Senate Committees on Government Operations and
Commerce and Consumer Protection
Hawaii State Capitol, Room 229
February 6, 2015; 10:00 AM

LATE

Written Testimony of Jim Halpert
on behalf of the
State Privacy and Security Coalition, Inc.

RE: SB 1186 - Relating to Personal Information – Requesting Amendments

Dear Chairs Dela Cruz and Baker, Vice Chairs Nishihara and Taniguchi and Members of the Committees:

Thank you very much for the opportunity to testify on Senate Bill 1186 Relating to Personal Information.

The State Privacy & Security Coalition is comprised of 25 major technology and media companies and 6 trade associations representing companies in the technology, media and advetising sectors. We have worked actively on nearly all of the 47 breach notice laws, and we share your goal of informing consumers about breaches that create a risk of identity theft or fraud.

To improve this bill, we have three requested changes:

1. On page 1, line 11, we propose inserting "in combination with any required" after "credit or debit card," to clarify that notice is not required when a credit card number alone is breached. Without additional information, such as an access code or expiration date, credit card numbers cannot be processed, even if the cardholder's name has also been breached. Therefore, name + credit card number poses no risk of harm to consumers.

2. On page 2, line 5, we propose deleting ", or any information in an individual's application and claims history, including any records of appeal." "Information related to" an application or claims history is vague and overbroad. It would include any information on the form, including information that is already covered under the personal information definition (e.g., name) and information in the public domain (e.g., date of birth and address) that poses no risk of identity theft or fraud.

3. Finally, on page 3, line 1, we propose inserting: "In the case of a security breach involving personal information defined in Section 487N-1(6), the business or government agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the business or government agency and all other online accounts for which the person whose

personal information has been breached uses the same user name or email address and password or security question or answer."

For email account and password breaches, this language would be far more helpful to consumers and is better for online security than the notice currently required in the bill. Notice to the state resident quickly to stop using the password at this account and all other accounts where the state resident uses it is the optimal security step to take in the case of a password breach. In fact, it reflects best practices. It is also consistent with California's breach notice law, which was the first to include username/password in its law. *See* Cal. Civ. Code § 1798.82(d)(4).

By contrast, the notice that is required for breach of other data elements in the bill is far less useful and would do nothing to solve the security problem posed by breaches of user name or email address and password or security question and answer. Warning users to check accounts for fraud would in almost all cases be superfluous because the breach of a non-financial account does not create a risk of fraud against the state resident. However, this sort of breach does create a risk that the resident's online account will be hijacked to launch of cyber attack or to attempt to defraud other Internet users. These risks would in no way be addressed by checking the state resident's credit accounts, but would be solved by the state resident ceasing to use the same password or other authenticator to the extent that they are for non-financial accounts.

Please feel free to contact us if you have any questions or would like to discuss our concerns in greater detail. We thank you for addressing this important issue and would be happy to assist as the bill moves forward.

Respectfully submitted,

James J. Halpert
General Counsel

500 8th Street NW
Washington, DC 20005
(202) 799-4000
Jim.Halpert@dlapiper.com

THE SENATE
TWENTY-EIGHTH LESIGLATURE, 2015
STATE OF HAWAII

S.B. NO. 1186

A BILL FOR AN ACT

RELATING TO PERSONAL INFORMATION.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. Section 487N-1, Hawaii Revised Statutes, is amended by amending the definition of "personal information" to read as follows:

""Personal information" means 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 elements are not encrypted:

(1) Social security number;

(2) Driver's license number or Hawaii identification card number; [~~or~~]

(3) Account number, credit or debit card number, in combination with any required[1] access code, or password that would permit access to an individual's financial account[~~.~~];

[1] Payment card number without expiration date cannot be used to engage in a fraudulent payment card transactions. Furthermore, name plus payment card data with or without security code is not enough to commit ID theft without a government ID number.

