

SESSION OF 2006

**SUPPLEMENTAL NOTE ON HOUSE
SUBSTITUTE FOR SENATE BILL NO. 196**

As Amended by House Committee of the Whole

Brief*

House Sub. for SB 196 would enact new law by allowing for protection and restriction of the use of certain personal information and amend existing identity theft law and the Fair Credit Reporting Act. The bill also would create associated penalties and remedies for violations of the use of personal information. Specifically, the bill would create new law for the illegal possession or use of scanning devices, protections for personal identifying information and notification requirements associated with a breach of security of computerized data, allowances for the use of and protections associated with security freezes on consumer reports, and procedures for the destruction of data.

Illegal Possession or Use of Scanning Devices and Reencoders

The bill would create provisions, as part of the Kansas Criminal Code, to make it unlawful for any person to knowingly and with the intent to defraud, possess or use a scanning device to access, read, obtain, memorize or store, either temporarily or permanently, information encoded on the computer chip or magnetic strip or stripe of a payment card. The bill also would make it unlawful for the defrauding, possession, or use of a reencoder. A violation of these provisions would be a severity level 6, nonperson felony.

Personal Identifying Information; Breach of Information

The bill also would prohibit, unless required by federal law, a document that is available for public inspection or copying from containing an individual's social security number if such document contains an individual's personal information. Personal information would include the name, address, phone number, or e-mail address. These personal information requirements would not apply to

*Supplemental notes are prepared by the Legislative Research Department and do not express legislative intent. The supplemental note and fiscal note for this bill may be accessed on the Internet at <http://www.kslegislature.org>

documents recorded in the official records of any recorder of deeds of the county or to documents filed as official records of the court, including, but not limited to, the following documents of any records that when filed constitutes:

- A consensual or nonconsensual lien;
- An eviction record;
- A judgment;
- A conviction or arrest;
- A bankruptcy;
- A Secretary of State filing; or
- A professional license.

Persons, including individuals, firms, corporations, associations, partnerships, joint ventures, or other business entities would be prohibited from soliciting, requiring, or using for commercial purposes, an individual's social security number unless that number is necessary for the person's normal course of business and there is a specific use for the number that no other identifying number may be used. This provision would not apply to or limit access to documents or records that are recorded or required to be open to the public. In addition, this provision does not apply to the collection, use or release of social security numbers for the purposes of mailing documents that include social security numbers that are sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number; internal verification or administrative purposes; investigate or prevent fraud and for other purposes, including conducting background checks, conducting social or scientific research, collecting a debt, obtaining a credit report or furnishing data to a consumer reporting agency, and locating an individual who is missing; and as otherwise required by state or federal law or regulation. An individual who is aggrieved by a violation of the personal data requirements would be permitted to recover a penalty of no more than \$1,000 for each violation.

The bill also would provide a number of definitions associated with the unauthorized access and use of computerized data that compromises the security, confidentiality or integrity of personal information. The bill would define the term "security breach" as the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity

reasonably believes has caused or will cause, identity theft to any consumer. Good faith acquisition of personal information by an employee or agent of an individual or commercial entity would not be considered a breach of security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure. Notification requirements for a security breach would include:

- Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. A reasonable and prompt investigation would be required to be conducted prior to the notification to determine if personal information has been or will be misused, and if misuse has or is likely to occur, the person or entity must give notice as soon as possible to the Kansas resident.
- An individual or a commercial entity that maintains the computerized data that includes personal information, that the individual or entity does not own or license, is required to give notice to the owner or licensee of the information of any breach of security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an authorized person.
- The required notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. This required notice is to be made in good faith without unreasonable delay and as soon as possible after the agency determines that notification will no longer impede the investigation.
- An individual or entity that maintains its own notification procedures as part of its information security policy, and whose procedures are otherwise consistent with the timing requirements of this bill, would be deemed to be in compliance with the notice requirements of the bill if the individual or entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system.
- If an individual or entity that is regulated by state or federal law and maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or

guidelines establish by its primary or functional state or federal regulator, the individual or entity would be deemed to be in compliance with this bill's provisions. This provision would not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.

- If a person discovers circumstances requiring notification of more than 1,000 consumers at one time, the person would be required to notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis of the timing, distribution, and content of the notices.

The Attorney General would be empowered to bring action in law or equity to address security breach provisions and for other relief that may be appropriate. Separately, the Insurance Commissioner would have the sole authority to enforce the security breach provisions for insurance companies licensed to do business in this state who violate such provisions.

