Approved: Mar. 20, 2006
Date

MINUTES OF THE HOUSE FINANCIAL INSTITUTIONS COMMITTEE

The meeting was called to order by Chairman Ray Cox at 3:30 P.M. on March 15, 2006 in Room 527-S of the Capitol.

All members were present except:
Bob Grant- excused

Committee staff present:
Melissa Calderwood, Kansas Legislative Research Department
Bruce Kinzie, Revisor of Statutes Office
Patti Magathan, Committee Secretary

Conferees appearing before the committee:
Representative Ed O'Malley
Mike Welli - Mid American Credit Union

Others attending:
See attached list.

Chairman Cox opened hearings on **HB3003-Protection of certain personal information; restricting disclosure or use, and HB3008-Protection of personal information in possession of business.** He called the Committee's attention to a handout that is an overview of the bill prepared by Legislative Research Assistant, **Melissa Calderwood**. Attachment 1

The first proponent to testify was **Representative Ed O'Malley** who explained that he had been working with Chairman Cox on this bill for some time. Representative O'Malley stated that there was a clause in the bill dealing with Social Security Numbers in Court records that will be deleted. He then defined identity theft to the committee as the use of a person's identity usually for financial purposes. Most people do not know that their identity has been stolen until they apply for credit. He then summarized each section of the bill and provided the expected benefits expected from a favorable passage. Attachment 2

The second proponent was **Mike Welli** of Mid American Credit Union. Mr. Welli stated that the crime of identity theft is expensive for victims, financial institutions, and various entities that deal with client personal information. Kansas consumers have no tools other than protection of personal information available to them to prevent identity theft. This bill contains an option to freeze security with credit service bureaus rendering possession of personal data worthless to an identity thief. Attachment 3

Following a brief question and answer session, Chairman Cox explained that there were several people representing various entities that had expressed an interest in amending sections of the bill as it now stands. To expedite the process and achieve an output acceptable and in the best interest of all parties, he asked those people to stay in an informal working subcommittee setting chaired by Representatives O'Malley and Dilmore. Representative Burgess also stayed. The committee was dismissed at 4:30 P.M.

The next meeting will be Monday, March 20, 2006.

FINANCIAL INSTITUTIONS COMMITTEE
GUEST LIST

DATE: March 15, 2006

NAME	REPRESENTING
Jim Hacc	American Council of Life Insurers
Natalie Haag	Security Benefit
Patricia Lightner	ITSBC
Derek Hein	Hein Law Firm
Matt Goddard	ICBA
Mike Welli	MID AMERICAN CREDIT UNION
D. & Koch	PSWS
[redacted]	LGR
Kim Stubna	First Data Corporation
Chantele Mack	Consumer Data Industry Association
Teresa Jennings	Reed Elsevere
Evan Wilson	TransUnion
Ron Gaches	Consumer Data Industry Association
Renee Ann Lowey	KAHP

KANSAS LEGISLATIVE RESEARCH DEPARTMENT

545N-Statehouse, 300 SW 10th Ave.
Topeka, Kansas 66612-1504
(785) 296-3181 ◆ FAX (785) 296-3824

kslegres@klrd.state.ks.us http://www.kslegislature.org/klrd

March 15, 2006

To: House Committee on Fiancial Institutions

From: Melissa Calderwood, Principal Analyst

Re: Overview of 2006 HB 3003

HB 3003

In addition to the bill summary that follows, attached is a copy of the sentencing grid for non-drug offenses (Attachment 1).

Brief

HB 3003 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, and to allow for the use of and protections associated with security alerts and security freezes on consumer reports.

Illegal Possession or Use of Scanning Devices and Reencoders (Section 1)

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 without the permission of the authorized user of the payment card. The bill also would make it unlawful for the defrauding, possession, or use of a reencoder without the permission of the authorized user of the payment card from which the information is being reencoded. A violation of these provisions would be a severity level 6, nonperson felony.

Personal Identifying Information; Breach of Information (Sections 2-4)

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. 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.

