

MINUTES OF THE HOUSE JUDICIARY COMMITTEE

The meeting was called to order by Chairman Mike O'Neal at 3:30 P.M. on March 14, 2005 in Room 313-S of the Capitol.

All members were present except:

Michael Peterson- excused  
Mike Kiegerl- excused  
Jim Ward - excused

Committee staff present:

Jerry Ann Donaldson, Kansas Legislative Research  
Jill Wolters, Office of Revisor of Statutes  
Cindy O'Neal, Committee Secretary

Conferees appearing before the committee:

Representative Ed O'Malley  
Kathy Olsen, Kansas Bankers Association  
Ron Gaches, Consumer Data Industry Association  
Mike Stewart, TransUnion  
Lana Walsh, Office of Judicial Administration  
Judge Steve Leben, 10<sup>th</sup> Judicial District, Johnson County  
Matthew Goddard, Heartland Community Bankers Association  
Will Larson, Associated General Contractors of Kansas

The hearing on **SB 145 - public court records filed on & after July 1, 2005 shall have references to individual's social security number removed or rendered unreadable**, was opened.

Representative Ed O'Malley appeared on behalf of Senator Barbara Allen who is the sponsor of the proposed bill. The bill was introduced to protect Kansans social security numbers to troth identity theft. Identity theft is a huge problem that continues to grown each year. It is most easily committed when an individual gains access to a potential victim's social security number. Court records are available to the public and may have the requirement, by either state statute or court rule, that a social security number be listed on the form. (Attachment 1)

Kathy Olsen, Kansas Bankers Association, was concerned that the proposed bill would cause unintended consequences affecting the accuracy of credit reports. Bankers rely heavily on credit reports and background checks and social security numbers are a way of confirming identity of an individual. She requested an amendment which would make court documents with social security numbers exempt from the Kansas Open Records Act, and provide a list of those legitimate business who can access the records. (Attachment 2)

Ron Gaches, Consumer Data Industry Association, supported the concept of the bill but had concerns. Also supported the Kansas Bankers Association proposed amendment. He believed that the current bill is broad and would not be in the best interest of a loan consumer. Social security numbers are the most reliable identifiers in: child support cases, credit reports, law enforcement, homeland security and employee screening. Mr. Gaches has done research and could not find any instance where court records were causing identity theft. (Attachment 3)

Mike Stewart, TransUnion, stated that many courthouses are placing their information on computers and allowing businesses to upload names, address and social security number. However, each business must be certified to get the data from the courthouse.

Lana Walsh, Office of Judicial Administration, agreed with the intent of the proposed bill and understands why records should not be open to the public. She was concerned with court clerks removing social security numbers in files that are already input into the system. She suggested that removing the social security number should be responsibility of the party filing the document and that the implementation date of the bill be delayed. (Attachment 4)

Judge Steve Leben, 10<sup>th</sup> Judicial District, Johnson County, suggested that the proposed Kansas Bankers

CONTINUATION SHEET

MINUTES OF THE House Judiciary Committee at 3:30 P.M. on March 14, 2005 in Room 313-S of the Capitol.

Association's amendment would be a big nightmare because the clerks would have to take the time to check every file. He does not believe that access to court records are causing identity theft. He suggested that the subject be an interim study. Possible solutions could be deleting section b, adopting Supreme Court rules giving the court flexibility or including the last four digits of the social security number with the rest being under seal of the court. (Attachment 5)

The hearing on SB 145 was closed.

The hearing on SB 112 - material man's liens; property of claims; property under construction, was opened.

Kathy Olsen, Kansas Bankers Association, requested the proposed bill to address the Court of Appeals decision in Mutual Savings Assoc. v Res/Com Prop, which indicates that the priority date for all subsequent lienholders under this law can be established by a contractor or subcontractor who has been paid in full and no longer has a claim on the property and that work that is not visible can establish the priority date for all other subsequent lineholders. In discussion with other interested parties, it was determined that requiring that work be visible can be problematic and agreed to strike language in the bill requiring that the work establishing the priority date for all other lineholders be visible. (Attachment 6)

Matthew Goddard, Heartland Community Bankers Association, supported the bill and proposed amendment by the Kansas Bankers Association. (Attachment 7)

Will Larson, Associated General Contractors of Kansas, appeared before the committee in opposition to the proposed bill because it allows for the alteration of lien priorities at the time of foreclosures simply because the lender did not obtain a lien prior to filing a mortgage. (Attachment 8)

The hearing on SB 112 was closed.

The committee meeting adjourned at 5:00 p.m. The next committee meeting was scheduled for March 15, 2005 at 3:30 p.m. in room 313-S.



TOPEKA

SENATE CHAMBER

March 3, 2005

BARBARA P. ALLEN  
SENATOR, EIGHTH DISTRICT  
JOHNSON COUNTY  
9851 ASH DRIVE  
OVERLAND PARK, KANSAS 66207  
(913) 648-2704  
STATE CAPITOL, ROOM 143-N  
TOPEKA, KANSAS 66612-1504  
(785) 296-7353

Mr. Chairman, Members of the Committee:

SB 145 passed the Senate 40-0 on February 24, 2005. It would require that court records of this state which are filed or submitted on and after July 1, 2005 and available for public inspection or copying shall have any references to an individual's social security number (SSN) removed or otherwise rendered unreadable.

As you know, identity theft is a huge problem that continues to grow each year. It is most easily committed when an individual gains access to a potential victim's SSN. We need to continue to be vigilant in our efforts to enhance and protect Kansans' security. Toward that end, in the last few years, this Legislature has proposed and enacted into law legislation that strengthens the security of Kansas Driver's Licenses, and prohibits the use of SSN's on Kansas Driver's licenses, health insurance cards, and university I.D. cards.

SB 145 is the next step. A similar bill was introduced late in the 2004 session, which received a huge fiscal note due to its retroactive application. This year, in an effort to reduce the fiscal note and still begin the process of removing SSN's from court records, the bill was drafted to apply only prospectively. This should greatly cut down on the fiscal note, as the expense of going through old court files and deleting past information will not be necessary. While this isn't a perfect fix, it is a great first step, and will go a long way in protecting the privacy and security of Kansans.

I am submitting with my testimony the following attachments for your review.

1. Testimony in support of SB 145 from Johnson County District Attorney Paul Morrison.
2. E-Mail from a former House colleague and attorney, Dale Sprague, sent to Senator Emler this year expressing his concern about this issue.
3. Standing Order from Rules of Practice of the U.S. District Court for the District of Kansas re Privacy Policy Regarding Personal Data Identifiers. (2003)
4. Bankruptcy Rule Amendments to Protect Privacy. (2005)
5. E-Mail from Kathy Porter, Office of Judicial Administration, dated February 3, 2004, enumerating Kansas Statutes and one Supreme Court Rule that either require or request a SSN on court documents.
6. Fiscal Note
7. K.C. Star Articles 2-22-05 and 2-23-05 re ChoicePoint national identity theft scheme

I believe you will hear testimony from an opponent of SB 145 today arguing that credit reporting agencies and data collection companies need the ability to access SSN's through court records, because a person's criminal history is a good indicator of his/her credit risk, and the SSN is the only way to truly identify

someone. In essence, they oppose the peanut of SB 145, which is to prospectively remove SSN's from court records, if those records are available for public inspection or copying.

Let me direct you to two K.C. Star newspaper articles attached to my testimony re a very recent national identity theft scheme that involved more than 3,000 Missouri and Kansas residents, among 145,000 consumers nationwide, including 60 U.S. Senators. These consumers' SSN's were sold electronically to fraud artists who had opened 50 bogus accounts with the Georgia-based ChoicePoint.

ChoicePoint is a spinoff of Equifax, one of the nation's three big credit reporting agencies, and one of the nation's largest commercial data collection companies. ChoicePoint inadvertently sold a variety of personal and financial information kept on 1635 Missourians and 1613 Kansans to criminals posing as legitimate businesses. While there was no intention to do harm, the damage was done to innocent consumers, who face risks, especially in having to repair any damage caused to their credit reports.

So what's the problem with SSN's being made available to the public? **Your personal, private information provided on documents such as court records is not-so-private.** Here's how the ChoicePoint system works:

1. **From You:** The consumer fills out a few forms exposing vital information, such as SSN (for ex., court filings.)
2. **...To Who Knows Where:** After you've given out your information, companies and government agencies can sell it to companies such as ChoicePoint, which repackage the data to make it more useful.
3. **Where It Ends Up:** The information is sold to loan officers, debt collectors, telemarketers, law offices, government, and the media.
4. **What They Get Out Of It:** Mining the data from your records, ChoicePoint says it can tell what cars you've purchased, whether you've been arrested, your credit rating, jobs you've applied for, reference checks, results of drug tests, and even your DNA!

Thank you for your time and consideration. I would appreciate your support of SB 145. It is one further step in our effort to strengthen and protect the privacy and security of Kansans' identity.

Barbara P. Allen



Senator, District 8



OFFICE OF DISTRICT ATTORNEY  
PAUL J. MORRISON, DISTRICT ATTORNEY

February 14, 2005

Senate Judiciary Committee  
STATE OF KANSAS

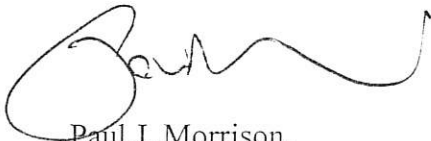
RE: Senate Bill 145

Dear Committee Members:

I wanted to write this note expressing my support for Senate Bill 145. As most of you are aware, Identity Theft is a very serious problem in our society today. This crime is most easily committed when a criminal gains access to a potential victim's Social Security number. Unfortunately, there are many places one might find that information. Oftentimes we see Social Security numbers placed in public documents inside court files. This bill would stop that practice. As it is prospective, the expense of going through old court files and deleting past information will not be necessary.

We all need to do everything possible to protect the private information of our citizens that can ultimately be used to victimize them by the unscrupulous among us. This bill goes a long way in helping achieve that end.

Sincerely,



Paul J. Morrison,  
District Attorney

:tli

**From:** Sprague Law <spraguelaw@sbcglobal.net>  
**To:** <emler@senate.state.ks.us>  
**Date:** 1/26/2005 1:34:01 PM  
**Subject:** SSN Disclosure

Jay

I've communicated a couple of times with Judge Dickinson about a concern I have regarding Domestic Relations Affidavits and required (by Supreme Court Rule and form) disclosure of a party's SSN.

Given the increase of online access it **only seems reasonable to me that Kansas Courts delete the SSN requirement from public access documents and adopt a procedure similar to that of the US Bankruptcy Courts whereby a separate, non-public pleading is filed specifically for the SSN's.**

This might make a nice little amendment to the Code of Civil Procedure to append to the right bill floating past the Senate.

Hope sanity continues for you !!

Dale

STANDING ORDER NO. 03-3. IN RE PRIVACY POLICY REGARDING PERSONAL DATA IDENTIFIERS

D.Kan. S.O. 03-3

West's Kansas Court Rules  
RULES OF PRACTICE OF THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF KANSAS  
XVI. STANDING ORDERS IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF KANSAS

*Current with amendments received through October 1, 2003.*

STANDING ORDER NO. 03-3. IN RE PRIVACY POLICY REGARDING PERSONAL DATA IDENTIFIERS

In compliance with the policy of the Judicial Conference of the United States and the E-Government Act of 2002 (Pub. L. 107-347, which was enacted on December 17, 2002), and in order to promote electronic access to case files while also protecting personal privacy and other legitimate interests, parties shall refrain from including, or shall partially redact where inclusion is necessary, the following personal data identifiers from all pleadings filed with the court, including exhibits thereto, whether filed electronically or in paper, unless otherwise ordered by the court:

- 1.) **Social Security** Numbers. If an individual's **social security** number must be included in a pleading, only the last four digits of that number shall be used.
- 2.) Names of Minor Children. If the involvement of a minor child must be mentioned, only the child's initials shall be used.
- 3.) Dates of Birth. If an individual's date of birth must be included in a pleading, only the year shall be used.
- 4.) Financial Account Numbers. If financial account numbers are relevant, only the last four digits of these numbers shall be used. The parties and counsel are solely responsible for redacting the personal data identifiers. The clerk will not review each pleading for compliance with this general order.

In addition, parties may refrain from including, or may partially redact where inclusion is necessary, the following confidential information: personal identifying numbers, such as driver's license numbers; medical records, treatment, and diagnosis; employment history; individual financial information; and proprietary or trade secret information.

In compliance with the E-Government Act of 2002, a party wishing to file a document containing the personal data identifiers or other confidential information listed above may file an unredacted document under seal. This document shall be retained by the court as part of the record. The court may, however, still require the party to file a redacted copy for the public file.

----- 2670-----

IT IS SO ORDERED.

Dated this 22nd day of April, 2003.



## Bankruptcy Rule Amendments to Protect Privacy Require Changes in Ch. 13 Trustee Procedures

By Donald F. Walton, Acting General Counsel and  
Mark Redmiles, Civil Enforcement Co-Coordinator

Over the past several years the alarming rise in identity theft, arising in part from the growing amount of personal data on individuals that is now available electronically through public sources, has prompted the federal courts to examine whether Social Security numbers should be omitted from certain publicly filed documents. One result of this examination is the amendment of Bankruptcy Rules 1005, 1007, and 2002, and the creation of Official Form 21, all of which took effect December 1, 2003. These rule changes require the United States Trustees and the Chapter 13 trustees to change certain procedures relating to debtor identification.

The changes in the Bankruptcy Rules and Official Form are as follows:

- Rule 1005 was amended to implement the Judicial Conference's privacy policy limiting disclosure of a debtor's full Social Security number (SSN) on bankruptcy petitions to only the last four digits.
- Rule 1007(f) was amended to require the debtor to "submit" a verified statement of his or her full SSN with the petition.
- New Official Form 21, which implements amended Rule 1007, requires the debtor to "submit" a statement under penalty of perjury setting forth the debtor's full SSN. Because the form is submitted but not "filed" in the case, it will not become part of the official court record or the electronic case record accessible through the Internet.
- Rule 2002(a)(1) was amended to require the Bankruptcy Clerk to include the debtor's full SSN on the Section 341 meeting notice that is sent to creditors, the U.S. Trustee, and the case trustee, but not on the Section 341 meeting notice that becomes part of the court record.

### Verification Procedures

Because a debtor's full SSN will no longer be in the public court record, certain procedures for verifying a debtor's identity must be adjusted. Under the amended Rules, U.S. Trustees and Chapter 13 trustees will receive the full SSN on the Section 341 meeting notice electronically, by mail, or by fax. The petition will contain only the last four digits, however, so during the Section 341 meeting the trustee must have access to each debtor's Section 341 meeting notice to compare it with the proof of identification and SSN presented by the debtor while under oath.

