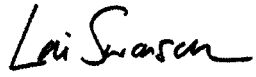
Jack Conway
Kentucky Attorney General

James "Buddy" Caldwell
Louisiana Attorney General

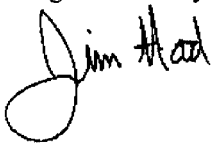


Janet Mills
Maine Attorney General

Bill Schuette
Michigan Attorney General



Lori Swanson
Minnesota Attorney General

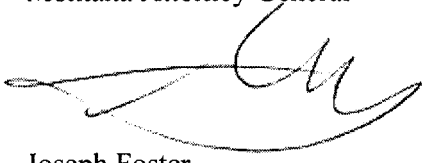


Jim Hood
Mississippi Attorney General

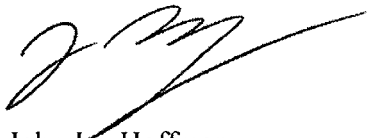
Chris Koster
Missouri Attorney General

Tim Fox
Montana Attorney General

Adam Paul Laxalt
Nevada Attorney General

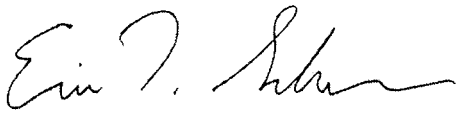


Joseph Foster
New Hampshire Attorney General



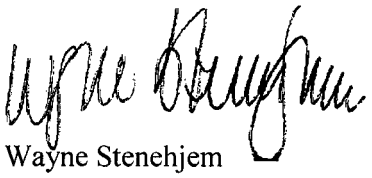
John Jay Hoffman
Acting New Jersey Attorney General

Hector Balderas
New Mexico Attorney General

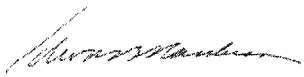


Eric Schneiderman
New York Attorney General

Roy Cooper
North Carolina Attorney General

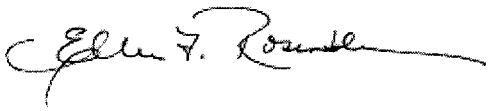


Wayne Stenehjem
North Dakota Attorney General

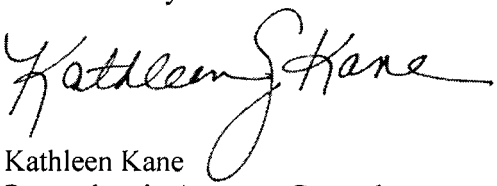


Edward Manibusan
Northern Mariana Islands Attorney General

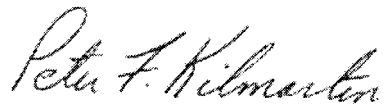
Mike DeWine
Ohio Attorney General



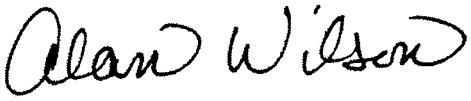
Ellen F. Rosenblum
Oregon Attorney General



Kathleen Kane
Pennsylvania Attorney General

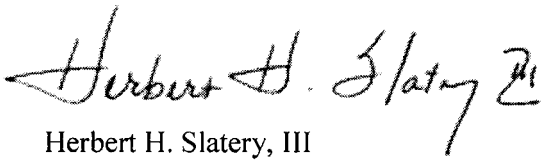


Peter F. Kilmartin
Rhode Island Attorney General



Alan Wilson
South Carolina Attorney General

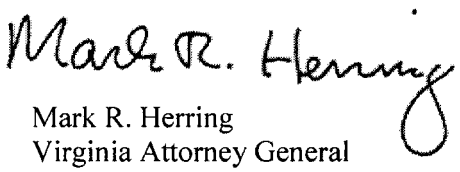
Marty J. Jackley
South Dakota Attorney General



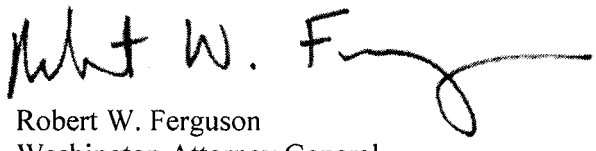
Herbert H. Slatery, III
Tennessee Attorney General

Sean Reyes
Utah Attorney General

William H. Sorrell
Vermont Attorney General



Mark R. Herring
Virginia Attorney General



Robert W. Ferguson
Washington Attorney General