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 authorized 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 or other fraud 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:

- Notification must be made in good faith, in the most expedient time possible and without reasonable 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 reasonable integrity of the computerized data system.

- 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 the information 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 provides greater protection to personal information than provided in the provisions of this bill, compliance with such state or federal law would be deemed 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.

Supreme Court Rules and State Forfeiture Law (Sections 5-9)

In addition to the new law enacted by HB 3003, current law would be amended to address rules for the state Supreme Court by requiring that on and after July 1, 2006, parties filing or submitting documents with the Kansas courts would not be allowed to include any references to an individual's social security number if such documents will be available for public inspection or copying. The Supreme Court would be required to adopt rules implementing the provisions for document protections.

KSA 2005 Supp. 21-4018, passed by the 2005 Legislature in 2005 HB 2087, would 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. 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 (Sections 10-13)

The Fair Credit Reporting Act would be amended to provide for security alerts and security freezes on a consumer report. A consumer would be permitted to place a security alert in their consumer's consumer report by making a request in writing or by telephone to a consumer credit reporting agency. The agency would be responsible for notifying a person who requests information from a consumer report if a security alert has been placed in the report, regardless of whether a full consumer report, credit score, or summary report is requested. A consumer credit reporting agency is to place a security alert in the consumer report no later than five business days after receiving a request from the consumer. The alert would then remain in place for at least 90 days and a consumer would have the right of renewal of the alert.

In addition, any person who uses information in a consumer's consumer report in connection with the approval of credit based on an application for an extension of credit, or with the purchase, lease, or rental of goods or non-credit-related services, and who receives notice of a security alert, would not be allowed to lend money, extend credit, or complete the purchase, lease, or rental of goods or non-credit services without taking reasonable steps to verify the customer's identity in order to verify that the application or purchase, lease, or rental is not the result of identity theft. The person also would be responsible for notification to the consumer by telephone if that request has been made in the consumer's security alert. If reasonable steps are taken to verify that an extension of credit is not the result of identity theft, those steps would be deemed to be in compliance with the security alert provisions. Extension of credit would not include an increase in the dollar limit of an existing open-end credit plan or any change to or review of an existing credit account.

A consumer credit reporting agency would be required to notify each consumer who has requested a security alert of the expiration date of the alert. Any agency which recklessly, willfully, or intentionally fails to place the security alert in the consumer's consumer report would be liable to the aggrieved consumer in a civil action brought in the district court for actual damages, a civil penalty in an amount not to exceed $2,500 for each violation, and reasonable attorney fees and costs of the action.

In addition, consumers 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 clear and proper identification, to a consumer reporting agency. 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. Information from the consumer report would not be allowed to be released to a third party without prior authorization from the consumer; however, a third party 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 five business days after the date of the request for a security freeze, is to provide the consumer with a unique personal identification number or password 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 replacement personal identification number or password;
- The consumer reporting agency would be required to provide the consumer, within seven days after receipt of the consumer request, with new, unique personal identification number or password to used by the consumer instead of the previously issued number or password.
- Notification to a person requesting a consumer report or score if a security freeze is in effect for the report;
- 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 proposed 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 to the purposes of facilitating the extension of credit; a person, for the purposes of prescreening as provided by the federal Fair Credit Reporting Act; a consumer reporting agency 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 (required to honor any security freeze placed on the report); a check services or fraud prevention services company; and a deposit account information service company.

A consumer reporting agency would be permitted to impose a reasonable charge, not to exceed $10, on a consumer for initially placing a security freeze on a credit report. The charge for temporarily lifting the freeze may not exceed $8 per request. On January 1 of each year, the reporting agency would be permitted to increase the charge for placing a security alert based proportionately on changes to the Consumer Price Index, with fractional charges rounded to the nearest $.25. An exception to this provision would allow a consumer who is a victim of identify theft and, upon request of the consumer reporting agency has provided the agency with a police report, or a consumer who is 62 years of age or older to be charged zero dollars by the consumer reporting agency placing the security freeze. A reporting agency would not be allowed to change official information in a consumer's file while a security freeze is in place. Agencies violating, whether negligently or intentionally, a security freeze by releasing a consumer report or credit score which has been placed under the freeze would be liable to the aggrieved consumer in civil action for actual damages, a civil penalty amount not to exceed $10,000 for each violation, and reasonable attorney fees and costs of the action.

