NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Steve DelBianco, Executive Director
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7482
www.netchoice.org

February 4, 2014

Rep. Eliseo Lee Alcon, Chair
Consumer & Public Affairs Committee
Room 315
Santa Fe, NM 87501

RE: ***Opposition to HB 224 – Creating the Data Breach Notification Act***

Dear Chairman Alcon:

We encourage you to replace HB 224 with a data breach notification model adopted by the Council of State Governments (CSG), the American Legislative Exchange Council (ALEC), and dozens of other states.

As currently written, HB 224 puts New Mexico at odds with existing laws in 46 states in: definitions, deadlines, and details.

Industry has for years worked with legislatures and attorneys general to protect consumer information and provide breach notifications. However, HB 224 imposes a new patchwork of notification mandates that is unworkable for industry and unhelpful to New Mexico residents.

HB 224's 10 day notice requirement may desensitize New Mexico consumers to breach notices

HB 224 could force businesses to send a breach notice before completing their investigation of the size and scope of the breach – especially when they face a $150,000 fine, $300 per violation civil statutory damages, and a very short window within which to make notifications. This means that consumers across New Mexico might receive breach notices even when their information was not compromised or there is no reasonable possibility that misuse will occur.

This over notification lessens the impact of breach notices when information was compromised and when there is a reasonable possibility of misuse.

HB 224 puts New Mexico at odds with other state data breach laws

Data breaches are rarely limited to records of residents of only one state. This means that businesses must look to data breach laws from 46 states and ensure compliance with each. And as a practical matter, notice for one state pretty much requires notice for all states.

If you pass HB 224, businesses could be forced to give premature notice to customers in all states, even customers whose state laws require us to wait for law enforcement to give the go-ahead. For example,

California requires that breach notification "shall be made after the law enforcement agency determines that it will not compromise the investigation."[1]

This places businesses in a dilemma, forcing them to choose between violating HB 224 or another state's data breach law.

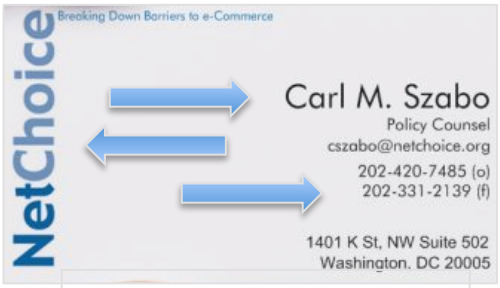
We urge you not to add yet another thread to the patchwork of state data breach laws.

HB 224 creates an unworkable new standard for notification

HB 224 creates a new definition for "personally identifiable information" (PII) that overly complicates notification of New Mexico residents by drastically expanding the nationally accepted definition.

For example, HB 224 makes "place of employment" PII thus requiring an employer to shred old business cards of New Mexico employees. Likewise, HB 224 adds "telephone number" to PII requiring businesses to shred old telephone books that include New Mexico residents.

Likely the authors did not intend this, however, this is the outcome if you pass HB 224 in its present form.



Falls under HB 224's Definition of Personal information

Please replace HB 224 with the data breach notification model adopted by CSG, ALEC, and dozens of other states

As you know, New Mexico does not yet have a data breach notification law. But rather than creating the problems discussed above, we suggest replacing HB 224 with CSG and ALEC's model data breach language.

This model, attached, creates effective data breach notification. It has been adopted by dozens of states and effectively balances requirements for breach notification with the threat of impeding investigations and over notifying consumers.

We appreciate your consideration of our views, and please let us know if we can provide further information.

Sincerely,

Steve DelBianco
Executive Director, NetChoice

Carl M. Szabo
Policy Counsel, NetChoice

NetChoice is a trade association of e-Commerce businesses. www.netchoice.org

cc: members of Consumer & Public Affairs Committee

[1] Cal. Civ. Code § 1798.29, 1798.80 et seq.

The Council of State Governments Suggested State Legislation

Computer Security Breaches

This Act is designed to help ensure that personal information about state residents is protected by encouraging data brokers to provide reasonable security for personal information. This bill borrows from a similar California statute which requires companies to notify residents in the event of a security breach involving personal financial data.

This bill requires an individual or a commercial entity that conducts business in the state and that owns or licenses computerized data that includes personal information to notify a resident of the state of any breach of the security of the system immediately following the discovery of a breach in the security of personal information of the state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notification must be made in good faith, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

The law incorporates alternative notification procedures and in a civil action to recover damages (for example, losses due to identity theft), the award is triple the amount of actual damages plus reasonable attorney fees.

Submitted as:
Delaware
HB 116
Status: Enacted into law in 2005.

Suggested State Legislation

(Title, enacting clause, etc.)

Section 1. [Short Title.] This Act may be cited as "An Act to Address Computer Security Breaches."

Section 2. [Definitions.] As used in this Act:

(1) "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;

(2) “Commercial entity” includes corporations, business trusts, estates, trusts, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit;

(3) “Personal information” means a resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

(a) Social Security number;
(b) driver's license number or state Identification Card number; or
(c) account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

The term “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records;

(4) “Notice” means:

(a) written notice;
(b) telephonic notice;
(c) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in §7001 of Title 15 of the United States Code; or
(d) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed [$75,000], or that the affected class of state residents to be notified exceeds [100,000] residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

(I) e-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of state residents; and

(II) conspicuous posting of the notice on the Web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and

(III) notice to major statewide media.

Section 3. [Disclosure of Breach of Security of Computerized Personal Information by an Individual or a Commercial Entity.]

(1) An individual or a commercial entity that conducts business in this state and that owns or licenses computerized data that includes personal information about a resident of this state shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a state resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected state resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(2) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

(3) Notice required by this Act may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this Act must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

Section 4. [Procedures Deemed in Compliance with Security Breach Requirements.]

(1) Under this Act, an individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this Act is deemed to be in compliance with the notice requirements of this Act if the individual or the commercial entity notifies affected state residents in accordance with its policies in the event of a breach of security of the system.

(2) Under this Act, an individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this Act if the individual or the commercial entity notifies affected state residents in accordance with the maintained procedures when a breach occurs.

Section 5. [Violations.] Pursuant to the enforcement duties and powers of the [Consumer Protection Division of the Department of Justice] under [insert citation], the [Attorney General] may bring an action in law or equity to address violations of this Act and for other relief that may be appropriate to ensure proper compliance with this Act or to recover direct economic damages resulting from a violation, or both. The provisions of this Act are not exclusive and do not relieve

an individual or a commercial entity subject to this Act from compliance with all other applicable provisions of law.

Section 6. [Severability.] [Insert severability clause.]

Section 7. [Repealer.] [Insert repealer clause.]

Section 8. [Effective Date.] [Insert effective date.