

MINUTES OF THE SENATE JUDICIARY COMMITTEE

The meeting was called to order by Chairman Vratil at 9:40 a.m. on January 16, 2003 in Room 123-S of the Capitol.

All members were present.

Committee staff present: Mike Heim, Kansas Legislative Research Department
 Lisa Montgomery, Office of the Revisor of Statutes
 Dee Woodson, Committee Secretary

Conferees appearing before the committee:

 Senator Barbara Allen
 Paul Morrison, Johnson Co. Dist. Atty.
 John Cowles, Johnson Co. Asst. Dist. Atty.
 Jon Stewart, President/CEO, Metcalf Bank
 Sheila Walker, Dir., Ks. Dept. of Revenue
 Chuck Stones, Sr. VP, Ks. Bankers Assn.
 Janet Schalansky, Secy. of SRS
 Paul Degener, Topeka

Others attending: see attached list

Chairman Vratil asked Vice Chairman Pugh to chair the Committee today due to his voice limitations. The Vice Chair called for bill introductions.

David Brant, Kansas Securities Commission, requests eight proposed bills be introduced; the first of which concerned securities fraud and the increase in criminal penalties and amending K.S.A. 17-1253(f). The second proposed bill relates to unregistered agents and amends K.S.A. 17-1254(f) to increase criminal penalties for offering or selling securities without being a registered broker-dealer, agent, investment adviser or investment adviser representative. The third bill involves unregistered securities, and would amend K.S.A. 17-1255(b) to increase the criminal penalties for unlawfully offering or selling securities. The fourth bill regards fines, and would amend K.S.A. 17-1266(a) to increase the maximum fine from \$5,000 to \$10,000 in administrative proceedings. The fifth proposed bill involves the scope of investigations, and would amend K.S.A. 17-1265 to enable securities investigators to investigate other criminal acts if discovered during the course of securities investigation. The sixth bill relates to financial statements and appraisals, and adding a new state law to prohibit influencing or misleading persons in the preparation financial statements or appraisals. The seventh bill concerns false filings, and amends K.S.A. 17-1264 to increase the criminal penalty for the filing of a false and misleading statement. The eighth bill involves the destruction of documents and retaliation against informants. (Attachment 1)

Senator O'Connor moved to introduce the proposed bills, seconded by Senator Umbarger, and the motion carried.

SB 16 - application requirements for drivers' licenses and identification cards

Vice Chairman Pugh opened the hearing on **SB 16**.

Senator Allen testified in support of **SB 16**, a bill she introduced. She explained the purpose of the bill, and stated it was to enhance public safety, protect Kansans' financial privacy, and reduce fraud losses to the retail businesses by strengthening the verifiability of state issued identification. She called the Committee's attention to a chart included in her written testimony, which showed what each state requires for driver's license and ID card issuance. The bill also proposes to increase the photo fee from \$2 to \$4 in order to cover the fiscal note of the bill. Senator Allen included with her written testimony an article

CONTINUATION SHEET

MINUTES OF THE SENATE JUDICIARY COMMITTEE on January 16, 2003 in Room 123-S of the Capitol.

entitled "Driver's License Integrity" published by CSG and NCSL, dated June 25, 2002 which talks about the importance of states verifying foundation documents. Senator Allen urged the Committee to pass **SB 16** as Kansas is far too lax about ensuring that driver's licenses's and ID cards are secure. (Attachment 2)

General questions included concerns about Kansas not verifying foundation documents, and biometric verification being done in other states and consideration for it being used in Kansas.

Conferee Morrison testified in support of **SB 16**, and spoke to the Committee in regard to increased "white collar" type crimes in the past few years. He said that the most notable was identity theft. Mr. Morrison also stated that Kansas was one of the most lax states in identification requirements for the issuance of a driver's license or state ID card. He concluded that this bill was simple and cost effective in helping prevent future crime and victimization. (Attachment 3)

Conferee Cowles spoke in favor of **SB 16** and his concern for the rapid increase of cases involving identity theft in Kansas because of the ease of immediately obtaining fraudulent State issued identification. Mr. Cowles gave several examples of drivers' licenses being used as ID cards. (Attachment 4)

Conferee Stewart testified in support of **SB 16** in order to curtail the lenient issuance of Kansas ID cards. Mr. Stewart spoke about how this problem is affecting the banking community, what measures they have to take to prevent crimes against innocent victims and businesses, and what the financial impact can be for the banks and victims. (Attachment 5)

Conferee Walker appeared before the Committee as a proponent for **SB 16**, and spoke in detail how this bill would give her department the tools to verify that a person is who they say they are. She said that the proposed legislation would eliminate the ability to have both a driver's license and a Kansas ID which foreigners do often with the present system. (Attachment 6)

General questions and discussion followed regarding the issuance of licenses to illegal immigrants and how that was rectified, what the mechanics will be for obtaining a new license, the issue of confidentiality, and concern over time required to verify all the required information before license or ID card is issued.

