# HOUSE BILL ANALYSIS

# HB 2631

***Title:*** *An act relating to the privacy of personal financial information in commercial transactions involving financial institutions and others who maintain and transfer information.*

***Brief Description:*** *Protecting privacy of personal information in commercial transactions.*

***Sponsors:*** *Representatives Bush, McIntire, Hatfield, McDonald, Constantine, Reardon, Cooper, Keiser, Murray, Wolfe, Sullivan, Kessler, Schual-Berke, Ruderman, Rockefeller, Kenney, Edmonds, Cody, Santos, Conway, Morris, Lovick, O'Brien, Kagi, Stensen, Lanz, Wood, Hurst, Poulsen, and Anderson; by request of the Attorney General.*

---

***HOUSE COMMITTEE ON FINANCIAL INSTITUTIONS & INSURANCE***

***Meeting Date:*** *January 25, 2000.*

***Bill Analysis Prepared by:*** *Charlie Gavigan (786-7340)*

---

***Background:*** *Until recently, there generally has been no clear delineation in the law regarding to what extent customer information held by financial institutions and other businesses can be used by that institution or business for transactions not initiated by the customers or shared with other private organizations.*

*Federal and State Constitutions - Both the federal and state constitutions contain a right to privacy as defined by the courts. However, this constitutional principle generally protects an individual from improper intrusion on his or her right to privacy by the government, not private organizations.*

*Federal Statutes - In addition to the recent federal financial services modernization legislation (S. 900), there are several federal statutes that deal with private financial information. These include:*

- *The Right to Privacy and Bank Secrecy Act prohibits a financial institution from sharing customer financial information with the government unless the government complies with certain legal requirements. (Although the financial institution is required to report some information, such as large cash transactions, to the government.)*
- *The Electronic Funds Transfer Act requires disclosure to consumers under what circumstances account information will be shared with others.*

- ***The Fair Credit Reporting Act regulates credit reporting agencies and generally prohibits disclosure of credit information by financial institutions and others except for customer initiated transactions and information normally provided to a credit reporting agency. Transactional and experiential data are not considered credit information under FCRA and disclosure is not prohibited under FCRA. FCRA does require that when credit information is shared with affiliates, the customer is provided with notice and an opportunity to opt out (prevent disclosure to the affiliate).***
- ***Federal credit unions, under the Federal Credit Union Act, must hold in confidence customer's personal information except to the extent it is needed to complete customer-initiated transactions or is normally reported to credit reporting agencies.***

***<u>State Statutes</u> - There are some Washington state statutes that deal with private financial information. These include:***

- ***Chapter 9.35 RCW prohibits identity theft and fraudulently obtaining financial information from a financial information repository.***
- ***The state Fair Credit Reporting Act provides similar protections as the federal FCRA.***
- ***The state Consumer Protection Act prohibits unfair and deceptive practices by businesses (as does the Federal Trade Commission Act).***

***<u>Common Law</u> - Court developed principles of contract, tort, and agency law provide consumers with some legal privacy rights regarding the use of their financial information and the sharing of that information with private organizations.***

***<u>S. 900 Title V on Privacy</u> - The federal Financial Services Modernization Act of 1999 authorizes greater affiliation of banks, insurance companies, and securities firms. While some affiliation did occur previously, it was more limited than the affiliation allowed by S. 900. Under S. 900, financial institutions and their affiliates have an affirmative duty to respect and protect the privacy of their customers' nonpublic personal information. Financial institution is defined broadly in this section of the new law to include most financial services providers. Regulatory agencies must establish standards to ensure the security and confidentiality of customer's records and information and to protect against hazards or unauthorized access to this information.***

***Every financial institution must disclose its privacy policy to new customers and re-disclose the privacy policy to customers at least annually. Before disclosing customer nonpublic personal information to a nonaffiliated third party, a financial institution must: (1) clearly and conspicuously disclose to the customer that the information may be disseminated to third parties; and (2) provide the customer with an opportunity to opt-out (not have the information released). A financial institution cannot disclose account numbers or other access numbers or codes to nonaffiliated third parties for***

*telemarketing or other marketing purposes. These restrictions do not apply to sharing information with affiliates.*