Trustees should follow their customary procedures for asking debtors to identify themselves for the record and for examining debtors' documents. A trustee should not orally recite full SSNs on the tape, because members of the public



may be present or may subsequently request a copy of the Section 341 meeting tape or transcript. Instead, the trustee should state on the record that the Social Security number listed on the Section 341 meeting notice was compared with the proof of identification and SSN presented by the debtor, and that the listed number is either accurate or inaccurate. The trustee could also have the debtor affirm on the record that the SSN contained on the Section 341 meeting notice is the debtor's SSN. The debtor should not recite his or her SSN while making this affirmation.

### Correction Procedures

Any mistake in an SSN should be corrected by instructing the debtor to submit an amended verified statement (Official Form 21) with the correct full SSN to the Bankruptcy Clerk, with notice of the correct number to all creditors, the U.S. Trustee, and the Chapter 13 trustee. The debtor should also be instructed to file with the Bankruptcy Court a truncated or redacted copy of the notice of the correct number, showing only the last four digits of the SSN, and a certificate of service. Only when a mistake occurs in the last four digits that appear on the petition should the trustee direct the debtor to file an amended petition and to notice all parties with a file-stamped copy of the amended petition.

Further, in the case of an incorrect SSN the trustee should complete the "Notice to United States Trustee of Debtor Identity Problem" (Notice) as a contemporaneous document that contains the correct and incorrect SSNs. The trustee should also follow the usual procedures for continuing the meeting and submitting to the U.S. Trustee's office a copy of the Notice on which has been indicated the SSN problem and what action needs to be taken. The Notice form should be amended, however, to indicate when the debtor needs to submit an amended Official Form 21 and (for reasons described below) to delete any reference to a notice to credit reporting agencies.

Another change in our procedures involves the notice to creditor reporting agencies. Before December 1, 2003, a trustee who found an SSN error on the petition instructed the debtor to send a "Notice of Correction of Social Security Number" to the three credit reporting agencies, with a file-stamped copy of the amended petition. This procedure was implemented to help innocent third parties whose credit reports may be affected by a bankruptcy filing. The amendments to the Bankruptcy Rules, however, limit access to full SSNs in bankruptcy cases to parties in interest who receive the Section 341 meeting notice. Therefore, credit reporting agencies and other non-parties will not receive the meeting notice that contains the full SSN, nor will they be able to obtain the full SSN on PACER.

Unless the last four digits of the debtor's SSN are incorrect, there is generally no need for Chapter 13 trustees to require or instruct debtors to send a notice to the credit reporting agencies with the correct full SSN. When appropriate, Chapter 13 trustees can seek a court order, which requires the debtor to give notice to the credit reporting agencies. Moreover, creditors may provide debtors' full SSNs and bankruptcy case information to the credit reporting agencies, and debtors may want to provide the credit reporting agencies with a Notice of Correction of SSN to ensure that debt discharge will appear on their credit file with the correct SSN.

If you have any questions about these procedural changes, please feel free to contact your U.S. Trustee district office. We will monitor these new procedures to ensure they carry out the requirements of the amended rules in a manner that is most effective and least burdensome for Chapter 13 trustees and U.S. Trustee staff.

[Back to Articles](#)

**FORM 21. STATEMENT OF SOCIAL SECURITY NUMBER**

[Caption as in Form 16A.]

STATEMENT OF SOCIAL SECURITY NUMBER(S)

1. Name of Debtor (enter Last, First, Middle): \_\_\_\_\_  
(Check the appropriate box and, if applicable, provide the required information.)

/ Debtor has a Social Security Number and it is: \_\_\_\_ - \_\_\_\_ - \_\_\_\_  
(If more than one, state all.)

/ Debtor does not have a Social Security Number.

2. Name of Joint Debtor (enter Last, First, Middle): \_\_\_\_\_  
(Check the appropriate box and, if applicable, provide the required information.)

/ Joint Debtor has a Social Security Number and it is: \_\_\_\_ - \_\_\_\_ - \_\_\_\_  
(If more than one, state all.)

/ Joint Debtor does not have a Social Security Number.

I declare under penalty of perjury that the foregoing is true and correct.

X \_\_\_\_\_  
Signature of Debtor Date

X \_\_\_\_\_  
Signature of Joint Debtor Date

\*Joint debtors must provide information for both spouses.

Penalty for making a false statement: Fine of up to \$250,000 or up to 5 years imprisonment or both. 18 U.S.C. §§ 152 and 3571.

## MEMORANDUM

To: Senator Barbara Allen  
From: Kathy Porter  
Re: Social Security Numbers on Court Documents  
Date: February 3, 2004

In response to your inquiry, Kansas statutes and one Supreme Court Rule either require or request a Social Security Number in the following instances.

K.S.A. 74-148(a) provides that a Social Security Number "shall be requested, if available, on the application" for a marriage license. However, K.S.A. 74-148(b) also states that: "[a]n agency or other body that accepts applications for . . . marriage licenses may permit the use of a Kansas driver's license number or a nondriver's identification car number on an application provided that the agency or body so advises the applicant."

K.S.A. 65-2422b provides that the "prevailing party" or the party's legal representative shall furnish information to the clerk who prepares a report of divorce to be filed with vital statistics. "The information provided shall include the social security number of both parties."

K.S.A. 59-2130 provides that a Social Security Number, if known, should be part of information provided with an adoption petition.

Current Supreme Court Rule 109, regarding supervision and reporting in probate cases, contains forms which have a space for the Social Security Number of the person under the conservatorship or guardianship.

The domestic relations affidavit filed in connection with past and current child support guidelines issued by the Supreme Court has spaces for Social Security Numbers of both the parents and the children.

K.S.A. 23-4,129 and 23-4108, concerning child support enforcement, and 39-7,136, regarding child support cases on the "state case registry," also request Social Security Numbers be provided, if known.

The current financial affidavit prescribed by the Board of Indigent Defense Services, K.A.R. 105-4-3, as per K.S.A. 22-4504(a), has a space for a Social Security Number.

In addition, other forms, such as those prepared by Judicial Council, may contain spaces for Social Security Numbers. Parties also may put these numbers on pleadings in cases, although this information is not required by statute or Supreme Court Rule.

Currently, if a Social Security Number is on these or other documents retained by the court, it can probably be obtained by going to the courthouse to look at the case file. The case file is generally a matter of public record, unless the file or documents included within it are

exceptions to the Open Records Act or unless otherwise ordered by the court. It is our understanding that court information available through the internet (*i.e.*, through the Information Network of Kansas), currently does not include access to Social Security Numbers and/or dates of birth.

In addition, some forms promulgated by the Judicial Council include spaces for the Social Security Number.

I hope this information is useful to you. If you need further information or have other questions, please feel free to contact me. My direct line is 785-296-2019.



February 14, 2005

The Honorable John Vratil, Chairperson  
Senate Committee on Judiciary  
Statehouse, Room 522-S  
Topeka, Kansas 66612

Dear Senator Vratil:

SUBJECT: Fiscal Note for SB 145 by Senate Committee on Judiciary

In accordance with KSA 75-3715a, the following fiscal note concerning SB 145 is respectfully submitted to your committee.

SB 145 would require that court records filed after July 1, 2005, and that are available for public inspection have all Social Security numbers removed or made unreadable. The Supreme Court would be required to adopt rules implementing this requirement.

The Office of Judicial Administration states SB 145 would have a fiscal effect because of the additional labor that the bill would require. The documents and the related fiscal effect would fall into three categories.

1. For documents which require a Social Security number, such as arrest warrants, the mandates of the bill would require labor intensive procedures that would increase Judiciary costs.
2. For documents containing the Social Security number that is no longer needed by the courts, it would require removing that information from the documents before they could be viewed or filed.
3. For documents that require the Social Security number and the case is pending, the procedures would be even more labor intensive, because the information would be required for the courts' use but could not be viewed by the public. One possible option

The Honorable John Vratil, Chairperson  
February 14, 2005  
Page 2—145

would be to maintain two sets of documents: one with the Social Security numbers and on without the numbers.

Sincerely,

A handwritten signature in cursive script that reads "Duane A. Goossen".

Duane A. Goossen  
Director of the Budget

cc: Brandy Wheeler, Judiciary

# Vital data swiped from thousands in Kansas, Missouri

KCS  
2-22-05

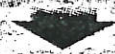
## NOT-SO-PRIVATE RECORDS

### From you ...

In today's digital, record-keeping world, you leave traces of your life everywhere.

Filling out just a few forms can expose your name, address, and other vital information, including Social Security number.

For example: birth, marriage and divorce records, school registration, court filings, property tax assessor files, professional licenses, vehicle registration, bankruptcy records, credit reports, bank records, insurance cases and demographic and lifestyle records.



### ... to who knows where

After you've given out your information, companies and government agencies can sell it to ChoicePoint and other companies, which repackage the data to make it more useful.



### Where it ends up

The information is sold to, among others, loan officers, debt collectors, telemarketers, law offices, government and the media.



### What they get out of it

Mining the data from your records, ChoicePoint says it can tell what cars you've bought, whether you've been arrested, your credit rating, jobs you've applied for, reference checks, results of drug tests, and even your DNA.

Source: Electronic Privacy Information Center and the Privacy Rights Clearinghouse

## Social Security numbers among fraud targets

By PAUL WENSKE  
The Kansas City Star

More than 3,000 Missouri and Kansas residents are among thousands of consumers whose private financial information was compromised in a national identity theft scheme.

ChoicePoint, one of the nation's largest commercial data collection companies, said Monday that a variety of personal and financial information kept on 1,635 Missourians and 1,613 Kansans was inadvertently sold to criminals posing as legitimate businesses.

Investigators have so far identified 145,000 consumers nationally whose Social Security numbers, birth dates, drivers license numbers and, in some cases, credit information were sold electronically to fraud artists who had opened 50 bogus accounts with the Georgia-based ChoicePoint.

Investigators expect the final tally of victims will grow, though they don't know how many consumers may suffer actual financial losses. Of the 145,000 victims so far, 750 have lost money, including a man whose bank account was drained of \$12,000.

The company said Monday it would offer victims free credit reports and credit-monitoring services for the next year. Victims will get a phone number and instruc-

See DATA, A-6

Go to [KansasCity.com](http://KansasCity.com) to find out what you can do to protect your credit.



# DATA: Thousands in area states affected

Continued from A-1

ons on how to contact the company and how to check their credit reports for suspicious activity. Unknown Monday night whether ChoicePoint had any financial responsibility to those whose identity was compromised. Company spokesman Chuck Wenske would say only that "ChoicePoint is a victim of this crime, but we are taking the responsibility to protect consumers."

Consumer experts said the theft might shock many Americans who are unaware of companies that track their most personal and private financial information. The database companies cater to the growing need of businesses to get consumer data quickly in deciding whether to grant loans, set interest rates and to approve car and home insurance.

"I am very concerned about the ChoicePoint incident and am looking into how it may affect Kansans and their families," said Kansas Insurance Commissioner Sandy Gaeger. Missouri officials could not be reached for comment Monday because of Presidents Day.

Consumer experts warned that thefts resulting from the breach at the company might not show up for months.

"Yes, ChoicePoint is doing the right thing to notify people, but people need to be on guard for another year or more," said Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit San Diego-based group that advocates privacy laws.

"One thing identity thieves will do is store information away until the heat is off," she said. "The crime is responsible for this theft are obviously no dummies."

ChoicePoint collects and analyzes more than 19 billion pieces of

## The details

If you're a victim of the ChoicePoint breach:

■ You will be notified by the company.

■ It will offer you free credit reports and credit-monitoring services for the next year.

■ You will get a phone number to contact the company and instructions on how to check your credit reports for suspicious activity.

■ For more about the fraud and what ChoicePoint is doing about it go to [www.choicepoint.com](http://www.choicepoint.com).

■ For more information on what consumers can do in general about identity theft, go to [www.privacyrights.org](http://www.privacyrights.org).

If you were a victim of the fraud on ChoicePoint and want to tell your story, call consumer reporter Paul Wenske at (816) 234-4454 or send e-mail to [pwenske@kcstar.com](mailto:pwenske@kcstar.com).

personal and financial data used by banks, insurers, financial businesses and government to run background checks on consumers. Businesses use the data to grant loans, screen job applicants and check credit ratings.

ChoicePoint and a few other companies such as Fair Isaac and LexisNexis prepare consumer reports for businesses. Some data is run through computer software to create credit scores, which reduce thousands of credit records to a number that reflects a consumer's credit worthiness.

They have become even more important in massaging sensitive private information on behalf of federal law enforcement and homeland security agencies, to help identify potential terrorists.

Kansas City consumer lawyer Dale Levin said that while he was shocked by the extent of the fraud, he was not surprised. "It's almost as if you don't own your own life anymore," he said.

"Your life story is in that computer. The sad fact is there is a crying need for more safeguards so it is

## First glance

■ Nationwide, personal information from about 145,000 consumers was inadvertently sold to scam artists.

■ It isn't yet known whether data-collection company ChoicePoint has any financial responsibility to those whose identity was compromised.

not as easy to get access to a person's private information."

ChoicePoint was spun off in 1997 from Equifax, one of the nation's three big credit reporting agencies. ChoicePoint reported a record \$918.7 million in revenue in 2004, up 15 percent from 2003.

In announcing the revenue report in January, chief executive Derek W. Smith said ChoicePoint was "well positioned to continue our successful track record of financial performance while helping to create a safer, more secure world through the responsible use of information."

Los Angeles investigators first uncovered hints of the theft last fall. The fraud artists apparently were able to convince the company they were legitimate businesses by using stolen and faked documents that appeared official, which they faxed to the company.

In late October, Los Angeles Sheriff's Department officials arrested a Nigerian citizen. They found a ChoicePoint service application and commercial mailbox address in his apartment.

The man, Olatunji Oluwatosin, 41, pleaded no contest to identity theft last week. He was sentenced to 16 months in state prison. Investigators still believe other people were involved.

ChoicePoint has changed the way it authorizes businesses that seek to become customers. For one thing, the company no longer allows documentation simply to be faxed to the company.

The company conceded that the fraud artists "were able to pass out customer authentication due diligence processes by using stolen identities to create and produce the documents needed to appear legitimate."

One reason the fraud was made public was that California is the only state with stiff laws requiring that residents be alerted to a security breach.

Consumer groups are urging Congress to pass national laws similar to California's.

Consumers Union has asked Congress to give consumers the right to lock up their credit file with a security freeze.

"It shouldn't be left up to a company that has had its security breached to decide which consumers to notify when sensitive information may have been compromised," said Gail Hillebrand, Consumers Union.



# States are scrutinizing breach of data security

KCS-05 58145  
 1-23  
 By PAUL WENSKE  
 The Kansas City Star

Attorneys general from Missouri and at least 18 other states want ChoicePoint to answer questions about the recent theft of financial data kept on thousands of consumers.

ChoicePoint, a large commercial data collection business, said Monday it inadvertently sold personal and financial information kept on 145,000 consumers, including 1,635 Missourians and 1,613 Kansans to criminals posing as legitimate businesses.