Petitions for Expungement of Arrest Records and Fees; Current Law Definition of Identity Theft; and the State Forfeiture Law

In addition to the new law which would be enacted by the bill, KSA 12-4516a would be amended to provide that a person who has been arrested as a result of being a victim of identity theft (under KSA 2005 Supp. 21-4018) that petitions the municipal court for an order of expungement would not be charged a fee for such petition. KSA 2005 Supp. 21-4018 would be amended to amend the designated penalty for identity theft (severity level 8, nonperson felony), to require that if the monetary loss to the victim or victims is more than \$100,000, identity theft would be a severity level 5, nonperson felony. Identity fraud would continue to be a severity level 8, nonperson felony. Damages or loss associated with violations of KSA 21-4018 would include, but not be limited to, attorney fees and costs incurred to repair the credit history or rating of the person whose personal identification documents were obtained and used in violation of such provisions, and to satisfy a debt, lien or other obligation incurred by the person whose personal identification documents were obtained and used in violation of such provisions.

KSA 2005 Supp. 22-2410 also would be amended to provide that no surcharge or fee could be imposed on any person filing a petition

for expungement of an arrest record with the district court who was arrested as a result of being a victim of identity theft (under KSA 2005 Supp. 21-4018) that files such petition.

The Kansas Asset and Seizure Forfeiture Act would be amended to include the violations that relate to the illegal use of scanning devices and reencoders. KSA 60-4105, would be amended to include property used or intended to be used in any manner to facilitate conduct giving rise to forfeiture, including but not limited to, any computer, computer system, computer network or any software or data owned by the defendant which is used in the commission of a violation of the scanning device and reencoder provisions of the bill.

Fair Credit Reporting Act Amendments

The Fair Credit Reporting Act would be amended to provide for security freezes on a consumer report. A consumer who is the victim of identity theft would be allowed to request a security freeze on a consumer report on the consumer's consumer report by written request and sent by certified mail, which includes a valid copy of a police report, investigative report or complaint that the consumer has filed with a law enforcement agency, and clear and proper identification, to a consumer reporting agency, at an address designated by the consumer reporting agency to receive such requests. The reporting agency would be required to place a freeze on the consumer report within five business days after receiving the written request from the consumer and proper identification, as defined by the bill's provisions. Information from the consumer report would not be allowed to be released to a third party without prior authorization from the consumer; however, a consumer reporting agency would be permitted to advise a third party that a security freeze is in effect with respect to a consumer report. Additional requirements for a security freeze would include:

- A personal identification number or password.
- The consumer reporting agency, within ten business days after the date the agency places a security freeze, is to provide the consumer with a unique personal identification number, password, or similar device to be used by the consumer when providing authorization for the access to the consumer's consumer report for a specific period of time. The agency also would be responsible to simultaneously provide to the consumer in writing the process of placing, removing and temporarily lifting a security freeze and the process for allowing access to

information from the consumer report for a specific period while the security freeze is in effect.

- A third party would be required to treat an application for credit or any other use as incomplete if a security freeze is in place and the consumer has not allowed the report to be accessed for a specified time.
- A freeze, if access has been limited, may be temporarily lifted if the consumer contacts the reporting agency and provides clear and proper identification, the unique personal identification number or password, and the proper information regarding the time period for which the report is to be available to users of the consumer's consumer report. The agency would have three business days to respond to the request.

A security freeze would not apply to a consumer report provided to a federal, state or local governmental entity, including a law enforcement agency or court; a private collection agency for the sole purpose of assisting in the collection of an existing debt of the consumer; a person or entity or the related agent or affiliate of a financial obligation in conjunction with the purposed purchase of the financial obligation or to whom the consumer has an assignment of account or contract for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument; a subsidiary or other agent or assignee to whom access has been granted for the purposes of facilitating the extension of credit; a person, for the purposes for the use of a credit report as defined in 15 U.S.C. §1681b; any person for the purposes of providing a consumer with a copy of the consumer's own report at the consumer's request; a child support enforcement agency; a consumer reporting agency that acts only as a reseller of credit information (would be required to honor any security freeze placed on the report); a check services or fraud prevention services company for the purpose of approving or processing negotiable instruments, electronic funds transfers or similar methods of payment; a deposit account information service company, for the purposes that include use only in the reviewing of a consumer request for a deposit account at the inquiring bank or financial institution, reports regarding accounts closures due to fraud, and substantial overdrafts; an employer in connection with any application for employment with the employer; any person administering a credit file monitoring subscription service to which the consumer has subscribed; or any person or entity for use in setting or adjusting a rate, adjusting a claim or underwriting for insurance

purposes.