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;
- Reseller or 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.

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.

Background

The bill was introduced by the House Committee on Federal and State Affairs at the request of Representative Ray Cox.

The provisions of 2005 HB 2438, which amend the Fair Credit Reporting Act, are incorporated into the bill. Provisions in the bill also incorporate 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.

The fiscal note prepared by the Division of the Budget was not available at the time this memorandum was created.

MSC/kal

SENTENCING RANGE - NONDRUG OFFENSES

Category →	A	B	C	D	E	F	G	H	I
Severity Level ↓	3 + Person Felonies	2 Person Felonies	1 Person & 1 Nonperson Felonies	1 Person Felony	3 + Nonperson Felonies	2 Nonperson Felonies	1 Nonperson Felony	2 + Misdemeanor	1 Misdemeanor No Record
I	653 620 592	618 586 554	285 272 258	267 253 240	246 234 221	226 214 203	203 195 184	186 176 166	165 155 147
II	493 467 442	460 438 416	216 205 194	200 190 181	184 174 165	168 160 152	154 146 138	138 131 123	123 117 109
III	247 233 221	228 216 206	107 102 96	100 94 89	92 88 82	83 79 74	77 72 68	71 66 61	61 59 55
IV	172 162 154	162 154 144	75 71 68	69 66 62	64 60 57	59 56 52	52 50 47	48 45 42	43 41 38
V	136 130 122	128 120 114	60 57 53	55 52 50	51 49 46	47 44 41	43 41 38	38 36 34	34 32 31
VI	46 43 40	41 39 37	38 36 34	36 34 32	32 30 28	29 27 25	26 24 22	21 20 19	19 18 17
VII	34 32 30	31 29 27	29 27 25	26 24 22	23 21 19	19 18 17	17 16 15	14 13 12	13 12 11
VIII	23 21 19	20 19 18	19 18 17	17 16 15	15 14 13	13 12 11	11 10 9	11 10 9	9 8 7
IX	17 16 15	15 14 13	13 12 11	13 12 11	11 10 9	10 9 8	9 8 7	8 7 6	7 6 5
X	13 12 11	12 11 10	11 10 9	10 9 8	9 8 7	8 7 6	7 6 5	7 6 5	7 6 5

Probation Terms are:
36 months recommended for felonies classified in Severity Levels 1-5
24 months recommended for felonies classified in Severity Levels 6-7
18 months (up to) for felonies classified in Severity Level 8
12 months (up to) for felonies classified in Severity Levels 9-10

Postrelease Supervision Terms are:
36 months for felonies classified in Severity Levels 1-4
24 months for felonies classified in Severity Level 5-6
12 months for felonies classified in Severity Levels 7-10

Postrelease for felonies committed before 4/20/95 are:
24 months for felonies classified in Severity Levels 1-6
12 months for felonies classified in Severity Level 7-10

LEGEND
Presumptive Probation
Border Box
Presumptive Imprisonment

(GRID: 2005 Supp 21-4704)

REP. EDWARD J. O'MALLEY JR.
STATE OF KANSAS, 24TH DISTRICT

Testimony in Support of HB 3003

Rep. Ed O'Malley
March 15, 2006

Identity theft is the fastest growing crime in America. There were over 10 million ID theft victims in the United States last year. Consumers lost $5 billion and businesses lost $48 billion due to ID theft in 2005. The average victim of ID theft will spend 607 hours and $1,495 of out-of-pocket expenses to resolve their case.

Over the last few years the Legislature has attempted to prevent identity theft by focusing on what I consider to be the "low-hanging fruit" of the ID theft debate.