The company said it expected to notify all affected consumers by the end of the week and would help them take steps to safeguard their banking and credit accounts.

But Scott Holste, a spokesman for Missouri Attorney General Jay Nixon, said Tuesday that many state officials still have questions about the ramifications of the security breach. "We are working

## Worried about ID theft?

You can place a fraud alert on your credit reports by contacting any one of the three big credit reporting agencies:

- Equifax, (800) 525-6285 or [www.equifax.com](http://www.equifax.com)
- Experian, (888) 397-3742 or [www.experian.com](http://www.experian.com)
- TransUnion, (800) 680-7289 or [www.transunion.com](http://www.transunion.com)

with a multistate group of attorneys general to find out exactly what happened," Holste said.

"It is of great concern to consumer protection agencies around the country that such sensitive information was able to get into the hands of people who intended to use it for criminal activity. We want to make certain such things cannot happen again," Holste said.

ChoicePoint, formed in 1997 as a

See DATA, C-5

# DATA: Theft scrutinized by states

Continued from C-1

spinoff of Equifax, the credit reporting agency, keeps a database of 19 billion records on personal information including drivers licenses, names, addresses, Social Security numbers, property records and credit information.

Industry and consumer groups disagreed about how much risk affected consumers face. Consumer groups said consumers face risks, especially in having to repair any damage caused to their credit reports. Industry officials said current laws already protect consumers' banking, credit card and debit card accounts.

"The consumer is already protected," said John Hall, a spokesman for the American Bankers Association, the main trade group for the banking industry.

"There is an alphabet soup of protections out there," Hall said. For example, he said consumers are not liable for unauthorized charges made on their credit or debit cards. And he said federal laws require banks to cover checking accounts drained by identity

thieves.

"If it's a transaction you didn't authorize, the bank will make you whole," he said.

But Jay Foley, a spokesman for the nonprofit Identity Theft Resource Center, said his organization hears from consumers who have difficulty convincing their banks that they didn't authorize the transactions, which may have been done electronically.

"I have a large number of customers who have to fight the bank tooth and nail to get their money back," Foley said. "The banks will say, 'Well, they had your PIN number, so it had to be an authorized transaction,'" he said. "There is a serious chance of losing money."

What everyone agrees on is that the theft of personal financial information can lead to huge hassles for consumers.

"Your major concern here is you don't want someone opening new accounts in your name," said Betsy Broder, a spokeswoman for the Federal Trade Commission and an expert on identity theft. She said a consumer may not even know his or her name has been used to open

new bank, credit card and cell phone accounts until the debt collectors start calling.

It can take weeks to get your name off the bogus accounts, convince creditors you are not responsible and clear up any resulting dings on your credit report, Broder said. Even so, she said consumers should not worry needlessly.

"If you haven't got a letter in the next week or so from ChoicePoint, don't worry about it," she said. "And if you do, there are steps to take to minimize the damage."

She recommended the following:

- Talk to your banker or credit card company about putting passwords on your accounts.

- Put fraud alerts on your credit reports.

- If you are a victim of fraud you can also get a free copy of your credit report.

- If you find inaccuracies, notify the credit reporting agency and ask it to investigate.

To reach Paul Wenske, consumer affairs writer, call (816) 234-4454 or send e-mail to [pwenske@kcstar.com](mailto:pwenske@kcstar.com).





March 14, 2005

To: House Judiciary Committee

From: Kathleen Taylor Olsen, Kansas Bankers Association

**Re: SB 145: Removing SSN from Court Records**

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you today regarding **SB 145**. This bill would require that all court records remove any references to an individual's Social Security number or otherwise render the number unreadable.

It appears that an unintended consequence of this requirement would be that it would affect the accuracy of credit reports. Matching a Social Security number to an individual is the most reliable means of confirming the identity of an individual. If, in fact, not having access to the Social Security number of individuals in court documents would cause credit reports to be less accurate, KBA members would be very concerned.

Our members rely heavily on the credit reports of potential customers as an accurate representation of that person's credit history. Credit history is one of the main components in making a decision with regard to the making of a loan or the opening of a new account.

In addition, due to the nature of the industry, most banks conduct background checks when engaging in employee screening. Every bank is responsible for the safekeeping of its customers' deposits and has a duty to its shareholders to employ trustworthy individuals. It would be important for a bank to know things such as whether an individual had committed check forgery or fraud in the past, or had embezzled money from a previous employer.

While we are concerned that removing an individual's Social Security number from court records could affect the accuracy of credit reports and impair an employer's ability to conduct background checks on prospective employees, we also recognize the significant impact of identity theft on an individual's life. In weighing these important issues, we have come up with an idea for a resolution which we hope would accomplish the goal of protecting an individual's Social Security number without hampering access to that important identifying number in certain circumstances.

We would ask the Committee to consider making the Social Security numbers of individuals in court documents an exception to the Kansas Open Records Act, followed by a list of those entities and individuals who may have access to those numbers for specific purposes. There is precedence for this in K.S.A. 44-550b(a)(4). This subsection contains exceptions to the KORA for information obtained in a workers' compensation claim. In pertinent summary, that subsection provides that Social Security numbers pertaining to an individual shall not be disclosed except to a specific list of entities or individuals.

We have also attached a copy of K.S.A. 79-1437f, for analogy purposes. This statute provides that the contents of Real Estate Sales Validation Questionnaires are to be made available only to the specific individuals and entities listed and for the purposes listed therein. For example, subsection (e) states that financial institutions may access the Questionnaires for conducting appraisals and evaluations as required by federal and state regulators.

In conclusion, by making the Social Security numbers found in court documents an exception to the Kansas Open Records Act, and also providing a list of those who have a legitimate business interest for obtaining those numbers, you will be protecting the Social Security numbers of individuals from being accessed unless an identified business interest is recognized.

## Kansas Legislature

[Home](#) > [Statutes](#) > Statute

[Previous](#)

[Next](#)

### 44-550b

#### Chapter 44.--LABOR AND INDUSTRIES

#### Article 5.--WORKERS COMPENSATION

**44-550b. Records open to public inspection, exceptions.** (a) All records provided to be maintained under K.S.A. 44-550 and amendments thereto and notwithstanding the provisions of K.S.A. 45-215, et seq., and amendments thereto, shall be open to public inspection, except:

(1) Records relating to financial information submitted by an employer to qualify as a self-insurer pursuant to K.S.A. 44-532 and amendments thereto;

(2) records which relate to utilization review or peer review conducted pursuant to K.S.A. 44-510j and amendments thereto shall not be disclosed except to the health care provider and as otherwise specifically provided by the workers compensation act;

(3) records relating to private premises safety inspections;

(4) medical records, forms collected pursuant to subsection (b) of K.S.A. 44-567 and amendments thereto, accident reports maintained under K.S.A. 44-550 and amendments thereto, and social security numbers pertaining to an individual which shall not be disclosed except:

(A) Upon order of a court of competent jurisdiction;

(B) to the employer, its insurance carrier or its representative, from whom a worker seeks workers compensation benefits;

(C) to the division of workers compensation for its own purposes;

(D) to federal or state governmental agencies for purposes of fraud and abuse investigations;

(E) to an employer in connection with any application for employment to an employer, its insurance carrier or representatives providing (i) a conditional offer of employment has been made and (ii) the request for records includes a signed release by the individual, identifies the job conditionally offered by the employer and is submitted in writing, either by mail or electronic means. Requests relating to an individual under this subsection shall be considered a record to be maintained and open to public inspection under K.S.A. 44-550 and amendments thereto, except social security numbers;

(F) to the workers compensation fund for its own purposes; and

(G) to the worker upon written release by the worker.

(b) This section shall be part of and supplemental to the workers compensation act.

**History:** L. 1984, ch. 187, § 12; L. 1993, ch. 286, § 52; L. 1997, ch. 125, § 11; L. 2000, ch. 160, § 14; L. 2002, ch. 122, § 4; July 1.



## Kansas Legislature

[Home](#) > [Statutes](#) > Statute

[Previous](#)

[Next](#)

### 79-1437f

#### Chapter 79.--TAXATION

#### Article 14.--PROPERTY VALUATION, EQUALIZING ASSESSMENTS, APPRAISERS AND ASSESSMENT OF PROPERTY

##### **79-1437f. Same; disposition and use of contents thereof, to and by whom.**

Except as otherwise provided by K.S.A. 79-1460, and amendments thereto, contents of the real estate sales validation questionnaire shall be made available only to the following people for the purposes listed hereafter:

- (a) County officials for cooperating with and assisting the director of property valuation in developing the information as provided for in K.S.A. 79-1487, and amendments thereto;
- (b) any property owner, or the owner's representative, for prosecuting an appeal of the valuation of such owner's property or for determining whether to make such an appeal, but access shall be limited to the contents of those questionnaires concerning the same constitutionally prescribed subclass of property as that of such owner's property;
- (c) the county appraiser and appraisers employed by the county for the appraisal of property located within the county;
- (d) appraisers licensed or certified pursuant to K.S.A. 58-4101 *et seq.*, and amendments thereto, for appraisal of property and preparation of appraisal reports;
- (e) financial institutions for conducting appraisals and evaluations as required by federal and state regulators;
- (f) the county appraiser or the appraiser's designee, hearing officers or panels appointed pursuant to K.S.A. 79-1602 or 79-1611, and amendments thereto, and the state board of tax appeals for conducting valuation appeal proceedings;
- (g) the board of county commissioners for conducting any of the board's statutorily prescribed duties; and
- (h) the director of property valuation for conducting any of the director's statutorily prescribed duties.

**History:** L. 1991, ch. 162, § 6; L. 1992, ch. 282, § 19; L. 1999, ch. 123, § 2; L. 2002, ch. 23, § 1; July 1.



**GACHES, BRADEN, BARBEE & ASSOCIATES**  
PUBLIC AFFAIRS & ASSOCIATION MANAGEMENT

---

825 S. Kansas Avenue, Suite 500 ♦ Topeka, Kansas 66612 ♦ Phone: (785) 233-4512 ♦ Fax: (785) 233-2206

House Judiciary Committee

Hearing on SB 145 – Regarding Access to Court Records

Testimony of Consumer Data Industry Association

Presented by Ron Gaches

Gaches, Braden, Barbee and Associates

Monday, March 14, 2005



# CDIA

CONSUMER DATA INDUSTRY ASSOCIATION  
*Empowering Economic Opportunity*

Contact: Eric J. Ellman

Telephone: 202-408-7407

Email: eellman@cdiaonline.org

**Kansas S.B. 145**  
**Position: OPPOSE**

**Legislative Proposal:** The bill would prohibit access to SSNs contained in court records.

**Current Law:** Consumer reporting agencies are heavily regulated by the federal Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*) and the Kansas credit reporting law (Kansas Code § 50-701). These laws strictly regulate who can obtain access to credit reports and under what circumstances. The laws also require consumer reporting agencies to adhere to certain accuracy standards. In addition, CDIA members are also regulated by the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq.*). The GLBA is the most comprehensive federal privacy law to date.

**Reasons for Opposition:** Social Security numbers from court records are used in a variety of ways that have a great deal of benefit to society at large.

- *Accuracy of Credit Reports.* While all CDIA members manage very large databases, the largest members maintain approximately 200 million consumer reports and update 2 billion pieces of information every month. There are 14 million annual address changes in the U.S., 6 million vacation or second homes, and 3 million marriages and divorces annually with attendant name changes. In addition, 4.5 million Americans have one of two last names (Smith or Johnson), 14 million have one of ten last names, 26.6 million females have one of ten first names and 57.7 million males have one of ten first and last names. The only way to correctly match the arrest, conviction, eviction, lien or judgment with the correct consumer is through the use of all nine digits of the Social Security number.
- *Law Enforcement.* Then-FBI Director Louis Freeh testified before Congress in 1999 and noted that in 1998, his agency made more than 53,000 inquiries to commercial on-line databases “to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations.” This information, according to Director Freeh, “assisted in the arrests of 393 fugitives, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning.” This information often comes from court records.
- *Child Support Enforcement.* The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the “deadbeat parents” they sought. This information often comes from court records.
- *Homeland Security.* Background checks on pilots, flight attendants, ramp workers, and others often includes court records. Without a ready way to identify whether someone has been arrested for forging government documents, or other potential threats, there is an increased threat to homeland security.
- *Employment Screening.* Employers conducting background checks on prospective employees need to know about court record history. For example, a bus company would like to know about DWIs, a bank would want to know about any forgeries, a day care center would want to know about pedophilia.

- *Residential Screening.* Landlords and property managers conducting background checks on prospective tenants need to know about court record history, including any records of eviction, or arrests or convictions for arson, burglary, or violent crimes.
- *Judicial Administration.* According to Mike L. Buenger, President of the Conference of State Court Administrators, “Absent the use of unique identifiers such as SSNs [found in credit headers], the entire justice community would come to a grinding halt and be unable to meet many state and federal mandates. SSNs provide a unique identifier by which court personnel can determine whether the current ‘John Smith’ is the same person as a previous ‘John Smith’ who appeared in an earlier case and whether this was the same ‘John Smith’ reported to the central criminal records repository.”

**Conclusion:** This bill could sharply reduce the availability of information necessary for law enforcement, homeland security, and other important functions necessary to protect the health and safety of the general public.



**House Judiciary Committee**  
**Comments of CDIA: Opposition to Passage of SB 145**  
**Submitted by Eric Ellman, Director State Government Relations, CDIA**  
**Thursday, March 3, 2005**

**Background about CDIA**

Founded in 1906, the Consumer Data Industry Association (CDIA), formerly known as Associated Credit Bureaus, is the international trade association that represents more than 400 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

From court records CDIA members obtain information such as tax liens and releases, wage-earner proceedings, civil judgments, including releases or vacations of those judgments, and records of arrest, conviction, and eviction. Court records are also used to obtain orders of support for spouses and children. The information obtained is used to ensure a safe and sound consumer reporting system, as well as to empower landlords, residential property managers, and employers to make decisions based on full, accurate and impartial information and to provide safe environments for their residents, employees, customers, and guests.

**The Fair Credit Reporting Act**

**Consumer Reporting Agencies**

CDIA members are governed under the federal Fair Credit Reporting Act (FCRA).<sup>1</sup> This Act, adopted in 1970 and substantially amended in 1997, is a comprehensive body of regulation and represents the first national privacy law in the United States. Nearly half the states have credit reporting laws as well. Since the adoption of the FCRA three decades ago, consumer reporting agencies have been required to maintain reasonable procedures to assure maximum possible accuracy.<sup>2</sup> Consumer reporting agencies, as part of the accuracy duties imposed by the FCRA, are required to make reasonable efforts to identify new prospective users of consumer reports and the uses requested.<sup>3</sup> When a consumer reporting agency provides a consumer report for employment purposes and that report contains public record information likely to be adverse to the applicant, the consumer reporting agency must notify the consumer of that fact along with the

---

<sup>1</sup> 15 U.S.C. § 1681 *et seq.* All references to the FCRA herein are to Title 15 of the U.S. Code.