(4) Medical information, including but not limited to any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a qualified health care professional;

(5) Health insurance information, including but not limited to an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify an individual~~, or any information in an individual's application and claims history, including any records of appeal~~;[2] or

(6) An online user name, email address, or social media user name or other identifier of a social media account that when used in combination with a password or security question and answer would permit access to an online account.

[2] "Information related to" an application or claims history is vague and overbroad. It would include any information on the form, including information that is already covered under the personal information definition here (e.g., name) and information in the public domain (e.g., date of birth and address) that poses no risk of identity theft or fraud.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."

SECTION 2. Section 487N-2, Hawaii Revised Statutes, is amended by amending subsections (a) to (e) to read:

"(a) Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) [~~of this section~~], and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system. Notification shall be made no later than forty-five

days following the determination of the breach, unless provided otherwise in this section.

(b) Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach [~~immediately~~] no later than ten days following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c).

(c) The notice required by this section shall be delayed if a law enforcement agency informs the business or government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the business or government agency documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be

provided [~~without unreasonable delay~~] pursuant to subsection (a) or (b) after the law enforcement agency communicates to the business or government agency its determination that notice will no longer impede the investigation or jeopardize national security.

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the business or government agency to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; [~~and~~]

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports[~~.~~];

(6) If the information is possible to determine at the time the notice is provided, then any of the following:

(A) The date of the breach;

(B) The estimated or approximate date of the breach; or

(C) The range of possible dates within which the breach occurred.

(7) Whether law enforcement caused a delay in notification, if the information is possible to determine at the time the notice is provided; and

(8) If the breach exposed a civil identification card number or social security number, the contact information for major credit reporting agencies.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:

(1) Written notice to the last available address the business or government agency has on record;

(2) Electronic mail notice, for those persons for whom a business or government agency has a valid electronic mail address and who have agreed to receive

communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. section 7001; provided that in the case of a security breach involving personal information including or involving the login credential of an email account, the business or government agency shall not provide notification of the breach to that email address and shall instead provide notice by another method set forth in this subsection;

(A) In the case of a security breach involving personal information defined in Section 487N-1(6), the business or government agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the business or government agency and all other online

accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.[3]

(3) Telephonic notice, provided that contact is made directly with the affected persons; and

(4) Substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds two hundred thousand, or if the business or government agency does

[3] The language we propose is far more helpful to consumers and is far better for online security than the notice currently required in the bill for email account and password breaches. Notice to the state resident quickly to stop using the password at this account and all other accounts where the state resident uses it is the optimal security step to take in the case of a password breach. In fact, it reflects best practices. It is also consistent with California's breach notice law, which was the first to include username/password in its law. *See* Cal. Civ. Code § 1798.82(d)(4).

By contrast, the notice that is required for breach of other data elements in the bill is far less useful and would do nothing to solve the security problem posed by the breach user name or email address and password or security question and answer. Warning users to check accounts for fraud would in almost all cases be superfluous because the breach of a non-financial account does not create a risk of fraud against the state resident. However, this sort of breach does create a risk that the resident's online account will be hijacked to launch of cyber attack or to attempt to defraud other Internet users. These risks would in no way be addressed by checking the state resident's credit accounts, but would be solved by the state resident ceasing to use the same password or other authenticator to the extent that they are for non-financial accounts.

not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

(A) Electronic mail notice when the business or government agency has an electronic mail address for the subject persons;

(B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and

(C) Notification to major statewide media."

SECTION 3. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 4. This Act shall take effect on July 1, 2015.

INTRODUCED BY:_____

S.B. NO. 1186

Report Title:
Personal Information; Security Breach; Notification

Description:
Expands definition of "personal information" and establishes or amends the timeline by which a business or government agency must notify persons affected by a security breach of personal information. Specifies additional information required in notification following certain security breaches. Prohibits the use of email as a means of notification of a security breach if login credentials for email were compromised.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

EAST\90583154.3