Conferee Stone testified in strong support of **SB 16**, and the use of biometric identifiers since they are the only true identifier of a person. In his detailed written testimony, Mr. Stone included articles regarding the rapidly increasing problem of identity theft. (Attachment 7)

Vice Chairman Pugh recessed the hearing on **SB 16** until the next Committee meeting.

The meeting was adjourned at 10:30 a.m. The next scheduled meeting is January 21, 2003.

SENATE JUDICIARY COMMITTEE GUEST LIST

DATE: Thursday, Jan. 16, 2003

NAME	REPRESENTING
Candy Shively	SRS
Jamie Corkhill	SRS
John Balger	SRS
David Brant	Securities Commissioner
Scott Schultz	Securities Commissioner
Alan Anderson	KMDR - Div of Vehicles
Sheila Walker	KDOR - DMV
Michael White	KCDAA
Margaret Deagle	SRS
Mike Norris	KS BANKERS ASSOC.
Chuck Stokes	"
PAUL DEGENER	CITIZEN
SCOTT SCHNEIDER	GIABA
Paul Jones	KSC
Kathy Olsen	KBA
Tom STEWART	METCALF BANK
Auni Hyten	JUDICIAL BRANCH
Paul Morrison	JS Co D.A.
John Cowles	JS Co DA

PROPOSED 2003 SECURITIES PENALTIES AMENDMENTS

Kansas Securities Commissioner

January 16, 2003

Proposal 1 - Securities Fraud: Amend K.S.A. 17-1253(f) to increase criminal penalties to severity levels 3 through 6 based upon the amount of loss rather than a single severity level 6 felony.

SECURITIES FRAUD	Current Severity Level with Sentencing Range for Defendant with No Prior Convictions		Proposed Severity Level with Sentencing Range for Defendant with No Prior Convictions	
\$1,000,000 or more	Level 6	17-19 months	Level 3	55-61 months
\$100,000 but less than \$1,000,000	Level 6	17-19 months	Level 4	38-43 months
\$25,000 but less than \$100,000	Level 6	17-19 months	Level 5	31-34 months
Less than \$25,000	Level 6	17-19 months	Level 6	17-19 months

Proposal 2 - Unregistered Agents: Amend K.S.A. 17-1254(f) to increase criminal penalties for offering or selling securities without being registered as a broker-dealer, agent, investment adviser or investment adviser representative to severity levels 4 through 7 based upon the amount of loss rather than a single severity level 7 felony.

Proposal 3 - Unregistered Securities: Amend K.S.A. 17-1255(b) to increase the criminal penalties for unlawfully offering or selling securities to severity levels 4 through 7 based upon amount of loss rather than a single severity level 7 felony.

Proposal 4 - Fines: Amend K.S.A. 17-1266a to increase the maximum fine from \$5,000 to \$10,000 in administrative proceedings.

Proposal 5 - Scope of Investigations: Amend K.S.A. 17-1265 to enable securities investigators to investigate other criminal acts if discovered during the course of securities investigation. This type of authority is already granted to law enforcement officers with other state agencies (Revenue, Lottery, and Racing and Gaming).

Proposal 6 - Financial Statements and Appraisals: Add new state law to prohibit influencing or misleading persons in the preparation of financial statements or appraisals.

Proposal 7 - False Filings: Amend K.S.A. 17-1264 to increase the criminal penalty for the filing of a false and misleading statement from level 10 to level 8.

Proposal 8 - Destruction of Documents and Retaliation against Informants: Add new state law to prohibit the destruction or falsifying of records and protect whistleblowers from retaliation for providing truthful information.