A consumer reporting agency would not be allowed to charge a fee for placing, temporarily lifting or removing a security freeze on a consumer report.

Any person who willfully fails to comply with the security freeze provisions with respect to any consumer would be liable to that consumer in an amount equal to the sum of: actual damages sustained by the consumer as a result of the failure or damages of not less than \$100 and not more than \$1,000; or such amount of punitive damages as the court may allow; and in the case of any successful action to enforce any liability under this provision, the costs of action together with reasonable attorney's fees as determined by the court. Any person who obtains a consumer report, requests a security freeze, requests the temporary lifting of the freeze, or the removal of the freeze from a consumer reporting agency under false pretenses or in an attempt to violate federal or state law would be liable to the agency for actual damages sustained by that agency or \$1,000, whichever is greater.

Additionally, any person who is negligent in failing to comply with any requirement imposed by the security freeze provisions with respect to any consumer, is liable to that consumer in an amount equal to the sum of: any actual damages sustained by the consumer as a result of the failure; and in the case of successful action to enforce any liability, the costs of the action together with reasonable attorney's fees as determined by the court. Upon a finding of the court that an unsuccessful pleading, motion or other paper filed in connection with an action was filed in bad faith or for the purposes of harassment, the court would award to the prevailing party attorney's fees reasonable in relation to the work expended in responding to the pleading, motion, or other paper.

The following entities would not be construed to require under the provisions of the bill a security freeze on a consumer report:

- Check services or fraud prevention services company;
- Deposit account information service company;
- A consumer agency that acts as a reseller of credit information;
- Database or file which consists solely of information adverse to the interests of the consumer, including information such as

criminal record information;

- Person, to the extent the person offers fraud prevention services; or
- Any bank, savings bank, trust company, savings and loan association, credit union or any other financial institution regulated by the state or any agency of the United States.

The bill also would address the destruction of data and would require a person or business, unless otherwise required by federal law or regulation, take reasonable steps to destroy or arrange for the destruction of a customer's record within its custody or control containing personal information which is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable by any means.

Finally, the bill includes a severability provision to allow that if any provision of the act or its application to person or circumstance is held invalid, the invalidity shall not affect any other provision or application of the act which can be given effect without the invalid provision or application.

The act would become effect upon publication in the statute book. The security freeze amendments to the Fair Credit Reporting Act would become effective on January 1, 2007.

Background

The House Committee on Financial Institutions recommended the substitute bill. The substitute incorporates the contents of HB 3003 with the amendments proposed by a number of conferees. In addition, the Committee inserted language to include a provision for the destruction of data. The bill was introduced by the House Committee on Federal and State Affairs at the request of Representative Cox. The provisions of 2005 HB 2438, which amend the Fair Credit Reporting Act were incorporated in the bill, as introduced. Provisions in the original bill also incorporated identity theft provisions found in California law and the Model State Clean Credit and Identity Theft Protection Act issued by the state Public Interest Research Groups and the Consumers Union of the United States, Inc.

Representative O'Malley testified in support of the bill at the time of the Committee hearing, and noted that the bill would take a comprehensive approach to address any number of identity theft issues and is modeled after the best practices of other states. A representative of the Mid American Credit Union, Wichita, testified in support of the bill. Representatives of the Heartland Community Bankers Association, the American Council of Life Insurers, and the Kansas Association of Property and Casualty Insurance Companies and the Kansas Life and Health Insurance Association, provided neutral testimony to the Committee.

Opponents testifying in opposition to the bill as introduced included representatives of the Consumer Data Industry Association, First Data Corporation, Reed Elsevier (parent company of LexisNexis), and TransUnion. The representatives highlighted concerns that included the proposed restrictions on the use of social security numbers, the protections provided by federal law including security alerts, the restricted access to public documents, and the timing of notification for consumers of any misuse or potential misuse of consumer data that has been breached. The opponents and neutral representatives proposed a number of amendments that were incorporated into the substitute bill.

The House Committee of the Whole amended the bill to provide that the municipal court and the district court would not be allowed to charge the fee associated with petitioning for order of expungement of an arrest record, for individuals who have been arrested as a result of being a victim of identity theft.

The fiscal note prepared by the Division of the Budget on the original bill, HB 3003, does not appear to apply to the substitute bill provisions in regard to the costs estimated by the Office of Judicial Administration. The Kansas Sentencing Commission did estimate that passage of the bill would result in the need for five to ten additional beds in FY 2007 and 19 to 36 additional beds by FY 2016. A fiscal note was not prepared on the substitute bill.