# SENATE BILL REPORT
# ESHB 1078

As of April 6, 2015

**Title**: An act relating to enhancing the protection of consumer financial information.

**Brief Description**: Enhancing the protection of consumer financial information.

**Sponsors**: House Committee on Technology & Economic Development (originally sponsored by Representatives Hudgins, Morris, Robinson, Kirby, Gregerson, Stanford, Ryu, Magendanz and Pollet; by request of Attorney General).

**Brief History:** Passed House: 3/04/15, 97-0.
**Committee Activity**: Law & Justice: 3/19/15, 3/31/15 [DP-WM].
Ways & Means: 4/06/15.

## SENATE COMMITTEE ON LAW & JUSTICE

**Majority Report**: Do pass and be referred to Committee on Ways & Means.
Signed by Senators Padden, Chair; O'Ban, Vice Chair; Pedersen, Ranking Minority Member; Darneille, Kohl-Welles, Pearson and Roach.

**Staff**: Lindsay Erickson (786-7465)

## SENATE COMMITTEE ON WAYS & MEANS

**Staff**: Steve Jones (786-7440)

**Background**: Washington Security Breach Laws. Under current law, any person or business that conducts business in Washington and that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any Washington resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information

---

*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.*

maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

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:

- 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.

Any waiver of the provisions of this law is contrary to public policy, and is void and unenforceable. Any customer injured by a violation of this law may institute a civil action to recover damages.

Notification Requirements. 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 is $250,000 or greater, 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:

- email notice when the person or business has an email 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.

There are no specific requirements for the content of the notification.

Disclosure of a breach must be made in the most expedient time possible and without reasonable delay. Delayed disclosure is allowed if disclosure would impede a criminal investigation.

Washington Consumer Protection Act. The Washington Consumer Protection Act (CPA) prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. Any person who is injured in the person's business or property by a violation of the CPA may bring a civil action to enjoin further violations, to recover actual damages, or both, and may recover costs of the lawsuit, including a reasonable attorney's fee. The court may triple the amount of damages awarded, not to exceed $25,000.

The Office of the Attorney General (AGO) may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, against any person to restrain or

prevent the doing of any action prohibited by the CPA. If the AGO prevails, the office may recover costs of the action, including a reasonable attorney's fee.

Federal Health Insurance and Accountability Act. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes nationwide standards for the use, disclosure, storage, and transfer of protected health information. Entities covered by HIPAA must have a patient's authorization to use or disclose health care information, unless there is a specified exception. An entity covered under HIPAA must comply with the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 notification requirements in cases of a data breach. Under HITECH, entities that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information must, in the case of a breach of such information that is discovered by the covered entity, notify each individual who is a citizen or resident of the United States whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

Gramm-Leach Bliley Act. The Gramm-Leach Bliley Act (GLBA) of 1999 requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. Under the GLBA, a financial institution follows the requirements of the Interagency Guidelines, which establish information security standards in cases of data breach. The Interagency Guidelines state that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay.

**Summary of Bill**: Parallel changes are made to the laws governing notice of security breaches for persons and businesses – RCW 19.255.010, and laws governing notice of security breaches for agencies – RCW 42.56.590. However, the GLBA exemption and the CPA apply only to the laws regarding persons and businesses.

Protected personal information is no longer limited to computerized and unencrypted data.

The term customer is replaced with consumer. The term secured means encrypted in a manner that meets or exceeds the National Institute of Standards and Technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

Notification Requirements. Notice is not required if the breach is not reasonably likely to subject consumers to a risk of harm.

If required, notice must meet the following minimum requirements:

- is written and in plain language;

- includes the name and contact information of the reporting person or business or agency;
- lists the type of personal information breached; and
- includes toll-free telephone numbers to major credit reporting agencies if the breach exposed personal information.

If a breach results in notification to more than 500 Washington residents, the person or business that is required to issue a notification must also electronically submit a copy of the security breach notification to the Attorney General along with the number of Washington consumers affected by the breach, or an estimate if the exact number is not known.

Notification of a breach of personal information to affected consumers must be provided no more than 45 days after the breach was discovered, unless an exception applies.

Enforcement. The Attorney General may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this law. For such actions, the Legislature finds that the practices covered by this law are matters vitally affecting the public interest for the purpose of applying the CPA. Any consumer injured by a violation of this law may institute a civil action to recover damages.

Exemptions. Persons, businesses, and agencies that are covered under HIPAA and are in compliance with HIPAA notification requirements are exempt from notification requirements. Specific financial institutions that are in compliance with notification requirements under the GLBA are also exempt from notification requirements. If more than 500 residents are affected by the breach, persons, businesses, and agencies that qualify for a HIPAA exemption and financial institutions that qualify for the GLBA exemption must report the breach to the AGO.

**Appropriation**: None.

**Fiscal Note**: Available.

**Committee/Commission/Task Force Created**: No.

**Effective Date**: Ninety days after adjournment of session in which bill is passed.

**Staff Summary of Public Testimony (Law & Justice)**: PRO: This bill updates the current statute, particularly in relation to recent cyber security issues that have been in the news – Target, Home Depot, Sony, Staples, and the most recent breach of Washington-based Premera Blue Cross. Two amendments that were adopted in the House make this bill consistent with federal law as it relates to the health industry and the financial industry. This is a growing concern to residents around the state and the AGO. Data breaches can lead to identity theft and insurance fraud. The AGO receives a significant number of calls from consumers and the number-one generator of calls relates to identity theft. In many situations, the AGO cannot provide consumers with meaningful information because they have not been provided with notification from the entity that has been breached. The state's current data breach notification statute is out of date and this bill fixes many of its weaknesses.

**Persons Testifying (Law & Justice)**: PRO: Representative Hudgins, prime sponsor; Shannon Smith, AGO.

**Persons Signed in to Testify But Not Testifying:** No one.

**Staff Summary of Public Testimony (Ways & Means)**: PRO: Consumers are best protected from the breach of their personal information by the notice requirements of this bill. Under current law, encrypted data are not subject to the notice requirement; this bill removes that exemption. The Attorney General is best equipped to review the notices of data breaches. This will help consumers understand the implications and potential consequences.

**Persons Testifying (Ways & Means)**: PRO: Mary Clogston, American Assn. of Retired Persons; Shannon Smith, AGO.