Senate Judiciary

1-16-03
Attachment 1-1

SENTENCING RANGE - NONDRUG OFFENSES

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

1-2

Probation Terms are:

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

Postrelease terms are:

- 36 months for felonies classified in Severity Levels 1 – 4
- 24 months for felonies classified in Severity Level 5 – 6
- 12 months for felonies classified in Severity Levels 7 - 10

Postrelease for felonies committed before 4/20/95

- 24 months for felonies classified in Severity Levels 1 - 6
- 12 months for felonies classified in Severity Level 7 - 10

LEGEND
Presumptive Probation
Border Box
Presumptive Imprisonment

BARBARA P. ALLEN
SENATOR, EIGHTH DISTRICT
JOHNSON COUNTY
9851 ASH DRIVE
OVERLAND PARK, KANSAS 66207
(913) 648-2704
STATE CAPITOL, ROOM 120-S
TOPEKA, KANSAS 66612-1504
(785) 296-7353



TOPEKA

SENATE CHAMBER

COMMITTEE ASSIGNMENTS
CHAIR: ELECTIONS AND LOCAL GOVERNMENT
MEMBER: ASSESSMENT AND TAXATION
FINANCIAL INSTITUTIONS AND INSURANCE

January 16, 2003

Mr. Chairman, Members of the Committee:

The purpose of S.B. 16, relating to driver's licenses and identification cards, is to enhance public safety, protect Kansans' financial privacy, and reduce fraud losses to our retail businesses by strengthening the integrity and verifiability of State-issued identification.

Attached to my testimony is a chart that shows what each state requires for driver's license and i.d. card issuance. Today, Kansas is one of the easiest states in the nation in which to obtain false identification. There are no security measures in place to protect Kansans, to ensure the person applying for a driver's license or i.d. card really is that person. A simple photograph yields an instant, permanent piece of government issued identification.

S.B. 16 would strengthen the security requirements for obtaining a driver's license or i.d. card in Kansas by:

1. Requiring that all applicants for a driver's license or i.d. card submit their s. s. # to obtain identification. Applicants would receive a temporary license or permit (or i.d. card) until the DMV verifies the identity of the applicant, at which time permanent i.d. would be issued.

Senate Judiciary

1-16-03
Attachment 2-1

The bill specifies “the distinguishing # assigned to the license or permit (or i.d. card) may be the applicant’s s.s. # if the applicant so requests in writing.” (p. 2, lines 8-10.) Thus, the s.s. # can only be placed on the driver’s license if requested in writing by the applicant.

2. No longer allowing a person to legally possess both a current valid Kansas driver’s license, and a current valid i.d. card. A person who has both can easily give one to someone else for an illegal purpose, and there is no reason why someone should have both simultaneously.

3. Requiring that after July 1, 2004, no driver’s license shall be valid until a colored photograph of the licensee has been taken and verified before being placed on the license. As you know, a color photo is already required in order to obtain a driver’s license.

This new verification language would allow the DMV to employ software to ensure a one-to-one match on photos (the David Adkins applying today is the same one who applied six years ago), and a one-to-many match on photos (David Adkins is not obtaining multiple ID’s under different names.) Basically, photos would be electronically compared and matched to ensure ID verification.

4. Increasing the photo fee from \$2 to \$4. This fee increase is necessary to cover the fiscal note of the bill.

- a. The first \$1 would cover DMV costs to verify the applicant’s s.s. # and color photograph.
- b. The second \$1 would cover DMV costs to verify “foundation documents” or “source data”.

An article entitled “Driver’s License Integrity” published by CSG and NCSL, dated June 25, 2002, talks about the importance of states verifying foundation documents:

Current Issues
Integrity of License Issuance

“All states verify the identity of a potential license holder before issuing a driver’s license. The documents used to verify identity for this purpose are known as “foundation documents” because they provide the building blocks of personal information on which the license is issued.

Foundation documents range from birth certificates, to utility bills, to passports, to other state’s driver’s licenses. The principal challenge related to foundation documents is states’ ability to verify their authenticity and validity.

States do not routinely verify, for instance, that the foundation documents with which they’re presented are authentic (i.e. that the document is genuine) or valid (i.e. that the document is eligible to be used). States must increase their ability to verify the authenticity and validity of foundation documents. Currently, few states actively verify foundation documents.”

With the passage of SB 16, Kansas would become one of the few states currently verifying foundation documents, and would thus greatly strengthen the security of our State-issued identification. After all, if the foundation upon which an applicant’s identity is based is false, then we cannot reliably verify the applicant’s identity either.

