

FINAL BILL REPORT

E2SHB 1149

C 151 L 10
Synopsis as Enacted

Brief Description: Protecting consumers from breaches of security.

Sponsors: House Committee on Financial Institutions & Insurance (originally sponsored by Representatives Williams, Roach, Simpson, Kirby, Dunshee, Nelson and Ormsby).

House Committee on Financial Institutions & Insurance
Senate Committee on Labor and Commerce & Consumer Protection

Background:

State Security Breach.

In 2005 a security breach law was enacted. The law requires any person or business to notify possibly affected persons when security is breached and unencrypted personal information is (or is reasonably believed to have been) acquired by an unauthorized person. A person or business is not required to disclose a technical breach that does not seem reasonably likely to subject customers to a risk of criminal activity.

"Personal information" is defined as an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number;
- driver's license number or Washington identification card number; or
- account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

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

The notice required must be either written, electronic, or substitute notice. If it is electronic, the notice provided must be consistent with federal law provisions regarding electronic records, including consent, record retention, and types of disclosures. Substitute notice is only allowed if: the cost of providing direct notice exceeds \$250,000; the number of persons to be notified exceeds 500,000; or there is insufficient contact information to reach the customer. Substitute notice consists of all of the following:

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

- electronic mail (e-mail) notice when the person or business has an e-mail address for the subject persons;
- conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and
- notification to major statewide media.

A customer injured by a violation of the security breach law has the right to a civil action for damages.

State Disposal of Personal Information Law.

State law places restrictions on disposal of certain types of personal. If a person or business is disposing of records containing personal financial and health information and personal identification numbers issued by a government entity, the person or business must take all reasonable steps to destroy, or arrange the destruction of, the information.

An individual injured by the failure of an entity to comply with the disposal or personal information law may sue for:

- \$200 or actual damages, whichever is greater, and costs and reasonable attorneys' fees if the failure to comply is due to negligence; or
- \$600 or three times actual damages (up to \$10,000), whichever is greater, and costs and reasonable attorneys' fees if the failure to comply is willful.

The Attorney General may bring a civil action in the name of the state for damages, injunctive relief, or both, against an entity that fails to comply with the law. The court may award damages that are the same as those awarded to individual plaintiffs.

Additional Federal and State Privacy Protections.

Federal and state health privacy laws generally include security provisions and safeguards for health information, including information relating to an individual's identity and payment information. These duties are imposed on health insurers, providers, and others in the health system.

Federal banking and insurance laws generally include security provisions and safeguards for individually identifiable health and financial information. These duties are placed on individuals and businesses in the banking community.

Payment Card Industry Security Standards Council.

The Payment Card Industry Security Standards Council (Council) is a limited liability corporation with the mission of enhancing payment account data security by fostering broad adoption of its standards for payment account security. The Council was established in 2004 by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. The Council developed the Payment Card Industry Data Security Standards (PCI DSS). According to the Council, there were six principles and requirements in developing the requirements for security management, policies, procedures, network architecture, software design and other measures:

- build and maintain a secure network;
- protect cardholder data;
- maintain a vulnerability management program;

- implement strong access control measures;
- regularly monitor and test networks; and
- maintain an information security policy.

The Council does not enforce the PCI DSS. Individual payment systems establish contractual terms and penalties for noncompliance.

Summary:

A number of definitions are created, including "account information," "breach," "businesses," "encrypted," "financial institution," "processor," and "vendor."

Businesses that process more than six million credit and debit card transactions and processors are liable to a financial institution for a failure to exercise reasonable care through encryption of account information when such failure is the proximate cause of a breach of security.

Vendors are liable to a financial institution to the extent that the damages are due to a defect in the vendor's software or equipment related to the encryption. A claim against a vendor may be limited or forestalled by another provision of law or by a contract with the financial institution.

A financial institution may recover reasonable actual costs for issuing new credit cards and debit cards to its account holders that live in Washington. If an action is brought, the prevailing party is entitled to recover its reasonable attorneys' fees and costs incurred in connection with the legal action. A trier of fact may reduce any award by any amount already recovered by a financial institution from a credit card company for the breach.

There is immunity for a business, processor, or vendor if:

- the breached account information was encrypted; and
- the business, processor, or vendor was certified compliant with security standards adopted by the Council. The compliance must have been established by an annual security assessment that occurred less than 12 months prior to breach of security.

There is nothing that prevents:

- any entity responsible for handling account information on behalf of a business or processor from being sued; or
- a business, processor, or vendor from asserting any defense including defenses of contributory or comparative negligence.

Votes on Final Passage:

House	63	31	
Senate	45	0	(Senate amended)
House	65	30	(House concurred)

Effective: July 1, 2010