Date of Hearing: May 5, 2014

ASSEMBLY COMMITTEE ON BANKING AND FINANCE
Roger Dickinson, Chair
AB 1710 (Dickinson & Wieckowski) – As Amended: April 24, 2014

SUBJECT: Personal information: privacy.

SUMMARY: Enhances privacy protections for sensitive personal information. Specifically, this bill:

1) Provides that a person or business that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device shall not store payment-related data, as defined, unless the person or business has and complies with a payment data retention and disposal policy that limits the amount and time that payment-related data is retained to only the amount and time required for business, legal, or regulatory purposes.

2) Provides that a person or business may not store sensitive authentication data subsequent to an authorization.

3) Prohibits storage of the following data elements: payment verification code; payment verification value; PIN verification value.

4) Prohibits retention of the primary account number unless retained in a manner consistent with the other specified requirements and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored.

5) Prohibits sending payment-related data over open public networks unless the data is encrypted using strong cryptography and security protocols or otherwise rendered indecipherable.

6) Requires a person or business to limit access to payment-related data to only those individuals whose job requires that access.

7) Exempts from the foregoing any person or business subject to Sections 6801 to 6809, inclusive, of Title 15 of the United States Code (Gramm Leach Bliley Act related to personal information) and state or federal statutes or regulations implementing those sections, if the person or business is subject to compliance oversight by a state or federal regulatory agency with respect to those sections.

8) Provides that nothing in the foregoing shall prohibit a person or business that sells goods or services to any California resident and accepts as payment a credit card, debit card, or other payment device from storing payment-related data for the sole purpose of processing ongoing or recurring payments, provided that the payment-related data is maintained in accordance with these requirements.

9) Provides that a person or business subject to the foregoing shall be liable for the reimbursement of all reasonable and actual costs of providing a notice pursuant to

subdivision (a) of Section 1798.82 and for the reasonable and actual costs of card replacement as a result of a breach, to the owner or licensee of the information.

a) If the person or business demonstrates compliance with #1-6 above at the time of the breach of security then the person or business may be excused from liability in regards to reimbursement.

10) Provides that existing personal information data security obligations apply to businesses that maintain personal information, in addition to those who own or license the information.

11) Defines "maintain" as personal information that a business maintains but does not own or license.

12) Provides that if a person or business owns or licenses computerized data in conformance with the Advanced Encryption Standard of the National Institute of Standards and Technology, Federal Information Processing Standards Publication 197, amended from time to time, then that person or business is not required to disclose a security breach of personal information.

13) Provides that in the event of a breach, in addition to notifying the owner or licensee of the data, the person or business that maintains the data shall notify persons affected by the breach, at the same time that notice is given to the owner or licensee, by United States mail if the person or business has a mailing address for the subject persons or email notice if the person or business has an email address for the subject persons. If the subject persons cannot be notified by mail or email, the person or business shall provide notice by the following methods:

a) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains an Internet Web site page, for at least 30 days; and,

b) Notification to major statewide media.

14) Provides that if the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 24 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed two kinds of personal information:

a) Social security numbers (SSNs); and,

b) Driver's license numbers.

15) Provides that a person or entity may not sell, advertise for sale, or offer to sell an individual’s SSN except where the SSN is incidental to the transaction.

a) Provides that in addition to other available remedies for a violation, a public prosecutor may bring an action to recover a civil penalty not to exceed $500 per violation.

EXISTING LAW:

1) Provides that a business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Further provides that a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

2) Requires any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information to disclose any breach of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Requires any person or business that maintains, but does not own, personal information to notify the owner or licensor of the data of any breach. Provides further that disclosure shall be made in the most expedient time possible and without unreasonable delay. [Civil Code, Section 1798.82]

3) Prohibits retailers from requesting or requiring as a condition to accepting a credit card as payment, any personal identification information related to the cardholder. Authorizes a person or entity that accepts credit cards to require, as a condition of accepting the card that the cardholder provides reasonable forms of identification, including but not limited to a driver's license or state identification card, provided that the identification is not written or recorded. [Civil Code, Section 1747.08]

4) Prohibits a person or entity from publicly posting or publicly displaying a person's SSN. Defines "publicly post" or "publicly display" to mean intentionally communicating or otherwise making available to the general public. [Civil Code Section 1798.85(a) (1)]

5) Prohibits a person or entity from doing certain things that might compromise an individual's SSN, including printing a SSN on any card required to access goods or services; requiring a person to transmit a SSN over the Internet without a secure connection or encryption; requiring a person to use his or her SSN to access an Internet website, except as specified; or printing an individual's SSN on any materials that are mailed to the individual, unless the SSN is required to be on the mailed document by state or federal law. [Civil Code Section 1798.85(a) (2)-(5)]

FISCAL EFFECT: None.