<sup>2</sup> § 1681e(b).

<sup>3</sup> § 1681e(a).



name and address of the user that is being supplied the consumer report. In addition, the consumer reporting agency must “maintain strict procedures designed” to ensure the currency of public record information.<sup>4</sup>

Consumers have a right to dispute information on their credit reports with consumer reporting agencies. The FCRA requires dispute resolution in not more than 30 days (45 days in certain circumstances).<sup>5</sup> If a dispute cannot be verified the information must be removed in the consumer’s favor.<sup>6</sup>

A consumer reporting agency that violates any provision of the FCRA is subject to private rights of action,<sup>7</sup> enforcement by the FTC,<sup>8</sup> state attorneys general,<sup>9</sup> or all three.

### **Data Furnishers**

Data furnishers are those entities that report data to consumer reporting agencies and may include financial institutions, landlords, collection agencies, the federal government and child support enforcement agencies. In addition to the accuracy standards set by the FCRA on consumer reporting agencies since 1970, data furnishers also have accuracy standards to which they must adhere as established by the 1997 amendments to the FCRA. Data furnishers are prohibited from furnishing data they know is inaccurate and they have an affirmative duty to correct and update information.<sup>10</sup> Furnishers also are liable to consumers if they continue to report data known to be inaccurate.<sup>11</sup>

### **Public Safety**

Court records obtained by CDIA members are used to determine if an applicant for a school bus driver position has been arrested for or convicted of DWI or reckless driving; if an applicant to work at a day care center is a pedophile or a registered sex offender; if a prospective tenant in an apartment building has been arrested for or convicted of a violent crime; or if a retail clerk or bank teller has liens or judgments outstanding. The court records collected by CDIA members also further vital national security interests. For example, records obtained by CDIA members are used to confirm the background and true identity of an applicant for a pilot license, a license to haul hazardous waste, a permit to fly a crop duster, to work on an airport ramp, or to work as a customs officer.

Then-FBI Director Louis Freeh testified before Congress in 1999 and noted that in 1998, his agency made more than 53,000 inquiries to commercial on-line databases “to obtain public source information regarding individuals, businesses, and organizations that are subjects of

---

<sup>4</sup> § 1681k.

<sup>5</sup> § 1681i. The majority of reinvestigations are completed in five days or less and 70% are resolved in ten days or less.

<sup>6</sup> § 1681i(a)(5).

<sup>7</sup> § 1681n-p.

<sup>8</sup> § 1681s(a).

<sup>9</sup> § 1681s(c).

<sup>10</sup> § 1681s-2.

<sup>11</sup> § 1681s-2(b). *See also Nelson v. Chase Manhattan Mortgage Corp.*, No. 00-15946 (9<sup>th</sup> Cir., March 1, 2002).

investigations.” This information, according to Director Freeh, “assisted in the arrests of 393 fugitives, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning.”<sup>12</sup> The importance of court record access cannot be understated or underestimated for public safety needs.

### **Social Security Numbers**

SB 145 proposes to eliminate access to social security numbers in court records. The only way to correctly match the arrest, conviction, eviction, lien or judgment with the correct consumer is through the use of all nine digits of the Social Security number.<sup>13</sup> Full SSN access provides benefits not just to consumer reporting agencies, but also to consumers who rely on a safe and sound credit system,<sup>14</sup> consumers who have come to expect safe working and living environments, and to governments that have an obligation to provide security and promote general welfare.

Without full SSN access consumer reporting agencies would face significant accuracy hurdles which could very well jeopardize public health, safety, and welfare. Reduced accuracy also increases the risk to financial institutions and leads to a slow erosion of safe and sound banking practices.<sup>15</sup>

---

<sup>12</sup> Senate Comm. on Appropriations Subcomm. for the Departments of Commerce, Justice, and State, and the Judiciary and Related Agencies, 106<sup>th</sup> Cong. (March 24, 1999) (Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation).

<sup>13</sup> The ability to match with more, rather than less, information is correctly stated in the commentary to § 4.40.

<sup>14</sup> A memorandum issued to CEOs under the subject “Consumer Credit Reporting Practices” from the Federal Financial Institutions Examination Council (“FFIEC”) on January 18, 2000 stated that

[t]he Agencies [Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Office of Thrift Supervision] note that both financial institutions and their customers generally have been well served by the long-established, voluntary self-reporting mechanism in place within the industry.

Additionally,

Comptroller of the Currency John Hawke, Jr. testified before Congress in 1999 that information exchanges serve a ‘useful and critical market function’ that ‘benefits consumers and businesses alike.’ Consumer credit markets provide a case in point. The current U.S. economic boom has significantly raised the standard of living for U.S. citizens through the availability of over \$5 trillion in outstanding mortgages and other consumer loans. Consumer credit finances homes and cars, funds college educations, and provides the credit cards that consumers use everyday to purchase goods and services. The ‘almost universal reporting’ of personal credit histories (under the rules of the Fair Credit Reporting Act) is, in the words of economist Walter Kitchenman, the ‘foundation’ of consumer credit in the United States and a ‘secret ingredient of the U.S. economy’s resilience.’ Studies have shown that the comprehensive credit reporting environment in this country has given U.S. consumers access to more credit, from a greater variety of sources, more quickly, and at lower cost than consumers anywhere else in the world.

Fred H. Cate, Michael E. Staten, *The Value of Information-Sharing*, The National Retail Federation’s, Protecting Privacy in the New Millennium Series (available at <http://www.netcaucus.org/books/privacy2001/>) (citations omitted).

<sup>15</sup> *Id.* (“Institutions rely heavily on such data...[and] their ability to make prudent credit decisions is enhanced by greater completeness of credit bureau files”).

While all CDIA members manage very large databases, the largest members maintain approximately 200 million consumer reports and update 2 billion pieces of information every month. There are 14 million annual address changes in the U.S., 6 million vacation or second homes, and 3 million marriages and divorces annually with attendant name changes. In addition, 4.5 million Americans have one of two last names (Smith or Johnson), 14 million have one of ten last names, 26.6 million females have one of ten first names and 57.7 million males have one of ten first and last names.

It bears repeating that the single best piece of information to correctly match the arrest, conviction, eviction, lien or judgment with the correct consumer is through the use of all nine digits of the Social Security number.

The Social Security number is *the* single universal identifier for Americans. The SSN is what allows a robust consumer reporting (and thus a vibrant credit) system, it is what allows rapid decision-making in employment and residential application situations, and it has enormous public safety uses.

On November 1, 2001, Jim Huse, Inspector General of the Social Security Administration said that “The SSN is used legitimately in so many areas of our lives that it is impossible to think that we can turn back the clock and reserve its use to tracking earnings and paying benefits, the uses for which it was originally designed.”<sup>16</sup> Six weeks later, it was noted that “[a]t least seven of the [September 11<sup>th</sup>] hijackers...obtained Virginia state ID cards, which would serve as identification to board a plane, even though they lived in Maryland motels. ‘If we can’t be sure when interacting that someone is who they purport to be, where are we?’<sup>17</sup>

The only way law enforcement, employers, security companies, and others can ever hope to sort out legitimate and non-legitimate SSN holders and track individuals across state lines is through full access to SSNs from as many disparate sources as possible, including court records.

The value of SSNs has been proven by government agencies as well to promote general welfare. Conversely, the loss of SSNs would be harmful to millions of Americans who, more than many, need the money that comes from locating individuals like delinquent parents. The Association for Children for Enforcement of Support reported that public record information provided through commercial vendors helped locate over 75 percent of the “deadbeat parents” they sought.<sup>18</sup>

One can look to the National Directory of New Hires (NDNH), heavily dependant on SSNs for matching, to illustrate the points made above. Since over 30% of child support cases involve parents who do not live in the same state as their children, creating the NDNH and matching data against it enables the federal Office of Child Support Enforcement (OCSE) to assist states in

---

<sup>16</sup> House Ways & Means Subcommittee on Social Security, 107<sup>th</sup> Cong. (Nov. 1, 2001) (testimony of: James G. Huse, Jr., Inspector General of the Social Security Administration).

<sup>17</sup> Robert O'Harrow Jr. & Jonathan Krim, *National ID Card Gaining Support*, Washington Post, Dec. 7, 2001, at A1 (quoting James Huse, Inspector General of the Social Security Administration).

<sup>18</sup> House Comm. on Banking and Financial Services, 105<sup>th</sup> Cong., (July 28, 1998) (statement of Robert Glass).



locating parents who are living in other states. Upon receipt of new hire information from other states, state child support enforcement agencies take the steps necessary to establish paternity, establish a child support order or enforce existing orders. Between October 1, 1997 and June 11, 1998, the National Directory of New Hires had just over one million matches and between 1997 and 2007 the New Hire reporting is expected to bring in over \$6.4 billion in child support.<sup>19</sup> Not only does the new hire program assist in locating delinquent parents, it also assists states in reducing unemployment and workers' compensation fraud.<sup>20</sup>

The truncation of SSNs reduces the ability to authenticate and identify. The digits in the Social Security number are sequenced such a way that the numbers and the placement in the sequence have meaning and relevance.

The Social Security number is divided into three parts: the area, group and serial numbers. The first three digits of a person's social security number, called the area, are determined by the ZIP Code of the mailing address shown on the application for a social security number. The second two digits are called the group<sup>21</sup> and the final four digits are called the serial number. Within each group, the serial numbers run consecutively from 0001 through 9999.<sup>22</sup> It is all nine digits in relation to and with each other, and not the last four that allows an effective match.

In early-2002, a CDIA member examined the 66.5 million names in the Social Security Administration's Death Master File ("DMF"), a database of SSNs assigned to now-deceased persons. The DMF pool is slightly less than one quarter (23%) the size of the total number of living Americans, which stands at 285 million. The chances that a person listed in the DMF with the same last name will share the last four digits of an SSN is better than one in ten (11.3%). It is fair to say that this statistic carries through to all 285 million Americans who have a last name in common with someone else. This statistic is meaningful to the person who pays a higher mortgage because a tax lien that is not theirs cannot be verified, or the person whose child attends a day care center with a pedophile whose arrest record cannot be properly authenticated, or the passengers on an airplane whose baggage is handled by an illegal alien whose fraudulent identity cannot be rejected. The harm caused by the loss of full SSN access far outweighs any

---

<sup>19</sup> U.S. Department of Health and Human Services, Administration for Children & Families, Office of Child Support Enforcement.

<sup>20</sup> U.S. Department of Health and Human Services, Administration for Children & Families, Office of Child Support Enforcement (visited March 25, 2002) <<http://www.acf.dhhs.gov/programs/cse/newhire/nh/nhbr/3benefit.htm>>. In 1998 Pennsylvania identified 4,289 overpayments with a dollar value of \$2.3 million, "solely through the use of this process." U.S. Department of Health and Human Services, Administration for Children & Families, Office of Child Support Enforcement, The Unemployment Insurance Crossmatch Project, July 13, 1999.

<sup>21</sup>

Within each area, the group number (middle two (2) digits) range from 01 to 99 but are not assigned in consecutive order. For administrative reasons, group numbers issued first consist of the odd numbers from 01 through 09 and then even numbers from 10 through 98, within each area number allocated to a State. After all numbers in group 98 of a particular area have been issued, the even Groups 02 through 08 are used, followed by odd Groups 11 through 99.

(visited March 18, 2002) <<http://www.ssa.gov/history/ssn/geocard.html>>.

<sup>22</sup> *Id.*

harm that would result in access to SSNs.<sup>23</sup> “If we can’t be sure when interacting that someone is who they purport to be, where are we?”<sup>24</sup>

## **Conclusion**

James Madison’s words in 1822 are as relevant today as they were then: “a popular government without popular information or the means of acquiring it is but a prologue to a farce or a tragedy, or perhaps both.”<sup>25</sup> There is no evidence to suggest that stalkers or identity fraud thieves are using the courthouse as a means to furthering their crimes -- the premise for closing court records is hypothetical.

The use of Social Security numbers provides safety and security to lenders, employers, apartment residents, airline passengers, school children, nursing home residents, and more. SSNs are an effective tool for law enforcement and a valuable safety net for governments to locate delinquent parents, unemployment and workers compensation fraudsters. The proper use of SSNs provide convenience, safety and security for businesses and consumers alike.

Sincerely,

Eric J. Ellman  
Director, State Government Relations

---

<sup>23</sup> As mentioned above, full SSN access serves a legitimate public interest and an attempt to close access based on § 1.00(a)(8) fails on the subsection’s own commentary.

<sup>24</sup> Robert O’Harrow Jr. & Jonathan Krim, at A1 (quoting Jim Huse, Inspector General of the Social Security Administration).

<sup>25</sup> James Madison, Letter to W. T. Barry (Aug. 4, 1822) (available at <<http://www.jmu.edu/madison/madison.htm>>)



## Most ID theft takes place offline

By Mindy Fetterman, USA TODAY

JANUARY 26, 2005

Identity theft is less likely to happen online than through traditional means, like losing or having your wallet stolen, according to a survey released Wednesday.

And when the identity of the thief is known, it's more likely to be one of your relatives.

There were 9.3 million new victims of identity fraud in 2004, or 4.3% of the U.S. adult population, according to the 2005 Identity Fraud Survey Report. It was released by the Council of Better Business Bureaus and Javelin Strategy & Research.

The survey found:

- Computer crimes accounted for 11.6% of identity theft in 2004, vs. 68% from paper sources.

### Stealing information

Identity theft is much less likely to occur through computer fraud than previously thought, according to a survey.

Lost or stolen wallet/ checkbook/credit card	28.8%
Accessed during transaction	12.9%
Friends/relatives	11.4%
Corrupt employee	8.7%
Stolen mail/ fraudulent change of address	8.0%
Computer spyware	5.2%
Taken from trash	2.6%
Computer virus/hacker	2.2%
E-mail sent by thieves posing as legitimate business	1.7%

Source: Javelin Strategy & Research, 2004 survey of 509 victims of identity theft

•The average loss for online identity theft was \$551, vs. \$4,543 from paper.

•Family members, friends and neighbors make up half of all known identity thieves.

"Computer theft is way down the list," says James Van Dyke of Javelin Strategy in

Pleasanton, Calif. Doing financial transactions via computer worries Americans, he says, because "It's the great unknown. But it's not where your primary risk from fraud is."

Computer identity theft can occur when fake e-mails claiming to be from your bank or credit card company warn you there has been a problem with your account and you need to log on to the attached link.

"This 'phishing' can look like the real thing, but it's sending you to a bogus site. You won't know that you're e-mailing a teenager's bedroom somewhere with your private information," Van Dyke says.

Only 2.2% of identity fraud comes from viruses or hackers; 1.7% from fake e-mails.

The biggest risk for identity fraud is from the old-fashioned theft of your wallet or paper records from your trash. And from people who know you. "People who are close to you can set up known accounts and have the information sent to a new address. So the fraud goes on longer and is harder to discover," Van Dyke says.