*States are authorized to provide stronger privacy protections than S. 900.*

***Summary of Bill:*** *Provisions are made to restrict the use of customers' personal and sensitive information by financial institutions and others, and to assist victims of identity theft. Information custodians must provide disclosures and a privacy policy to customers; customers must authorize (opt-in) use of sensitive information by financial institutions and others and must be allowed to opt-out of the use of more general personal information. Information custodians are restricted in how they obtain and use personal information and sensitive information. Affiliates and third parties who receive information from information custodians must keep it confidential and can only use it for the original intended purpose. Every information custodian must establish reasonable safeguards to ensure the confidentiality and safety of customers' personal and sensitive information.*

*Information custodian, personal and sensitive information - An information custodian is any entity: (1) that maintains data containing personal or sensitive information; and (2) that sells, shares or transfers that information to affiliates or third parties for other than customer-requested purposes, or uses the information for marketing purposes. Personal information is information that: (1) is provided by the customer in a commercial context; (2) is identifiable to that particular customer; and (3) pertains to finances, buying habits, business relationships, or demographic data. Sensitive information is information obtained in a commercial context that includes: credit card and account numbers, purchase amounts, identification numbers, and access codes.*

*Information that may be requested - An information custodian can request only information from the customer necessary to complete the transaction or maintain the business relationship with the customer. Requested information that is optional information must be disclosed as such and the customer be given an opportunity to not provide it.*

*Privacy policy - An information custodian must have a consumer privacy policy that discloses to existing and prospective customers the policies and practices of the information custodian regarding the use of customers' personal and sensitive information. The privacy policy must at least: (1) summarize the information custodian's responsibilities; (2) describe the rights and remedies of the customer; (3) describe to whom the customers' personal and sensitive information will be shared or sold; and (4) provide a reasonable means for the customer to review personal and sensitive information that the information custodian shares or sells and provide a reasonable process to correct inaccurate or incomplete information.*

***The information custodian must disclose the privacy policy to existing customers at least annually and when material changes in the policy occur. In addition, the privacy policy must be disclosed to existing customers within 60 days of the effective date of this act, to prospective customers within 30 days of the customer request for the policy, and at the time the business relationship is entered into for new customers. The privacy policy disclosure must be clear and conspicuous in writing and separate from other documents, posted on the website if applicable, and available for review at the information custodian's place of business.***

***<u>Disclosing personal information</u> - An information custodian can disclose a customer's personal information to affiliates and third parties only if the information custodian discloses to the customer, at the time a privacy policy is required to be provided, that the customer can prevent the personal information from being shared or sold by following a free and available procedure established by the information consultant. If the customer opts-out, marketing information must not be disclosed after 60 days and other personal information cannot be disclosed after 30 days. These restrictions do not apply to the following safe harbors: (1) customer requests to disclose information; (2) disclosures required by law; (3) disclosures required by court order; (4) completing customer requested transactions; (5) collection of bad debts or NSF checks; (6) protecting against fraud or unauthorized transactions; and (7) disclosures under the federal Fair Credit Reporting Act.***

***<u>Disclosing sensitive information</u> - An information custodian can only disclose sensitive information to affiliates and third parties for other than completing a customer requested transaction if: (1) a written notice is provided to the customer explaining the applicable information to be disclosed, the organizations who will receive the information, the purpose of the disclosure, and how long the information will be disclosable; and (2) the customer authorizes the disclosure in writing in a separate document that contains a description of the applicable information and the purpose of the disclosure. These restrictions do not apply to the safe harbors listed above.***

***<u>Remedies</u> - A violation of these privacy provisions is a violation of the Consumer Protection Act. A victim of a violation of these provisions can make a claim for $500 or actual damages, whichever is greater. The court can increase this amount up to three times actual damages or $1500, whichever is greater, if the violation is willful. A person cannot bring an action for a violation of the right to a disclosure to opt-out of the sharing of personal information unless the information custodian is notified in writing of the violation and again violates the disclosure requirement.***

***<u>Identity theft provisions</u> - Any person or business possessing information regarding potential or actual identity theft or violation of financial privacy provisions and who did business with the perpetrator of the violation must, at the victim's request, provide relevant information related to the violation. The person or business may require the victim to provide a copy of a police report and pay for the cost of providing the information. The person or business is not liable for providing the information for***

*purposes of identifying and prosecuting perpetrators of identity theft or violators of the financial privacy provisions.*

*A collection agency must apply one letter from a victim of identity theft explaining the circumstances of the disputed claims resulting from the identity theft to multiple checks that are used in the commission of identity theft. The victim must provide a copy of the police report.*

***Appropriation:*** *None.*

***Fiscal Note:*** *Requested.*

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