COMMENTS:

AB 1710 stems from the recent mega data breaches affecting specified retailers. Following these mega data breaches, the Assembly Banking and Finance Committee and the Assembly Judiciary Committee held an oversight hearing to discuss the current process for data breaches and how California can improve this process, titled, "Is Our Personal Data Really Safe and Secure: A Review of the Recent Data Breaches." AB 1710 addresses the issues raised at this hearing and reflects the areas of law that need clarification. The recent examples of mega data breaches

emphasized the importance of disclosure and accountability. All too often, data breaches happen and consumers receive a notice in the mail from a financial institution stating their personal information may have been breached. The consumer is not made aware where the personal information was compromised and might interpret the letter to believe the breach occurred at the financial institution. Under existing law, financial institutions are considered the owners of personal information and therefore must provide the notification, although the breach most often did not occur at a bank or credit union. AB 1710 will provide clarity to consumers because it will require the maintainers of personal information which could be a retailer to disclose to a consumer that a breach occurred and their personal information may have been breached. This allows a consumer to: 1) be proactive by contacting their financial institution and/or credit reporting agency; and, 2) have the option to not shop at a retail establishment that may not maintain personal information in a safe and secure manner.

Data Storage

Sections 1 and 2 of AB 1710, closely mirrors two previous bills that went through the legislative process. AB 779 (Jones, 2007 Legislative Year) and AB 1656 (Jones, 2008 Legislative Year) which made it to the Governor's desk (Former Governor Schwarzenegger) and vetoed. The contents of Section 1 are framed after the well-known industry standard referred to as the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a proprietary information security standard for organizations that handle cardholder information defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure through 12 requirements. Although the PCI DSS must be implemented by all entities that process, store or transmit cardholder data, formal validation of PCI DSS compliance is not mandatory for all entities. Currently both Visa and MasterCard require merchants and service providers to be validated according to the PCI DSS. Smaller merchants and service providers are not required to explicitly validate compliance with each of the controls prescribed by the PCI DSS although these organizations must still implement all controls in order to maintain safe harbor and avoid potential liability in the event of fraud associated with theft of cardholder data. A key component of PCI DSS is that organizations do not store sensitive payment cardholder information that is contained in the magnetic strip of the card. If information from the front side of the card is stored in some form, PCI DSS requires that information be protected via encryption.

According to the background report created by the Assembly Banking and Finance Committee for the oversight hearing referenced above, a report on PCI compliance, *Verizon 2014 PCI Compliance Report*, reported that 56% of U.S. businesses do not meet minimum compliance with overall PCI standards. Delving further into specific areas only 17% complied with security monitoring requirements that require detection and response when data has been breached. Furthermore, 24% were compliance with security testing requirements and 56% met standards for protecting stored sensitive data. Limiting access to personal cardholder information is described in the report as one of the “golden rules” of security, but, 71% of the organizations in Verizon’s PCI compliance index failed to adequately control access to cardholder data to the level required to be PCI compliant.

Retail data breaches of sensitive personal information continue to be a widespread and persistent problem, as shown by the recent large incidents involving the loss of over 110 million credit and debit card numbers and other consumer records. According to a Javelin Strategy and Research

report, credit card fraud has increased as much as 87% since 2010, culminating in aggregate losses of $6 billion nationwide.

According to many analysts, future data breaches may be inevitable. Sometimes these breaches are caused or exacerbated by carelessness. According to the 2014 Verizon Data Breach Investigations Report, two out of three breaches last year were accomplished simply by logging in using lost or stolen credentials. In other cases, companies are the victims of sophisticated and elaborate attacks. In either case, however, these breaches impose significant costs and risks for consumer and financial services companies, among others.

In order to minimize the risk of harm, this bill requires that businesses limit retention of payment data to the information and duration needed to conduct the transaction, and encrypt the data where it is sent over open public networks. In the event of a breach, the business would be liable for the reimbursement of all reasonable and actual costs of providing notice pursuant by the owner or licensee of that information and for the reasonable and actual cost of card replacement as a result of a breach described in that section, to the owner or licensee of the information. AB 1710 does have a provision that states if the person or business has complied with all the data storage requirements at the time of the security breach then they would not be liable for reimbursement costs.

Data Breach Notification

Existing law requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Inexplicably, the statute does not apply these same reasonable security standards to businesses that maintain but do not own or license personal information. This bill would close this loophole by extending these provisions to businesses that maintain personal information about a California resident.