Hispanics and African-Americans are twice as likely as Asians or whites to experience the most serious fraud where a thief uses information to set up new bank or credit card accounts.

The BBB and Javelin Strategy did a telephone survey of 4,000 Americans and found 509 who had suffered identity theft. They then questioned those people extensively.

<http://usatoday.printthis.clickability.com/pt/cpt?action=cpt&title=USATODAY.com+-+Most+ID+thef...>

3-10





The independent survey was paid for by a group of credit card companies and banks, including CheckFree Services, Visa and Wells Fargo Bank.

▪ [REPRINTS & PERMISSIONS](#)

**Find this article at:**

[http://www.usatoday.com/tech/news/internetprivacy/2005-01-26-id-theft\\_x.htm](http://www.usatoday.com/tech/news/internetprivacy/2005-01-26-id-theft_x.htm)

Check the box to include the list of links referenced in the article.

	<b>Teachers - Click here for drug prevention resources</b>	
---	--	---



**IDENTITY THEFT**  
Data Clearinghouse



# Identity Theft Victim Complaint Data

*Figures and Trends  
In Kansas*

*January 1- December 31, 2003*

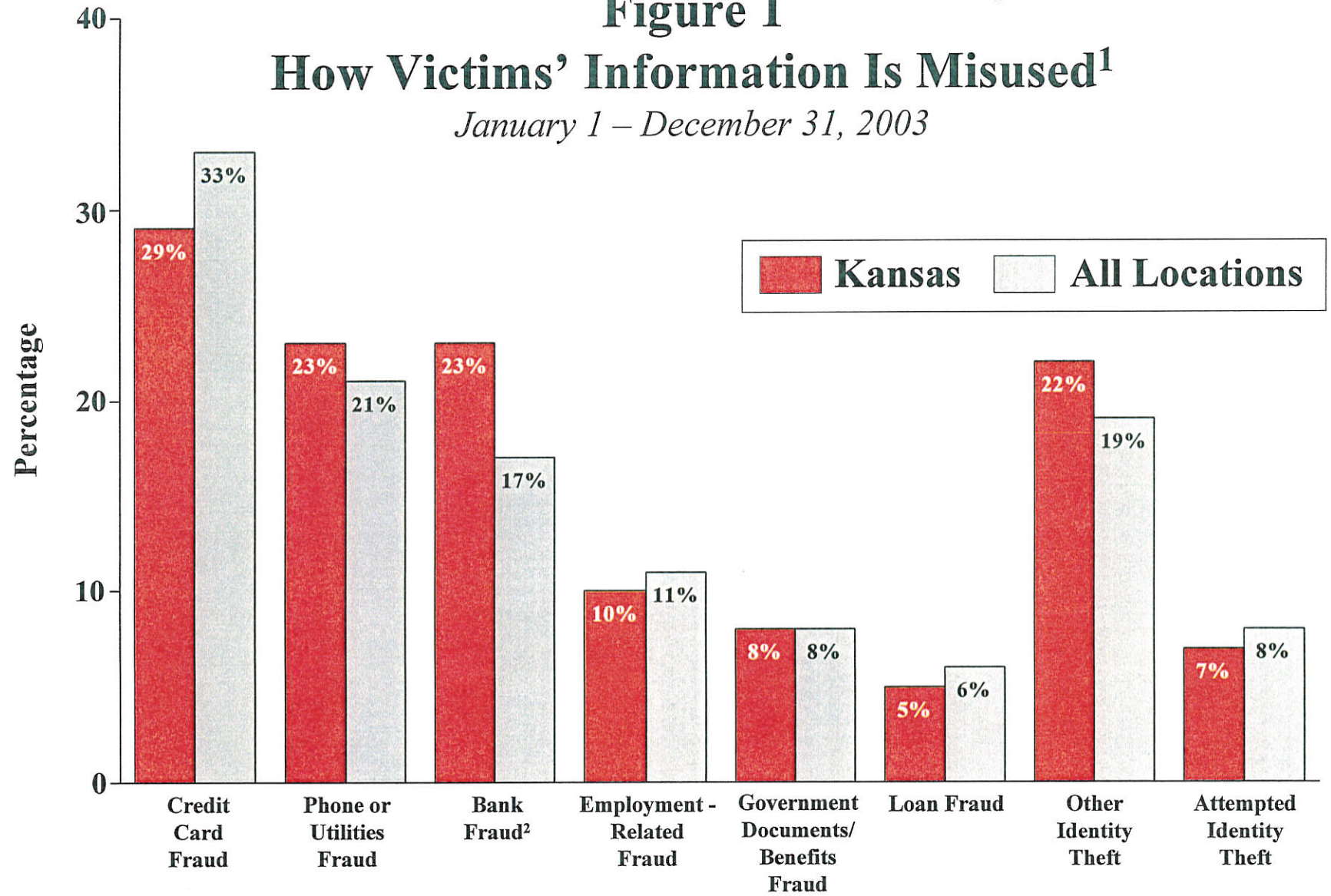


*Federal Trade Commission  
Washington, DC*

# Figure 1

## How Victims' Information Is Misused<sup>1</sup>

January 1 – December 31, 2003



<sup>1</sup>Percentages are based on the total number of victims reporting: 1,378 from Kansas and 214,905 from all locations. Percentages add to more than 100 because approximately 20% of victims from Kansas and 19% of victims from all locations reported experiencing more than one type of identity theft. All victims reported experiencing at least one type of identity theft.

<sup>2</sup>Includes fraud involving checking and saving accounts and electronic fund transfers.





# Figure 2

## How Victims' Information Is Misused<sup>1</sup>

January 1 – December 31, 2003

### Total Number of Identity Theft Victims:

**Kansas = 1,378**  
**All Locations = 214,905**

#### Credit Card Fraud

<i>Theft Subtypes</i>	<i>Kansas</i>	<i>All Locations</i>
New Accounts	16.8%	19.2%
Existing Accounts	11.5	12.0
Unspecified	0.9	1.4
<b>Total</b>	<b>29%</b>	<b>33%</b>

#### Phone or Utilities Fraud

<i>Theft Subtypes</i>	<i>Kansas</i>	<i>All Locations</i>
Wireless - New	9.1%	10.4%
Telephone - New	6.7	5.6
Utilities - New	5.7	3.8
Unauthorized Charges to Existing Accounts	0.9	0.6
Unspecified	0.3	0.8
<b>Total</b>	<b>23%</b>	<b>21%</b>

#### Bank Fraud<sup>2</sup>

<i>Theft Subtypes</i>	<i>Kansas</i>	<i>All Locations</i>
Existing Accounts	13.8%	8.2%
Electronic Fund Transfer	4.5	4.8
New Accounts	3.8	3.8
Unspecified	0.5	0.5
<b>Total</b>	<b>23%</b>	<b>17%</b>

#### Employment-Related Fraud

<i>Theft Subtype</i>	<i>Kansas</i>	<i>All Locations</i>
Employment-Related Fraud	9.5%	11.1%

#### Government Documents or Benefits Fraud

<i>Theft Subtypes</i>	<i>Kansas</i>	<i>All Locations</i>
Fraudulent Tax Return	2.8%	3.7%
Driver's License Issued / Forged	2.5	2.3
Gov't Benefits Applied For / Received	1.5	1.3
Social Security Card Issued / Forged	0.1	0.4
Other Gov't Documents Issued / Forged	0.7	0.4
Unspecified	0.0	<0.1
<b>Total</b>	<b>8%</b>	<b>8%</b>

#### Loan Fraud

<i>Theft Subtypes</i>	<i>Kansas</i>	<i>All Locations</i>
Business / Personal / Student Loan	2.1%	2.3%
Auto Loan / Lease	2.0	2.0
Real Estate Loan	0.7	1.0
Unspecified	0.2	0.3
<b>Total</b>	<b>5%</b>	<b>6%</b>

#### Other Identity Theft

<i>Theft Subtypes</i>	<i>Kansas</i>	<i>All Locations</i>
Other	12.2%	11.6%
Illegal / Criminal	2.1	2.1
Medical	2.5	1.8
Internet / E-Mail	2.6	1.7
Apartment / House Rented	0.7	0.9
Bankruptcy	0.4	0.3
Insurance	0.5	0.3
Property Rental Fraud	0.4	0.2
Child Support	0.2	0.2
Securities / Other Investments	0.1	0.2
Magazines	0.1	0.1
<b>Total</b>	<b>22%</b>	<b>19%</b>

#### Attempted Identity Theft

<i>Theft Subtype</i>	<i>Kansas</i>	<i>All Locations</i>
Attempted Identity Theft	6.7%	8.0%

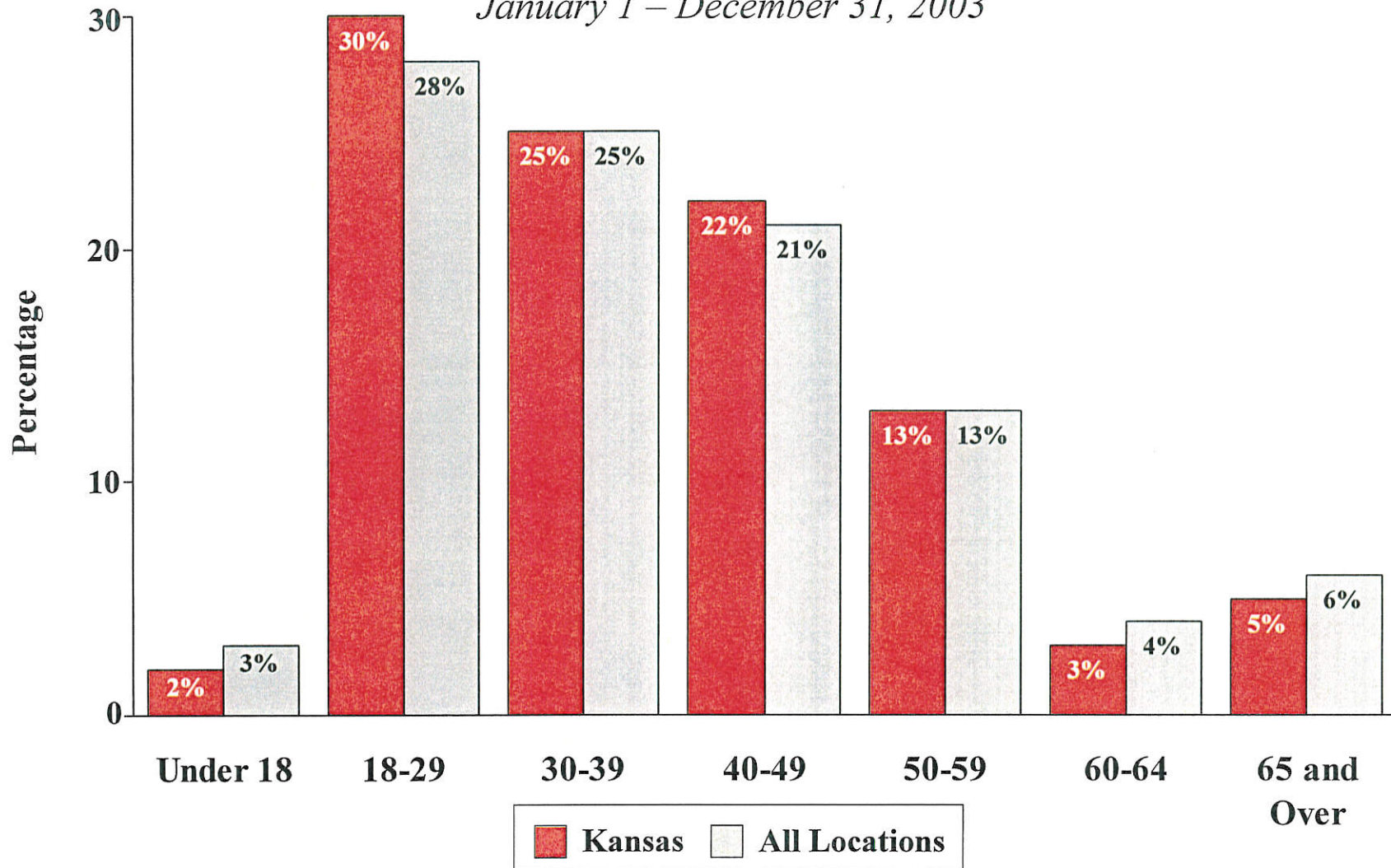
<sup>1</sup>Percentages are based on the total number of victims reporting: 1,378 from Kansas and 214,905 from all locations. Percentages add to more than 100 because approximately 20% of victims from Kansas and 19% of victims from all locations reported experiencing more than one type of identity theft. All victims reported experiencing at least one type of identity theft.  
<sup>2</sup>Includes fraud involving checking and saving accounts and electronic fund transfers.



### Figure 3

## Complaints by Victim Age<sup>1</sup>

January 1 – December 31, 2003



<sup>1</sup>Percentages are based on the number of victims who provided their age: 1,307 from Kansas and 197,475 from all locations. This chart represents 97% of victims reporting from Kansas and 95% of victims reporting from all locations who contacted the Federal Trade Commission directly.





# Figure 4a

## Identity Theft Victims by State (Per 100,000 Population)<sup>1</sup>

January 1 – December 31, 2003

Rank	Victim State	Victims Per 100,000 Population	Number of Victims	Rank	Victim State	Victims Per 100,000 Population	Number of Victims
1	Arizona	122.4	6,832	26	Kansas	50.6	1,378
2	Nevada	113.4	2,541	27	Rhode Island	49.9	537
3	California	111.2	39,452	28	Minnesota	49.7	2,517
4	Texas	93.3	20,634	29	Oklahoma	48.1	1,689
5	Florida	83.0	14,119	30	Ohio	48.0	5,494
6	New York	82.4	15,821	31	Tennessee	47.6	2,782
7	Oregon	81.7	2,909	32	Arkansas	47.5	1,294
8	Colorado	81.3	3,698	33	South Carolina	45.7	1,895
9	Illinois	77.4	9,792	34	Nebraska	44.9	781
10	Washington	77.3	4,741	35	Wisconsin	42.5	2,325
11	Maryland	74.9	4,124	36	Louisiana	41.7	1,875
12	Georgia	70.5	6,127	37	Alabama	40.5	1,823
13	New Mexico	70.3	1,317	38	New Hampshire	38.8	500
14	New Jersey	68.9	5,948	39	Mississippi	37.6	1,084
15	North Carolina	65.9	5,537	40	Idaho	36.1	493
16	Michigan	65.1	6,566	41	Alaska	35.6	231
17	Missouri	61.3	3,496	42	Wyoming	34.3	172
18	Indiana	59.1	3,660	43	Kentucky	32.3	1,332
19	Virginia	58.2	4,297	44	Montana	30.7	282
20	Delaware	57.7	472	45	Iowa	30.6	900
21	Massachusetts	56.5	3,634	46	West Virginia	28.1	508
22	Utah	56.4	1,326	47	Maine	27.0	353
23	Connecticut	54.9	1,913	48	Vermont	25.7	159
24	Pennsylvania	52.9	6,545	49	North Dakota	20.0	127
25	Hawaii	51.6	649	50	South Dakota	19.6	150

<sup>1</sup>Per 100,000 unit of population estimates are based on the 2003 U.S. Census population estimates (Table NST-EST2003-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2003). Numbers for the District of Columbia are: 917 victims and 162.8 victims per 100,000 population. 97% of the 214,905 total victims reporting indicated their state of residence.