Driver’s licenses are much more than a license to drive – they allow us to open bank accounts, cash checks, write

merchants checks, and step onto airplanes. They are the most widely used domestic document to verify a person's identity.

Kansas is far too lax about ensuring that driver's license's and i.d. cards are secure. I urge this Committee's passage of S.B. 16. Thank you, Mr. Chairman. I will stand for questions.

DRIVER LICENSE AND ID CARD ISSUANCE - 2002

STATE	Issuance Type	Digital Technology	Original Digital System Installation	Finger or Thumbprint Capture	Biometric Verification	SSN Required	Electronic SSN Verification	Legal Presence Required *	Electronic Legal Presence Verification	Annual DL/ID's Issued	Total DL/ID Records
Alabama	Central	Photo & signature	Jun-97	No	No	Yes	on-line	Yes	No	1,149,000	4,670,000
Alaska	Instant	N/A	N/A	No	No	Yes	No	No	No	180,000	500,000
Arizona	Instant	Photo & signature	Jun-95	No	No	Yes	on-line	Yes	No	1,244,000	5,513,000
Arkansas	Instant	Photo, fingerprint & signature	Oct-94	voluntary, right index, electronic	voluntary, right index fingerprint	Yes	No	Yes	No	600,000	1,900,000
California	Central	Photo, thumbprint & signature	Mar-91	mandatory, right thumb, electronic	facial/thumbprint being considered	Yes	batch	Yes	on-line	6,409,000	24,167,000
Colorado	Both	Photo, fingerprint & signature	1994	mandatory, right index, electronic	right index fingerprint and facial in July 2002	Yes	on-line July 2002	Yes	on-line July 2002	1,400,000	4,145,000
Connecticut	Instant	Photo & signature	Jun-92	No	Facial implementation in September 2002	Yes	No	No	No	840,000	2,300,000
Delaware	Instant	Photo & signature	Apr-95	No	No	Yes	No	Yes	No	200,000	760,000
Dist. of Columbia	Instant	Photo & signature	Aug-00	Being considered	facial recognition	Yes	on-line	Yes	No	120,000	470,000
Florida	Both	Photo & signature	Nov-95	No	No	Yes	No	Yes	No	5,367,000	14,346,000
Georgia	Both	Photo, fingerprint & signature	Sep-96	mandatory, left & right index, electronic	left & right index fingerprints	No	No	Yes	No	2,400,000	5,700,000
Hawaii	ID-Instant DL-Both	Photo, thumbprint (DL), fingerprint (ID) & signature	DL - 1990 ID - 1998	mandatory, right thumb (DL), left & right index (ID), electronic	No	Yes	No	No	No	ID-60,000 DL-300,000	ID-370,000 DL-788,000
Idaho	Instant	Photo & signature	Nov-01	No	No	Yes	on-line	Yes	No	391,000	901,000
Illinois	Instant	Photo & signature	Jan-99	No	facial recognition	Yes	Being considered	No	No	3,650,000	11,700,000
Indiana	Instant	Photo & signature	1999	No	No	Yes	No	No	No	1,700,000	6,362,000
Iowa	Both	Photo & signature	Dec-95	No	No	Yes	Being considered	No	No	1,025,000	2,913,000
Kansas	Instant	Photo & signature	Jul-94	Being considered - unknown at current	Being considered - unknown at current	CDL only	Being considered	Yes	Being considered	750,000	1,975,000
Kentucky	Instant	Photo & signature	Dec-01	No	facial recognition being considered	Yes	Being considered	Yes	Being considered	1,951,000	2,900,000
Louisiana	Instant	Photo & signature	Jun-95	thumb, electronic being considered	facial recognition being considered	Yes	Both	Yes	No	1,062,000	3,624,000
Maine	Central	Photo & signature	Oct-99	No	No	Yes	on-line	Yes	No	240,000	900,000
Maryland	Both	Photo & signature	Nov-90	No	facial recognition being considered	Yes	on-line	Yes	Being considered	1,300,000	3,700,000
Massachusetts	Central	Photo & signature	1993	No	No	Yes	on-line	Yes	Being considered	1,000,000	5,100,000
Michigan	Central	Photo & signature	Apr-98	No	No	Being Considered	Being considered	No	Being considered	2,200,000	7,500,000
Minnesota	Central	Photo & signature	Jun-94	No	No	CDL only	No	No	No	1,500,000	DL-3,582,000 ID-222,000
Mississippi	Instant	Photo & signature	Jul-96	Being considered	facial recognition being considered	Yes	on-line	Yes	No	740,000	2,100,000
Missouri	Both	Photo & signature	Sep-96	No	No	Yes	on-line	Yes	No	1,893,000	4,852,000
Montana	Central	Photo & signature	1993	No	No	Yes	No	Yes	No	150,000	680,000
Nebraska	Instant	N/A	Est. 2003	No	facial recognition being considered	Yes	on-line	No	No	547,000	1,213,000
Nevada	Instant	Photo & signature	Apr-02	No	No	Yes	on-line	Yes	No	860,000	1,731,000
New Hampshire	Instant	Photo & signature	1993	No	No	Yes	No	Yes	No	265,000	955,000