Under existing law, businesses that own, license or maintain computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The exemption for "encrypted" information appears to be absolute. As long as the data is encrypted in any fashion, however negligible, no notice is required despite the potential vulnerability of the information to decryption. When the data breach law was enacted years ago, this broad "safe harbor" may have served to encourage businesses who store consumer personal information to adopt any form of encryption. Now however encryption standards have improved and this bill would instead require that the data be encrypted to a reasonable standard specified by National Institute of Standards and Technology. This is the standard recommended by the Attorney General. (*See* California Department of Justice 2012 Date Breach Report, available at http://oag.ca.gov/sites /all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf.) If a person or business that owns personal information has this standard, the person or business does not have to provide notification.

In addition, the bill seeks to speed and improve consumer notification when a breach occurs by specifying that the person or business that maintains the data shall notify persons affected by the

breach at the same time that notice is given to the owner or licensee. This notice would be either by United States mail if the person or business has a mailing address for the subject persons or email notice if the person or business has an email address for the subject persons. If the subject persons cannot be notified by mail or email, the person or business shall provide notice by the following methods: (A) conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains an Internet Web site page, for at least 30 days; and, (B) notification to major statewide media.

In addition, AB 1710 seeks to protect consumers from the harms of identity theft that typically flow from a breach of the most sensitive personal information – SSNs and driver's license numbers. Under existing law, a business that suffers a breach of this information is required to do no more than notify the affected consumers, placing all costs and responsibility on the innocent consumers to protect themselves. In the interest of consumer relations, many companies voluntarily do more, such as offering credit monitoring and other services. Nevertheless, no preventive or mitigating steps are currently required. Under this measure, the person that was the source of the breach would be required to offer appropriate identity theft prevention and mitigation services, if any are available, at no cost to the affected person for not less than 24 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed two kinds of personal information: SSNs and driver's license numbers.

SSNs

Existing law regulates the publication and dissemination of SSNs in myriad ways. Perhaps surprisingly, however, the outright sale of SSNs is not prohibited.

In response to growing concerns about identity theft, the Individual Reference Services Group (IRSG) was established in the 1990's as a self-regulatory mechanism for the industry. Composed of companies specializing in identification and location services, the IRSG in conjunction with the Federal Trade Commission developed a comprehensive set of self-regulatory principles backed by audits and government enforcement. These principles however allowed the sale of SSNs without the knowledge and permission of the data subject, in a tiered system of standards contingent on how the numbers were acquired. The IRSG dissolved shortly after passage of the federal Gramm-Leach-Bliley Act in 1999, but many data brokers continue to conform to the group's principles.

This bill would close this apparent loophole by expressly prohibiting a person or entity from selling, advertising for sale, or offering to sell an individual's SSN except where the SSN is incidental to the transaction.

Previous Legislation

AB 1656 (Jones, 2008 Legislative Year) would have prohibited specified entities that sell goods or services from storing or failing to limit access to payment related information unless a specified exception applies. Vetoed by Governor Arnold Schwarzenegger.

AB 779 (Jones, 2007 Legislative Year) would have, beginning July 1, 2008, established a set procedure to be adhered to by a person, business, or public agency that sells goods or services to

any California resident, and accepts as payment a credit card, debit card, or other payment device. Vetoed by Governor Arnold Schwarzenegger.

Double Referral
This measure was heard in Assembly Judiciary Committee and passed out with a 6-3 vote.

Recommended Amendments

This amendment clarifies that SSNs sold incidental to a larger transaction and necessary for a legitimate business purpose would not be captured under Section 6. The language referenced below was enacted in Minnesota.

1) On page 14, line 4 delete "except where the social security number is incidental to the transaction"

2) On page 14 line 5 insert: "(b) "sell" does not include the release of an individual's Social Security number if the release of the Social Security number is incidental to a larger transaction and is necessary to identify the individual in order to accomplish a legitimate business purpose. The release of a Social Security number for the purpose of marketing is not a legitimate business purpose under this section."

This amendment deletes the civil penalty provision created for the sale of SSNs. Existing penalties seem to be sufficient.

3) On page 16, delete lines 24-28

REGISTERED SUPPORT / OPPOSITION:

Support

American Civil Liberties Union (ACLU)
Consumer Attorneys of California
Consumer Federation of California (CFC)
Consumer Watchdog
Privacy Rights Clearinghouse (PRC)
1 Individual

Opposition

California Association of Licensed Investigators
California Bankers Association
California Chamber of Commerce
California Hospital Association
California Manufacturers & Technology Association
California Medical Association (CMA)
California Restaurant Association
California Retailers Association
CTIA The Wireless Association
Direct Marketing Association

MasterCard
Motion Picture Association of America
Reed Elsevier
State Privacy and Security Coalition, Inc.
TechAmerica
The Internet Association

Analysis Prepared by: Kathleen O'Malley / B. & F. / (916) 319-3081