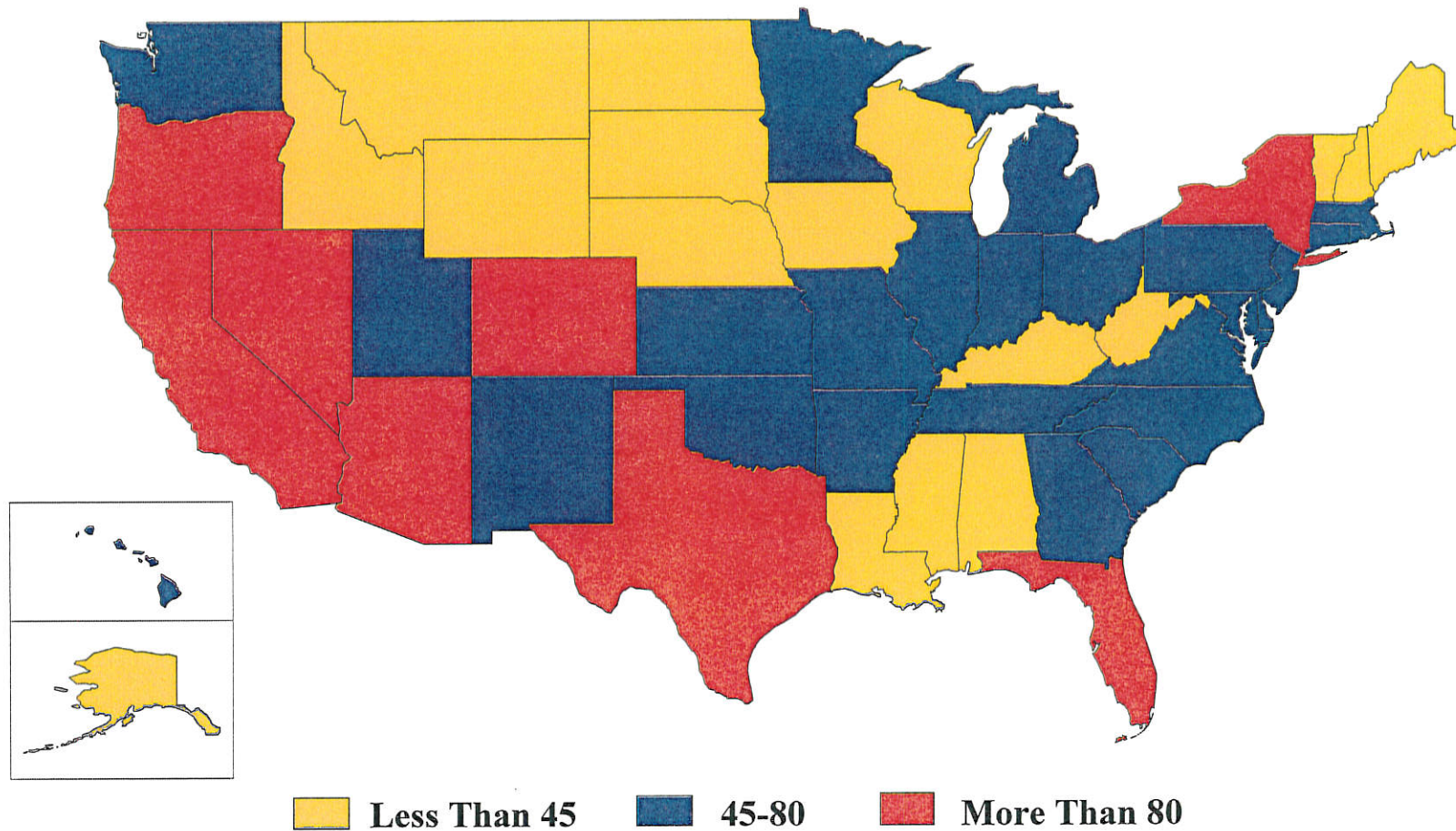




# Figure 4b

## Identity Theft Victims by State (Per 100,000 Population)<sup>1</sup>

January 1 – December 31, 2003

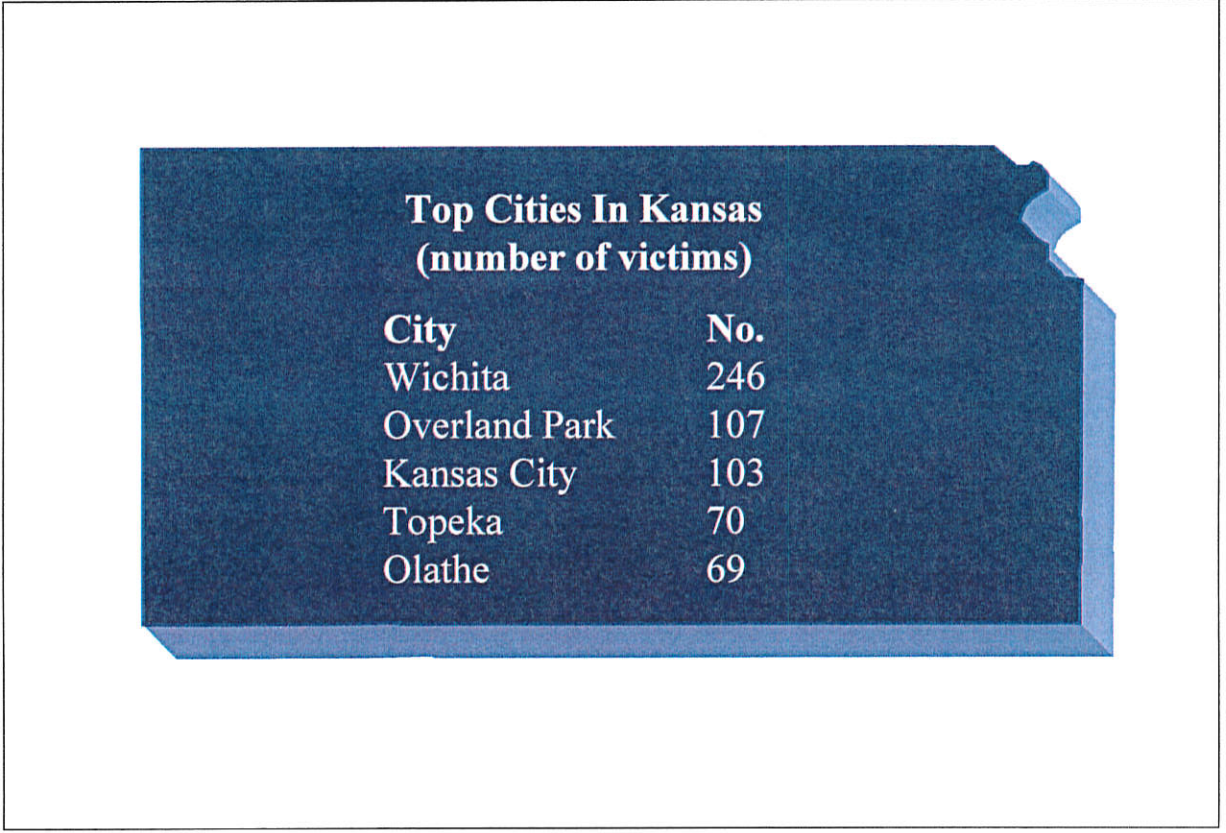


<sup>1</sup>Per 100,000 unit of population estimates are based on the 2003 U.S. Census population estimates (Table NST-EST2003-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2003). Numbers for the District of Columbia are: 917 victims and 162.8 victims per 100,000 population. 97% of the 214,905 total victims reporting indicated their state of residence.

# Figure 5

## Top Cities in Kansas<sup>1</sup>

January 1 – December 31, 2003



<sup>1</sup>99.9% of the 1,378 victims reporting from Kansas indicated their city of residence.



State of Kansas

## Office of Judicial Administration

Kansas Judicial Center  
301 SW 10<sup>th</sup>  
Topeka, Kansas 66612-1507

(785) 296-2256

House Judiciary Committee

Monday, March 14, 2005  
Testimony on SB 145

Lana Walsh

The Judicial Branch shares the concerns that prompted SB 145, and has for some time been working to resolve the issue of social security numbers that may be present in court records. We appreciate the prospective nature of SB 145, because efforts to make the clerks of the district court redact social security numbers that may be found in documents presently on file with the court would have been unworkable. It would have meant that, every time a file was requested for copying or viewing, the clerk would have had to inspect each page to make sure that no social security number was on the page. This could have required the clerks to inspect literally hundreds of pages in many cases. By keeping social security numbers out of documents filed with the courts that will be available to the public, we will be helping to address an area of concern in a manner that will not impose an unworkable burden on the clerks of the district court.

The court system currently is working on a procedure that will prohibit parties from placing social security numbers on documents that will be accessible to the public. It appeared that the majority of this issue resolved with a plan requiring the parties to fill out a cover sheet that would provide statistical information about the case being filed, as well as the social security numbers of the parties. The social security numbers would be entered into our computer system and would be available for court use as needed, but would not be available to the public.

We know there remain some problems with documents that contain social security numbers and we are working to resolve those issues. However, Judge Steve Leben from the 10<sup>th</sup> Judicial District (Johnson County), who is here this afternoon to testify on this bill, has called to our attention further instances in which social security numbers are embedded in court documents. At this point, it does not appear the court system can meet the expectation that all social security numbers be removed from court documents available to the public by July 1, 2005. While we intend to continue working on this issue, we request that action on this bill be delayed while these issues are resolved.

In the alternative, I have attached a balloon amendment that would clarify that the burden is on the parties to delete social security numbers, rather than on the clerks. Adopting this amendment, however, would only provide a partial solution, and would not take care of the issues Judge Leben will address in more detail.

Thank you for the opportunity to testify on this issue.

House Judiciary  
3-14-05  
Attachment 4

**SENATE BILL No. 145**

By Committee on Judiciary

1-31

Parties filing or submitting documents with the courts of this state on and after July 1, 2005, which will be available for public inspection or copying shall not include any references to an individual's social security number.

9 AN ACT concerning court records; amending K.S.A. 20-160 and re-  
10 pealing the existing section.  
11  
12 *Be it enacted by the Legislature of the State of Kansas:*  
13 Section 1. K.S.A. 20-160 is hereby amended to read as follows: 20-  
14 160. (a) The supreme court may adopt rules to govern the reproduction,  
15 preservation, storage and destruction of court records of this state, not  
16 inconsistent with ~~this act~~ *the provisions of K.S.A. 19-250, 20-159, 20-357*  
17 *and 60-465a, and amendments thereto.*  
18 ~~(b) Court records of this state which are filed or submitted on and~~  
19 ~~after July 1, 2005 and available for public inspection or copying shall have~~  
20 ~~any references to an individual's social security number removed or oth-~~  
21 ~~erwise rendered unreadable. The supreme court shall adopt rules imple-~~  
22 ~~menting the provisions of this subsection.~~  
23 Sec. 2. K.S.A. 20-160 is hereby repealed.  
24 Sec. 3. This act shall take effect and be in force from and after its  
25 publication in the statute book.



**Testimony of Judge Steve Leben**  
**Regarding Senate Bill 145**  
House Judiciary Committee  
March 14, 2005

Mr. Chairman and Members of the Committee,

Thank you for letting me appear before you today. I have been a trial judge in Johnson County since 1993; my docket includes civil, criminal, and domestic cases.

Senate Bill No. 145 is a simple, two-sentence bill. "Court records" filed or submitted after July 1 *and* available to the public must either have no Social Security numbers or have the numbers made unreadable. And the Supreme Court shall adopt rules to implement that.

When they work, simple solutions are the best ones. Here, though, we are trying for a simple solution to only a single part of a complex problem. And there is good reason to believe it won't achieve the intended result, that it will cause unintended problems, and that it will increase costs to both the judiciary and to citizens who find themselves in some court proceedings. For these reasons, I ask that you not move forward with Senate Bill 145 at this time.

There are really two, quite complex but interrelated problems we are dealing with here. First, we have identity theft. Certainly, we don't want public records used for that. Second, we have privacy concerns as court records move from paper records—which can only be reviewed by coming to the courthouse—to electronic files, which can be made available over the Internet.

Senate Bill 145 is intended to address identity theft. Even its proponents would surely concede that it does not address the major sources of personal information used by identity thieves. I talked with Paul Morrison, the Johnson County District Attorney, on Friday about this bill and about identity theft generally. His office has never been aware of a case in which they have prosecuted someone for identity theft in which the criminal found any of his

information in a court file. Rather, the sources they encounter are generally “dumpster dives” through discarded trash, stolen mail, purse or billfold thefts, or folks who have taken data-entry jobs at financial-service companies to obtain such information.

I’m here today for two reasons. First, I took the time to read through an OJA summary of pending legislation and noted this bill. That led to my contacting Kathy Porter to tell her of some problems I thought might be caused by the bill. That’s the direct reason for my ending up here today. Second, I am concerned about all of the issues that come together with respect to this bill. We have a duty to provide open access to court records and proceedings to the people of Kansas. We also want to do whatever can be done to limit the chances for criminal activity, including identity theft. And, as we move toward electronic access to court records—something I’ve been working on with other judges and staff in Johnson County now for several years—we have to consider the ways in which this raises legitimate privacy concerns.

Now let me talk for a minute about some specific problems with Senate Bill 145. I have attached to my written testimony a copy of testimony given last year to Congress by Mike Buenger, the state court administrator for Missouri who was then the president of the Conference of State Court Administrators. As he notes, Social Security numbers are pervasive in state court documents and this is frequently *required by law*. Examples he gives include pleadings and court orders related to child support, where Social Security numbers are needed to help track those who owe support and to intercept tax refunds that can go to pay back child support. He notes that federal regulations even explicitly require that a Social Security number appear on garnishment orders involving postal employees. He provides many other reasons that state court pleadings include these numbers.

One other example that I’m aware of causes me some concern about this bill. In divorce cases, any time that retirement benefits, pension plans, or 401(k) plans are to be divided, an order called a Qualified Domestic Relations Order—or

QDRO (pronounced “quad-roh”)—must be entered. These orders are governed by federal law under ERISA. And the form of order appears to require Social Security numbers. Certainly in practice, *all* of these orders always include them. In practice, the way this generally works is that the attorneys work with the administrator of the pension plan at issue. Each plan will have a form order that it prefers and agrees is acceptable. Usually the attorneys prepare a form based on that form order. I can’t say for sure that plan administrators will turn down QDROs if the Social Security numbers are provided in a separate cover letter or document that is not in the public court file. My guess is that many would. What I am sure of, though, is that there would be greater expense to the parties in divorce cases involving QDROs for quite some time while this gets sorted out. And it may just be that Senate Bill 145 would not be workable with respect to these orders.