DRIVER LICENSE AND ID CARD ISSUANCE - 2002

STATE	Issuance Type	Digital Technology	Original Digital System Installation	Finger or Thumbprint Capture	Biometric Verification	SSN Required	Electronic SSN Verification	Legal Presence Required *	Electronic Legal Presence Verification	Annual DL/ID's Issued	Total DL/ID Records
New Jersey	Both	N/A	N/A	No	No	Yes	Being implemented	No	Being considered	2,128,000	6,080,000
New Mexico	Instant	Photo & signature	1998	No	Being considered, unknown which type	Yes	Being considered	Yes	Being considered	468,000	1,500,000
New York	Central	Photo & signature	Nov-92	No	facial/fingerprint being considered	Yes	on-line	Yes	No	4,234,000	11,850,000
North Carolina	Instant	Photo & signature	Sep-96	No	facial recognition being considered	Yes	Being considered	No	No	1,248,000	7,085,000
North Dakota	Both	Photo & signature	Jan-96	No	No	Yes	No	Yes	No	180,000	480,000
Ohio	Instant	Photo & signature	Feb-95	No	No	Yes	batch	Yes	No	3,100,000	8,500,000
Oklahoma	Instant	N/A	N/A	Being considered, w/AAMVA standards	facial & thumb print being considered	Yes	Being considered	Yes	No	935,000	2,298,000
Oregon	Instant	Photo	Jun-97	No	No	CDL only	No	No	No	826,000	DL-2,675,000
Pennsylvania	Both	Photo & signature	1994	No	No	Yes	Being considered	Yes	No	4,129,000	8,204,000
Rhode Island	Instant	Photo & signature	In six months of 3/2002	no	Being considered, unknown which type	No	No	No	No	280,000	650,000
South Carolina	Instant	Photo & signature	Nov-93	No	No	Yes	Being considered	Yes	No	800,000	3,000,000
South Dakota	Both	Photo & signature	May-90	No	No	Yes	on-line	Yes	No	200,000	555,000
Tennessee	Both	Photo & signature	Aug-96	No	No	Yes	on-line	No	No	1,400,000	6,100,000
Texas	Central	Photo, signature & thumbs	Mar-95	mandatory, both thumbs, electronic	thumbprint being considered	DL only	Being considered	No	No	6,250,000	17,000,000
Utah	Central	Photo & signature	Sep-02	No	No	Yes	Being considered	No	No	430,000	1,900,000
Vermont	Instant	Photo & signature	1993	No	No	Yes	No	No	No	90,000	450,000
Virginia	Both	Photo & signature	1991	No	No	DL only	batch	No	No	1,000,000	5,500,000
Washington	Central	Photo & signature	Jun-01	No	No	Yes	on-line	No	No	1,600,000	4,711,000
West Virginia	Instant	Photo, fingerprint & signature	Jan-98	voluntary, right index, electronic	voluntary right index & mandatory facial	Yes	No	No	No	461,000	1,352,000
Wisconsin	Instant	Photo & signature	Oct-97	No	facial recognition being considered	Yes	Being considered	No	No	1,237,000	4,110,000
Wyoming	Central	Photo & signature	Apr-93	No	No	Yes	on-line	Yes	on-line	135,000	406,000

Additional Information:

Georgia is over the counter for renewals and centralized for first time applicants.

Louisiana uses batch SSN processing for existing DL-ID records and on-line processing for new (original) DL-ID records.

Nevada expects to be digitized by mid 2002.

New Jersey expects to be digitized by April 2003.