We have removed social security numbers from drivers' licenses, student identification cards and insurance cards. We have also strengthened the integrity of our overall driver's license system. Tailored after the best practices of other states, HB 3003 takes a comprehensive approach to many additional ID theft issues.

Passage of HB 3003 would do the following:

1. Make the use and or possession of "skimmer" devices illegal,
2. Prohibit the use of social security numbers on any public document, unless required by federal or state law,
3. Prohibit public agencies or private entities from requesting an individual's social security number unless it is absolutely needed,
4. Require companies to notify customers if personal information was breached,
5. Increase the penalty for ID theft,
6. Enable law enforcement agencies to more easily seize computers and computer equipment used by ID thieves,
7. Allow victims of ID theft to recoup costs associated with repairing credit and restoring identity, and
8. Allow individuals to place a "security freeze" on their credit report.

I encourage the committee's favorable support for HB 3003.

STATE CAPITOL
TOPEKA, KS 66612
(785) 296-7672
o'malley@house.state.ks.us

DISTRICT ADDRESS:
4804 W. 57TH STREET
ROELAND PARK, KANSAS 66205

House Financial Institutions
Mar. 15, 2006
Attachment 2

STATEMENT OF MIKE WELLI

MIDAMERICAN CREDIT UNION, WICHITA, KANSAS

TO THE HOUSE FINANCIAL INSTITUTIONS COMMITTEE

REPRESENTATIVE RAY COX, CHAIR

REGARDING H.B. 3003

MARCH 15, 2006

Mr. Chairman and Members of the Committee, I am Mike Welli, marketing director for Mid American Credit Union in Wichita, Kansas. My credit union serves about 200 employers and 19,000 members. I would like to thank you for the opportunity to come before you today and speak in favor of H.B. 3003.

Part of my job is to educate credit union members on issues such as identity theft. The crime of identity theft is expensive for victims, and it also expensive for the financial institutions they deal with. In addition to investing in educational programs for awareness, my credit union helps its members through the process of recovering from identity theft. These programs are all provided at no cost to our members.

Getting our members to protect their personal and financial data is the first step in preventing identity theft. But no matter how careful they are, too much of their personal information is not under their control. The databases of employers, financial institutions, insurance companies, healthcare providers, data brokers, schools and even churches contain personal information that is of value to identity thieves. These entities invest significant resources in security to safeguard consumers' personal data; however, there are still opportunities for mistakes and for theft.

In 2005, CardSystems Solutions, a third-party credit card processor, put more than 40 million Visa and MasterCard holders at risk of fraud when its database was compromised, including about 300 Mid American Credit Union members. CardSystems Solutions was not even authorized by Visa or MasterCard to retain cardholders' personal data long term. The company admitted to doing so for the purpose of marketing research. In another case from last year, ChoicePoint, a data broker based in Georgia that maintains profiles of nearly every U.S. consumer, inadvertently sold personal data of 140,000 individuals to criminals posing as legitimate businesses.

What kind of tools do consumers have to protect themselves? Two options currently available to Kansans are free annual credit reports or to pay a monthly fee for a credit monitoring service. The problem is that neither of these tools can prevent identity theft. They simply inform consumers that they have become a victim. Placing a fraud alert with the credit service bureaus is another option, but it is only available to those whose identities have already been compromised.

House Financial Institutions
Mar. 15, 2006
Attachment 3

The best option for consumers to protect their identity is a security freeze with the credit service bureaus. A security freeze keeps a credit report closed until the consumer agrees to let someone view it. Without that authorization, credit-issuing companies will be told they cannot see an individual's file. At this point, most companies would not open an account for an applicant. The net effect is that a security freeze makes a consumer's personal information worthless to an identity thief.

Placing a security freeze on a credit report is now an option for all consumers in nine other states. Four additional states allow security freezes for victims of identity theft. For the benefit of Mid American Credit Union members, I believe the option should be available to all Kansans, allowing it to work as tool for preventing identity theft. H.B. 3003 would accomplish this goal.