When I say not workable, one might reply that there are two options to comply with the bill. You can make any record with a Social Security number inaccessible to the public *or* you can make the number unreadable in the public file. The first option cuts against both legal and traditional requirements of openness in the courts. As a general matter of state and federal law, what happens in court is public. The U.S. Supreme Court said in 1947, “A trial is a public event. What transpires in the court room is public property.” *Craig v. Harney*, 331 U.S. 367, 373 (1947). Of course, there are exceptions. But the exceptions are narrow ones and the general rule that proceedings of the judicial branch of government are open remains true.

The other option—making the numbers unreadable in some way—may have tremendous costs to the judicial branch. And we are unable to estimate those costs without completely cataloging all of the places Social Security numbers may appear *and* considering how the move over the next decade to electronic court records will impact that situation.

I come back, then, to my initial comments. This bill will do very little to prevent identity theft. Paul Morrison also authorized me to tell you that he and his office would be glad to work with an interim committee to consider what further steps could be taken to improve laws relating to identity theft.

This bill, though, will have unintended consequences. Any number of laws require the use of Social Security numbers. I'm fairly certain that this one-size-fits-all solution will cause problems in divorce cases—with QDROs and with child support matters. Both the judiciary *and* citizens who are involved in those proceedings will have increased costs as a result.

We need to address the problem of identity theft and we need to make sure that public records are not the preferred source for thieves. I know that OJA staff have been working on this issue for some time. I'm sorry that I ended up pointing out some problems to the work-in-progress solution that they had in mind. Two states that I'm aware of—Minnesota and New York—have had statewide commissions spend several months reviewing issues involved in public access to court records, including Social Security numbers, in the past year. Minnesota's final report was issued in June 2004 and New York's was issued in February 2004. Minnesota's report is 83 pages plus appendices; New York's is 66 pages. There are complex issues involved. I hope that you will give your judiciary a bit more time to try to do something constructive here.



## House Committee on Ways and Means

Statement of Mike L. Buenger, President, Conference of State Court Administrators, Jefferson City, Missouri

Testimony Before the Subcommittee on Social Security  
of the House Committee on Ways and Means

June 15, 2004

Mr. Chairman and Members of the Subcommittee,

The Conference of State Court Administrators (COSCA) is pleased to present testimony on today's hearing "Enhancing Social Security Number Privacy" as the subcommittee examines the issue of protecting privacy and preventing the misuse of Social Security Numbers (SSNs).

### SUMMARY

Mr. Chairman and members of the subcommittee, for the past several years the state court community has been grappling with the issue of protecting privacy, and private information, as it relates to court records. Although the immediate issue for the committee is protecting the privacy of SSNs, privacy protection for information in court records is actually a much broader issue. The use of Social Security Numbers in court records is, thus, a subset of much larger issues that involve balancing public access to government records with the legitimate privacy interests of citizens with actual capacity of courts to operationally accommodate privacy and public access concerns. To this end, we helped develop guidance for state courts through a project entitled "Public Access to Court Records: CCJ/COSCA Guidelines for Policy Development by State Courts." This guidance outlines the issues that courts must address in developing rules and policies governing access to court records. The *Guidelines* touch on the use of SSNs in court records and other private information. The text of the *Guidelines* can be found at <http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf>. Both the Conference of Chief Justices and COSCA adopted a resolution endorsing the *Guidelines* and urged the states to use them in developing their own standards, rules, and policies.

Mr. Chairman, SSNs are pervasive in state court documents, frequently as mandated by state and federal law. For example, federal law requires us to collect SSNs for various reasons related to tracking deadbeat parents. By federal law, SSNs must *appear* on pleadings and court orders related to child support. Even federal regulations require that a SSN must appear on garnishment orders involving postal employees. *See*, 39 CFR 491.3 Along with other identifiers, courts use SSNs to associate parties to a case, i.e. to determine whether John Smith 1 is different from John Smith 2. We use SSNs to collect fines and crime victim restitution, to report criminal records to central repositories, and to aid in the enforcement and collection of child support. In addition, many SSNs appear in the public record in many types of court cases including, but not limited to, bankruptcy, divorce, paternity, and child support determination.

Mr. Chairman, the most important message I can deliver to you today is that the Conference stands ready to work with you in crafting solutions to address the problem of identity theft. But I think it is also important for the sub-committee and the Congress to understand that this is not a problem that can be solved through a simple mandate. It is complex not only in terms of your responsibility to establish consistent public policy but also in terms of the ability of states, and in this case state courts, to actually implement that policy. The threat of identity theft is real and we want to do our part to eliminate it. We are at the same time concerned about the effort to require us to redact or expunge SSNs that appear in public records. We feel that this type of requirement could impose an incalculable burden on the state courts in this country, both with respect to

resources and funding to achieve that goal. The cost to fulfill this requirement would be high because many SSNs appear in paper documents as well as other hard-to-redact microfilm/microfiche.

### ABOUT COSCA

Before I begin my remarks, I would like to provide some background on our group and our membership. I submit this testimony as the President of the Conference of State Court Administrators (COSCA). COSCA was organized in 1955 and is dedicated to the improvement of state court systems. Its membership consists of the principal court administrative officer in each of the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and the Territories of American Samoa, Guam, and the Virgin Islands. A state court administrator implements policy and programs for a statewide judicial system. COSCA is a nonprofit corporation endeavoring to increase the efficiency and fairness of the nation's state court systems. State courts handle 97% of all judicial proceedings in the country, over 96 million cases annually. The purposes of COSCA are:

- To encourage the formulation of fundamental policies, principles, and standards for state court administration;
- To facilitate cooperation, consultation, and exchange of information by and among national, state, and local offices and organizations directly concerned with court administration;
- To foster the utilization of the principles and techniques of modern management in the field of judicial administration; and
- To improve administrative practices and procedures and to increase the efficiency and effectiveness of all courts.

Although I do not speak for them, I also would like to tell you about the Conference of Chief Justices (CCJ), a national organization that represents the top judicial officers of the 58 states, commonwealths, and territories of the United States. Founded in 1949, CCJ is the primary voice for state courts before the federal legislative and executive branches and works to promote current legal reforms and improvements in state court administration. COSCA works very closely with CCJ on policy development and administration of justice issues.

### NATIONAL EFFORT TO CRAFT PUBLIC ACCESS GUIDELINES TO COURT RECORDS

Our project entitled, "Public Access to Court Records: CCJ/COSCA Guidelines for Policy Development by State Courts" was a joint effort of CCJ and COSCA to give state court systems and local trial courts assistance in establishing policies and procedures that balance the concerns of personal privacy, public access and public safety.

The State Justice Institute (SJI) funded this project in 2001 and the project was staffed by the National Center for State Courts (NCSC) and Justice Management Institute (JMI). The project received testimony, guidance and comments from a broad-based national committee that included representatives from courts (judges, court administrators, and clerks), law enforcement, privacy advocates, the media, and secondary users of court information.

The *Guidelines* recommend the issues that a court must address in developing its own rules and policies governing public access to its records. The *Guidelines* are based on the following premises:

- Retention of the traditional policy that court records are presumptively open to public access
- The criteria for access should be the same regardless of the form of the record (paper or electronic), although the manner of access may vary
- The nature of certain information in some court records is such that remote public access to the

information in electronic form may be inappropriate, even though public access at the courthouse is maintained

- The nature of the information in some records is such that all public access to the information should be precluded, unless authorized by a judge
- Access policies should be clear, consistently applied, and not subject to interpretation by individual courts or court personnel

The *Guidelines* Committee examined the use of SSNs in current court practices. They looked at the inclusion of SSNs in bulk distribution of court records, and information in other documents besides SSNs that courts traditionally protect, such as addresses, phone numbers, photographs, medical records, family law proceedings, and financial account numbers. Finally, the Committee examined various federal laws and requirements governing SSN display and distribution by state and local entities.

On August 1, 2002, CCJ and COSCA endorsed and commended "the Guidelines to each state as a starting point and means to assist local officials as they develop policies and procedures for their own jurisdictions."

### STATE COURTS' INTEREST IN COLLECTING AND USING SOCIAL SECURITY NUMBERS

Why is this question of concern to state courts? Why do state courts need to require parties to provide their SSNs in the course of state court litigation?

Identification of parties. A growing number of court systems are using case management information systems in which an individual's name, address, and telephone number are entered once, regardless of the number of cases in which the person is a party. Such "party based" systems are rapidly replacing "case based" systems. The advantage of these systems is multifold: they enable courts to update an address or telephone number for all cases in which the person is a party by a single computer entry, they provide judges and court personnel with a fuller array of justice information, and they allow for cleaner information sharing with other justice community participants such as law enforcement, prosecutors, probation systems, and the like. Absent the use of unique identifiers such as SSNs, the entire justice community would come to a grinding halt and be unable to meet many state and federal mandates. SSNs provide a unique identifier by which court personnel can determine whether the current "John Smith" is the same person as a previous "John Smith" who appeared in an earlier case and whether this was the same "John Smith" reported to the central criminal records repository.

The need for SSNs in the future may be substantially reduced by the use of other "unique" identifiers, e.g., biometric identifiers in criminal cases. Moreover, the ability to mask SSNs becomes easier as state courts implement sophisticated case management systems. Certainly the move to "automate" state courts with high-end technology allowing such services as electronic filing can provide opportunities for greatly limiting access to personal information such as SSNs. However, the time and costs of moving to such systems necessarily means that the ability to mask or redact such information is, for many courts, a future event not something that can or will be done overnight simply because there is federal mandate to do so.

Collection of fees, fines and restitution by courts. SSNs are the universal personal identifier for credit references, tax collection, and commercial transactions.

When courts give a criminal defendant an opportunity to pay an assessment resulting from a criminal infraction in periodic payments, the court needs to be able to function as a collection agency. Having the convicted person's social security number is necessary for use of state tax intercept programs (in which a debt to the state is deducted from a taxpayer's state income tax refund) and other collection activities. Moreover, SSNs are often used for purposes such as enforcing criminal fines and restitution orders or denying of motor vehicle registration.



Creation of jury pools and payment of jurors. SSNs are a necessary part of identifying eligible jurors through a process by which multiple lists (for instance, registered voters and registered drivers) are merged to eliminate duplicate records for individual citizens in creating a master source list for the random selection of jurors. Duplicate records double an individual's chance of being called for jury duty and reduce the representativeness of jury panels. Some courts use SSNs to pay jurors as well.

Making payments to vendors. SSNs are used as vendor identification numbers to keep track of individuals providing services to courts and to report their income to state and federal taxing authorities.

Facilitating the collection of judgments by creditors and government agencies. Courts are not the only entities that need to collect judgements. Judgment creditors need SSNs to locate a judgment debtor's assets to levy upon them. Courts often require that the judgment debtor make this information available without requiring separate discovery proceedings that lengthen the collection process and increase its costs. Federal law now requires state courts to place the parties' SSNs in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgements in order to facilitate the collection of child support. On October 1, 1999, that requirement was extended to include the SSNs of all children to whom support is required to be paid.

Notification to the Social Security Administration of the names of incarcerated and absconded persons. The Social Security Administration cuts-off all payments to persons incarcerated in federal, state or local prisons or jails, and to persons who are currently fugitives from justice. The savings to the federal budget from this provision are substantial. To implement this process, Social Security Administration needs to identify persons who have been sentenced to jail or prison and persons for whom warrants have been issued. The agency has traditionally obtained this information from state and local correctional agencies. See 42 USC §402(x)(3). The state courts of Maryland are involved in an experimental program to provide such information directly from court records. The Maryland program has two additional future advantages for state courts. First, the program offers the possibility of obtaining better addresses for many court records; social security and other welfare agencies have the very best address records because of beneficiaries' obvious interest in maintaining their accuracy. Second, cutting off benefits may provide a useful incentive to those persons subject to outstanding warrants without requiring law enforcement to expend resources to find and serve such persons.

Transmitting information to other agencies. In addition to the Social Security Administration, many states provide information from court records to other state agencies. A frequently occurring example is the Motor Vehicle Department, to which courts send records of traffic violations for enforcement of administrative driver's license revocation processes. These transfers of information often rely upon SSNs to ensure that new citations are entered into the correct driver record.

## PROPOSED LEGISLATION

Mr. Chairman, your legislation, H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003, contains the following provision:

### *SEC. 102. RESTRICTIONS ON THE SALE OR DISPLAY TO THE GENERAL PUBLIC OF SOCIAL SECURITY ACCOUNT NUMBERS BY GOVERNMENTAL AGENCIES*

*"(x)(I) An executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or political subdivision thereof or trustee appointed in a case under title II, United States Code (or person acting as an agent of such an agency or instrumentality or trustee) in possession of any individual's social security account number may not sell or display to the general public such number."*



June 15, 2004, President, Conference of State Court Administrators, Jefferson City, Missouri, M... Page 5 of 6

This section has serious implications for state courts in a variety of contexts.

For example, *federal* law requires courts to enter SSNs on court orders granting divorces or child support or determining paternity. Some states' laws contain similar requirements in other types of cases. As noted previously, given that over 96 million cases are filed annually in state courts, the task of redacting SSNs from existing documents is not only daunting, it may actually violate federal law in some cases and certainly violates many state "sunshine laws" to the extent that access to documents is required.

SSNs appear in many financial documents, such as tax returns, which are required to be filed in court (e.g., for child support determinations) or are appended to official court documents, such as motions for summary judgments. Restricting access to SSNs in such documents is difficult because often such information can be buried in a stack of documents, which are generally not reviewed by courts or clerks until the case is actually heard.

Courts will have substantial increased labor costs in staff time to redact or strike the appearance of SSNs in paper records or in microfilm/microfiche if the above requirement is imposed.

In addition, we are unclear whether H.R. 2971 applies to newly made court records or all records in a court's inventory. Obviously, asking courts to retroactively expunge or redact social security from all court records would be time consuming and expensive. Given the extensive records retention policies applicable to court filings, retroactive redaction or masking could be an impossible task in some states.

Finally, in an effort to make courts and court records more open, many courts are now beginning to make available many public records on the internet either as text/character documents or by scanning and placing them online through imaging software (PDF files). While the removal of SSNs in text/character documents may be relatively easy in some computer generated records (XML), other scanned records, such as PDF files, will be harder to change necessitating more staff and an increase in labor costs.