Maryland has over the counter transactions for walk-ins and centralized issuance for drivers renewing while absent from the state.

Ohio currently uses batch processing for SSN up till July or August 2002. By then, they anticipate using on-line verification.

Rhode Island is working on proposal to digitize.

Virginia uses centralized method for juveniles and instant for everyone else. SSN is not required for acquiring an ID and only required for DL applicants who have one.

Washington issues black & white temporary photograph when customer is at a DMV office. SSN on-line verification only used when fraud is suspected.

Abbreviations: CDL - Commercial Driver License; DL - Driver License; ID - Identification Card; N/A - Not Applicable; SSN - Social Security Number

Source of information: Survey by California Department of Motor Vehicles in mid February, 2002 with follow-ups from March through May, 2002. Legal presence requirement information from AAMVA.

questions: Contact Steve Fong (916) 657-8715 or sfong@dmv.ca.gov, California Department of Motor Vehicles, Licensing Operations Division.

* Legal Presence Requirements Map, produced by AAMVA 02/2002.

Testimony to the House Judiciary Committee

Regarding Senate Bill 16

Paul J. Morrison, District Attorney - Tenth Judicial District
January 16, 2003

I have been a prosecutor for 22 years. I've been the District Attorney in Johnson County for 14 years. During my career I've prosecuted just about all types of crimes and studied and watched various crime trends. One of the most disturbing trends I've noticed in the past few years is the emergence of well thought out, deliberate "white collar" type crimes that are highly destructive to individuals, businesses and our society. Most notable of these is identity theft. We have seen a literal explosion of this type of crime, both in Johnson County and across the state.

I've heard much said over the last few years about problems with fraudulently produced and altered drivers' licenses. In most states this is a big issue as driver's licenses are the most commonly used form of identification to open bank accounts, fill out credit applications, etc. In Kansas, however, our problems are a bit different. Fraudulent and altered drivers' licenses don't seem to be such a big problem here because one can easily get authentic Kansas drivers' license using phony identification. As such, I suspect many crooks think, "why should I alter a driver's license when I can get a real one so easy?" It's for this reason that we are so supportive of Senate Bill 559. This bill addresses a simple change that will make it much more difficult for criminals to obtain a Kansas driver's license or ID card using phony identification, the requirement of a social security number by the applicant. Most of you probably don't know that among states Kansas is one of the most lax in identification requirements for the issuance of a driver's license or state ID card. By simply requiring a social security number and allowing some time for the Department of Motor Vehicles to verify that number before issuance of a permanent driver's license will be one of the most effective steps we can take in fraud prevention.

As you will hear today, the cost of implementing this bill is minimal.

This bill in its most basic form is extraordinarily simple and cost effective. It will go a long way in preventing future crime and victimization.

Senate Judiciary

1-16-03
Attachment 3-1

Testimony to the House Judiciary Committee

Regarding Senate Bill 16

John E. Cowles,
Assistant District Attorney, Johnson County, Kansas

THE ACCELERATING PROBLEM OF IDENTITY THEFT

In 2001, there were 476 victims of Identity Theft in Kansas who reported their cases to the Federal Trade Commission. The Johnson County District Attorney's Office filed cases against 45 defendants alleging Identity Theft in 2002, up from 32 cases the year before, and the pace so far in 2003 is more than one new case of Identity Theft filed every week in Johnson County.

THE CONSEQUENCES TO VICTIMS OF IDENTITY THEFT

The Kansas Legislature recognized the severe consequences to victims of Identity Theft when the criminal statute (K.S.A. 21-4018) was amended in 2000 to increase the severity level of the crime to a level 7 person felony. It is not uncommon for victims of Identity Theft to work at repairing their credit ratings and other financial identity for more than a year after falling victim to an identity thief. In the meantime, they suffer the frustrations of having their checks and credit cards declined by merchants. Sometimes the consequences are much more severe, such as subjecting the innocent victim to arrest by law enforcement for crimes committed by the identity thief using the victim's identification, and denial of medical treatment because the identity thief has abused narcotic prescriptions in the name of the victim. The Kansas Identity Theft statute was an effective first step in combating Identity Theft. However, much more can and should be done to deter the perpetrators and improve detection of their crimes.

Senate Judiciary

1-16-03
Attachment 4-1

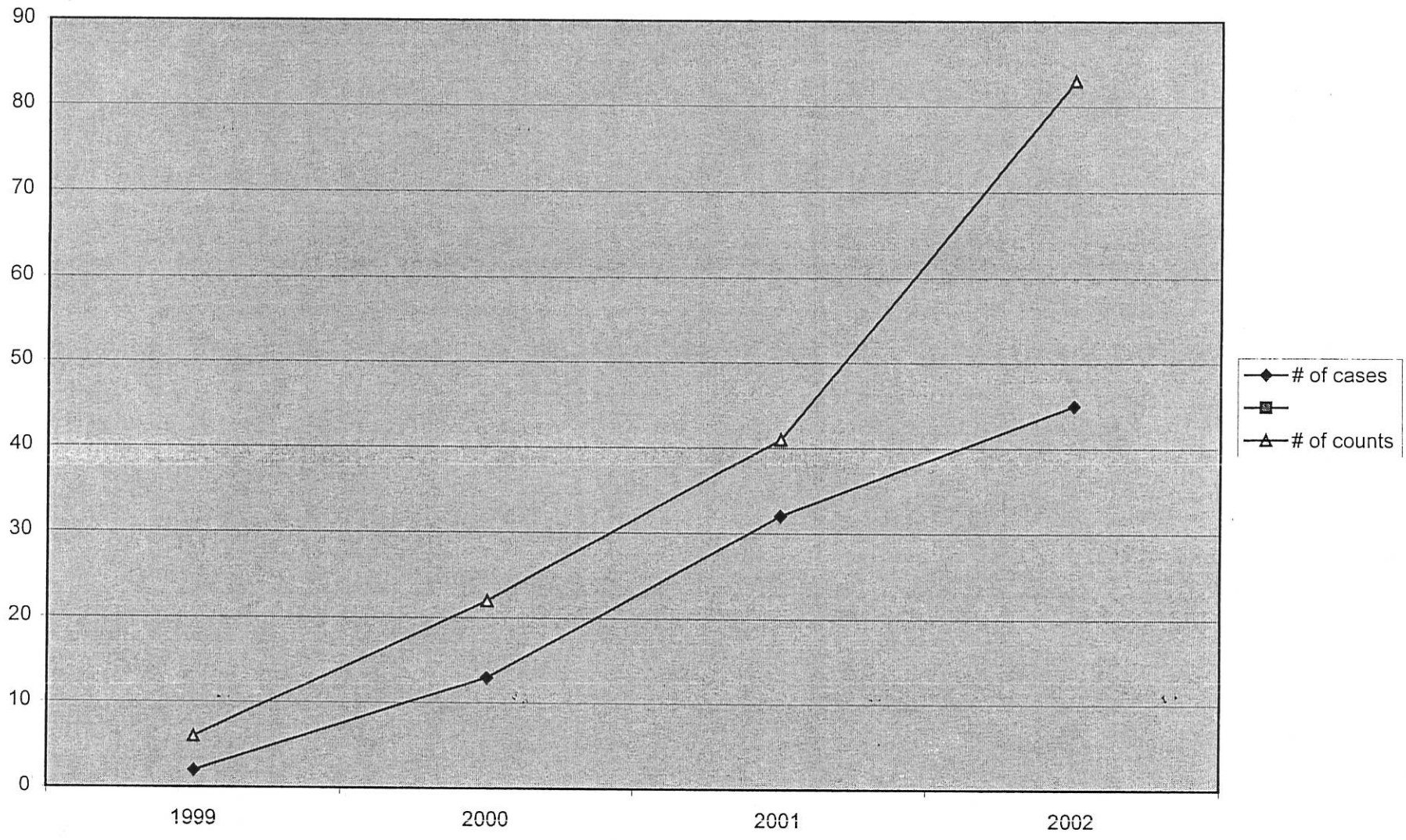
WHY IDENTITY THIEVES COME TO KANSAS

In addition to experiencing the rapid increase of cases involving Identity Theft, law enforcement has recognized a trend in which Identity Theft is being perpetrated in Kansas by persons from other States using stolen victim information from other States. Through interviews of perpetrators, a common explanation for traveling to Kansas is the ease of immediately obtaining fraudulent State-issued identification. Obtaining fraudulent State-issued identification is essential to the identity thief because the identification is necessary in opening bank accounts, applying for credit cards and obtaining instant credit. Investigating and prosecuting Identity Theft rings from distant States is extremely burdensome for both law enforcement and prosecutors, as the perpetrators often flee to their home states before the crimes are detected, and the individual victims are located in a distant State. However, Kansas banks and retailers frequently bear the financial losses from the Identity Theft schemes, which often reach \$100,000 or more after a well-organized ring has left the area. This results in much higher investigation costs, extradition costs, and expenses associated with bringing witnesses to Kansas to convict the perpetrators.