### COSCA RECOMMENDATIONS

We have recommended that state courts adopt the following policies, unless state law directs them otherwise:

Official court files. State courts should not attempt to expunge or redact SSNs that appear in documents that are public records, and certainly this should not be required on a retroactive basis. As was mentioned earlier, federal law requires state courts to place the parties' SSNs in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgement in order to facilitate the collection of child support. The purpose of placing that data on judgments is not just to provide it to child support enforcement agencies; it is also to provide it to the parties themselves for their own private enforcement efforts. Any other approach puts the courts in an untenable position – having an affirmative obligation to provide judgments in one form to parties and child support enforcement agencies and in another form to all other persons.

This same reasoning applies to income tax returns or other documents containing SSNs filed in court. It would be unreasonable, and expensive, to expect courts to search every document filed for the existence of SSNs. Further, court staff has no business altering documents filed in a case; the SSN may have evidentiary value in the case – at the very least to confirm the identity of the purported income tax filer.

Case management information databases. Data in automated information systems raises more privacy concerns than information in paper files. Automated data can be gathered quickly and in bulk, can be manipulated easily, and can be correlated easily with other personal data in electronic form. Data in an automated database can also be protected more easily from unauthorized access than data in paper files. It is feasible to restrict access to

individual fields in a database altogether or to limit access to specific persons or to specific categories of persons. Consequently, state courts should take steps to restrict access to SSNs appearing in court databases. They should not be available to public inquirers. Access to them should be restricted to court staff and to other specifically authorized persons (such as child support enforcement agencies) for whose use the information has been gathered.

Staff response to queries from the public. When court automated records include SSNs for purposes of identifying parties, court staff should be trained not to provide those numbers to persons who inquire at the public counter or by telephone. However, staff may confirm that the party to a case is the person with a particular SSN when the inquirer already has the number and provides it to the court staff member.

In short, staff may not read out a SSN but may listen to the number and confirm that the party in the court's records is the person with that number. This is the same distinction applied to automated data base searches. This distinction is one commonly followed in federal and state courts.

### CONCLUSION

Mr. Chairman, we recognize the serious role of SSNs in incidences of identity theft and the fact that such information is readily available in a host of public records. The current state of affairs with regard to the treatment of SSNs provides lawbreakers the continued opportunity to exploit the current system at the expense of ordinary Americans. The threat of identity theft is real and we want to do our part to eliminate it. However, as previously noted, there is no simple solution and certainly no cheap solution to this problem. Even the public policy coming from Congress evidences the complexity of the issue by requiring the collection, use and availability of such information on one hand and then seeking to restrict access to its use on the other. We also hope that you assist the state courts in dealing with the unfunded mandate H.R. 2971 presents.

I have presented several ways our courts utilize SSNs and finding solutions to protect an individual's privacy will be complex and difficult. Many state courts are already taking steps to fashion solutions in response to the problem. Washington state, for example, is pioneering an innovative solution where they are creating two sets of court records: a public and a private one. Other states are experimenting with different approaches.



March 14, 2005

To: House Committee on Judiciary

From: Kathleen Taylor Olsen, Kansas Bankers Association

**Re: SB 112: Materialman's Lien Statute**

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you today to in support of **SB 112**, a bill that amends several statutes relating to the priority of Kansas materialman's liens. These amendments are the result of a collaborative effort among the Kansas Land Title Association, the Heartland Community Bankers Association and the Kansas Bankers Association. This bill draft represents this group's attempt to address a recent Kansas Court of Appeals decision, *Mutual Savings Assoc. v. Res/Com Prop.*, 32 Kan. App. 2d 48, 79 P.3d 184 (2004).

K.S.A. 60-1101, establishes the basis for determining priority of claims against property under construction. We believe that this statute provides that all unpaid materialmans' liens relating to the same improvement have equal rank with one another, and that all have priority over any other lien that is recorded subsequent to the commencement of visible work on the property.

There are two very important keys to this law: 1) that the priority for materialmans' liens over other liens is measured from the date that the earliest **unpaid** lienholder began work on the property, and not the date work began by some party who has been paid in full; and 2) that the work establishing the priority date for all other lienholders must be something that is **visible** at the property site.

The Court in the *Mutual Savings* case cast doubt on the reliability of the law as we know it to be. The Court decision indicates that the priority date for all subsequent lienholders under this law can be established by a contractor or subcontractor who has been paid in full and no longer has a claim on the property; and that work that is not visible can establish the priority date for all other subsequent lienholders under this law.

In discussions with all interested parties, the KBA acknowledged that requiring that the work be visible can be problematic. We have agreed to strike language in the bill requiring that the work establishing the priority date for all other lienholders be visible. This would, in effect, reinstate the standard set by our Supreme Court in *Haz-Mat Response, Inc. v. Certified Waste Services Ltd.*, 259 Kan. 166, 170, 910 P.2d 839 (1996). I have attached the 7 considerations that the Kansas Supreme Court identified as necessary for determining whether activity improves property and is thereby, lienable.

**SB 112**

March 14, 2005

Page Two

We strongly believe that the remaining amendments are necessary to re-establish the long-understood rule that allowed a mortgagee to ensure the priority of the recorded mortgage against unknown lienholders under this law by providing that those who have been paid in full and who no longer have a claim on the property cannot establish the priority date for subsequent lienholders.

Thank you and we would respectfully request that the Committee act favorably on **SB 112**.



Subsequent to *Mark Twain*, however, our Supreme Court in *Haz-Mat Response, Inc.*, 259 Kan. 166, clarified the test to be used in determining what types of activity were and were not lienable.

The *Haz-Mat* court noted that the statutory phrase "improvement of real property" is not defined in the Kansas statute. The only reported Kansas case construing the requirement was *Mark Twain*, 14 Kan. App. 2d 714. The *Haz-Mat* court went on to discuss the *Mark Twain* case and concluded that *the cases cited in Mark Twain did not support the conclusion that there must be visible effect on the real property for the work to be lienable*. While "improvement" is generally defined as any physical addition made to the real property that enhances the value of the land, there is no requirement under our present law that there be a physical addition made to real property. See *Benner-Williams, Inc. v. Romine*, 200 Kan. 483, 437 P.2d 312 (1968). Further, improvement is not necessarily synonymous with enhancement of market value. *Haz-Mat*, 259 Kan. at 171-72.

After reviewing a number of prior Kansas cases as well as cases from other states dealing generally with the meaning of the phrase "improvement of real property," the *Haz-Mat* court devised seven (7) considerations for determining if an activity is considered to improve real property.

➔ "(1) What is or is not an improvement of real property must necessarily be based upon the circumstances of each case; (2) improvement of the property does not require the actual construction of a physical improvement on the real property; (3) the improvement of real property need not necessarily be visible, although in most instances it is; (4) the improvement of the real property must enhance the value of the real property, although it need not enhance the selling value of the property; (5) for labor, equipment, material, or supplies to be lienable items, they must be used or consumed and thus become part of the real property; (6) the nature of the activity performed is not necessarily a determining factor of whether there is an improvement of real property within the meaning of the statute; rather, the purpose of the activity is more directly concerned in the determination of whether there is an improvement of property which is thus lienable; and (7) the furnishing of labor, equipment, material, or supplies used or consumed for the improvement of real property may become lienable if established to be part of an overall plan to enhance the value of the property, its beauty or utility, or to adapt it for a new or further purpose, or if the furnishing of labor, equipment, material, or supplies is a necessary feature of a plan of construction of a physical improvement to the real property." 259 Kan. at 175.

Finally, the *Haz-Mat* court adopted the Black's Law Dictionary definition of the phrase "improvement of real property" as it is used in K.S.A. 60-1101: "A valuable addition made to real property (usually real estate) or an amelioration in its condition, amounting to more than mere repairs or replacement, costing labor or capital, and intended to enhance its value, beauty or utility or to adapt it for new or further purposes." 259 Kan. at 175-76 (citing Black's Law Dictionary 757 [6th ed. 1990]). As we understand, *Haz-Mat* disapproved of *Mark Twain's* holding that improvement to the property must be visible before the work can be lienable.

Here, the first issue is whether Peridian's preliminary staking and surveying, done prior to Mutual's mortgage, constituted an "improvement" as used in K.S.A. 60-1101. Applying the considerations set out in *Haz-Mat*, we conclude Peridian's efforts were lienable. It is undisputed that the labor and capital expended in the surveying and staking work done by Peridian were actually used in the development of the property. This record is silent as to whether stakes installed by Peridian were still on the property at the time Mutual's mortgages were filed, but this is irrelevant under the *Haz-Mat* test. If they were in fact visible, this lends further support to the subcontractors' claim.

The next issue is, if Peridian's work is lienable, when did that lien attach. Once again K.S.A. 60-1101 reads in relevant part:

To: House Judiciary Committee  
From: Matthew Goddard  
Heartland Community Bankers Association  
Date: March 14, 2005  
Re: Senate Bill 112

The Heartland Community Bankers Association appreciates the opportunity to appear before the House Committee on Judiciary to express our support for Senate Bill 112.

The Heartland Community Bankers Association represents savings associations in Kansas, Arkansas, Colorado, Nebraska and Oklahoma. Our Kansas membership makes more than \$250 million in construction loans annually for residential and commercial properties.

A ruling by the Court of Appeals in *Mutual Savings Association v. Res/Com Properties*, 32 Kan. App. 2d 48, 79 P.3d 184 (2004), has caused concern among Kansas lenders and has the potential to jeopardize future construction lending. The ruling upset our long-time understanding of Kansas law as it relates to the priority of materialman's liens. Senate Bill 112 addresses our biggest concern with the *Mutual* decision. The amendments added in the Senate Judiciary Committee represent a compromise between lenders and some of the opponents of SB 112 as it was originally introduced.

Currently, K.S.A. 60-1101 provides the basis for determining the priority of materialman's liens. The first lien can be filed when labor, equipment, material or supplies are used or consumed for the improvement of real property. The lien enjoys priority over all other liens which are subsequent to the start of the furnishing of labor, equipment, material and supplies at the property that is the subject of the lien. When two or more liens are filed on the same improvement, all of the liens are similarly preferred to the date of the earliest unsatisfied lien.

In the *Mutual* case, the court found that even when Mutual Savings, which had second priority with its mortgage, paid the contractor with first lien priority and took assignment of its priority lien, the liens of contractors who subsequently performed lienable work still had priority over Mutual because of the "piggy-back" effect of materialman's liens. The court essentially said that the "earliest unsatisfied lien" remains so even after it is paid off. It was the expectation of our industry that Mutual would have first priority after paying the original lienholder and taking assignment of its lien. Senate Bill 112 addresses this by providing that if an earlier unsatisfied lien is paid in full, the preference date for everyone with a claim becomes the date of the next earliest unsatisfied lien.

HCBA is also concerned with the *Mutual* ruling because it seems to permit liens for work which is not visible and allows those liens to set the priority date for subsequent lienholders. Prior to *Mutual*, and affirmed in a 1977 opinion, work performed at a site constituted notice of the existence of the lien. Post-*Mutual*, we now live in an era of uncertainty as that standard seems to no longer be valid. Lenders are

concerned that they may no longer know when lienable work has commenced. However, in the effort to reach common ground with those who had concerns with SB 112's original language, the compromise Senate amendments removed the requirement that materials or work be visible in order to be lienable.

The ruling in *Mutual v. Res/Com* does not impact the vast majority of construction projects where the lender who is financing the construction files its lien prior to the commencement of work on the property. However, in instances where work begins or supplies are furnished before the lender files its lien, the uncertain presence of materialman's liens risks the project's financing. Although the Court of Appeals stated that lenders may protect the priority of their mortgage by obtaining lien waivers, any risk associated with that process may prompt the lender to abandon the project altogether. HCBA believes that by allowing the status quo to remain in place, lenders will be more likely to withdraw financing than risk losing out on the priority of its claim.

We respectfully request that the House Committee on Judiciary recommend SB 112 favorable for passage.

Thank you.



TESTIMONY OF WILLIAM A. LARSON,  
GENERAL COUNSEL TO THE ASSOCIATED  
GENERAL CONTRACTORS OF KANSAS  
TO THE HOUSE JUDICIARY COMMITTEE ON  
SENATE BILL 112  
March 15, 2005

The Associated General Contractors of Kansas, is an Association consisting of the majority of commercial general contractors (other than in Wyandotte and Johnson County) in the commercial construction building industry. The Association, however, does not just represent general contractors. It also has in Kansas a large number of subcontractor members as well as associate members including material suppliers who have lien rights under our current mechanics liens laws. The Associated General Contractors of Kansas (AGC) opposes Senate Bill No. 112.

Senate Bill No. 112 is a reaction to the Kansas Court of Appeals case of *Mutual Savings Association v. Res /Com Properties, LLC, et al.*, 32 Kan.App.2d 448, 79 P.3d 184 (2003). In this case, Mutual Savings Association was attempting to foreclose on its mortgage against the owner of a project that defaulted on payments to Mutual Savings as well as to its contractor and subcontractors. Succinctly put the Court of Appeals held that the Mutual Savings Association did not have a first and prior lien to the mechanic's lien claimants and further held that it was not absolutely necessary that work on the site be visible prior to a mechanic's lien attaching. While it would probably not be productive to go into a detailed explanation of the *Mutual Savings Association* case, it suffices to say that the situation that occurred in the *Mutual Savings* case, was very unusual.

The AGC of Kansas has historically opposed changes to the mechanic's lien laws unless there was a very good reason for them. The reason is that the mechanic's lien laws are currently understood as a result of industry practice and numerous court interpretations of the law. Any time a change is made in the lien laws, it often results in multiple court decisions before the changes or the effects of those changes can be accurately evaluated by those involved in commercial construction industry in Kansas.

The AGC would agree with the Kansas Bankers Association and other financial institutions who support this law to the extent that where a project is financed, the financing entity would normally have a first and prior lien. In most cases, this is not an issue because the project does not go forward until the financing is in place. The problem in the *Mutual Savings* case was that because of a change in ownership work had been done on the project prior to the mortgage being filed. We believe that under existing laws, there was a very clear means of protecting Mutual Savings' interest. Mutual Savings could have and should have obtained lien waivers from all of those who had performed any work on the project prior to



filing the mortgage. It is our understanding that it is common practice for financial institutions to determine exactly what work, if any, has been done on a project prior to filing a mortgage and obtaining lien waivers or lien subordination agreements pertaining to those entities. In this case, Mutual Savings simply failed to do that for whatever reason. We do not believe it is appropriate to change the lien laws to try and alleviate a situation that normally would not and should not occur.

The effect of the change advocated for K.S.A. 60-1101 would be to allow any party to change the preference date of all lien claimants after all of the encumbrances have been filed and during foreclosure procedures. This would involve what we believe would be a fairly drastic change in the lien laws which historically have stated that all mechanic's lien claimants are similarly preferred to the date of the earliest unsatisfied lien when the liens are filed. We do not believe that the law should be changed in reaction to a single case which involves a very unusual circumstance.

In short, the AGC takes the position that the amendment proposed to the lien laws in Senate Bill No. 112 is simply not necessary. There are existing ways for financial institutions to protect themselves when financing a project.