SECURE DRIVER'S LICENSES AND ID CARDS WILL DETER CRIME

Kansas is one of only a few remaining States that will provide any applicant an immediately issued driver's license or identification card, with no requirement of a social security number, no fingerprint, and no other biometric information. The absence of these safeguards is an open invitation to identity thieves to come to Kansas, cause enormous economic damage, and create difficult and expensive police investigations and prosecutions.

Identity Theft filings in Johnson County, Kansas



Kansas State Senate Committee on Judiciary

*Testimony of Jon L. Stewart, President & CEO
Metcalf Bank, Overland Park
January 16, 2003*

Senate Bill No. 16

Good morning. Thank you for the opportunity to address the Committee today on the topic of fraudulent IDs.

As noted, I represent Metcalf Bank, which has six locations in Johnson County and one in Miami County. Throughout the 40-year history of our institution, we have taken pride in offering customer-friendly service.

But please consider this. When an individual approaches one of our associates, makes a request to open a new account and then hands us an *official* Kansas Identification Card, one of the first thoughts that crosses our minds is, "Criminal activity."

And you know what? Most of the time we're right.

Certainly this is not the frame of mind we want to be in when dealing with a potential new customer . . . with any customer. Metcalf Bank strives to serve every customer in the friendly, unbiased manner of a community bank. That is our niche and sets us apart from our competitors.

But we know from experience that a high percentage of Kansas Identification Cards presented to our employees are illegitimate. These IDs are used fraudulently by criminals to procure funds from counterfeit checks, to raid the account of an unsuspecting victim or to obtain cash and checks.

We respect the original intent of the Kansas ID card program, which is to provide genuine identification to those who cannot obtain a driver's license, namely elderly or disabled persons. But the truth is, rarely do users of Kansas IDs fit this mold. It's not uncommon for users of these identification cards to drive to the front door of the bank and then present a Kansas ID card showing they have no driving privileges.

Such blatant criminal behavior is made possible by what we believe is a lenient issuance process. The State of Kansas is among the most permissive when it comes to distributing identification cards.

The application process for a Kansas identification card requires no Social Security number, no electronic Social Security number verification, no finger- or thumb-print capture. Applicants need only present a photo and signature to obtain an official identification card.

The system is literally inviting criminals to take advantage of it. And they are

Senate Judiciary

1-16-03

Attachment 5-1

This situation puts a great deal of pressure on the banking community. We have become part of the front lines of defense in identifying and, to some extent, capturing these criminals. In 2001, for example, our bank was involved in the arrest of two eastern European men attempting to open a bank account with a Kansas ID Card and a counterfeit passport. An arrest was made in the lobby of one of our banks.

Uncommon? Hardly. Our bank reports instances frequently where a Kansas ID is presented for fraudulent purposes. There have been times when these people have been arrested in our lobbies and escorted out in handcuffs.

And don't overlook the financial impact. I can tell you that Metcalf Bank's losses from fraud involving Kansas ID cards in 2001 and 2002 greatly exceeded theft from outright robberies. But we consider fraudulent use of ID cards to be robbery in its own right. And we expend time, energy and funds to guard against it. We know from experience that criminals are reluctant to provide any information that may tie them to a crime. In July 1999, Metcalf Bank joined other Kansas banks in a thumb print program for non-customer check cashing. Prior to this program we experienced frequent and significant losses due to criminals presenting and cashing checks stolen or counterfeited from our customers. Since implementing the program this form of criminal activity is non-existent at our bank. Today criminals complete the same type of crime by simply obtaining a state issued identification card and using that card to open a checking account.

While bank fraud losses number in the thousands of dollars because of fraudulent IDs, we acknowledge it is Kansas retailers who suffer the most damage from these ID abuses. When a retailer submits a check for payment to our bank and there are no funds in the account to cover the amount, we simply return the check to the retailer. When those checks are accepted based on a fraudulent ID, the retailer has no recourse other than to pass these costs on to their customers in the form of higher prices.

In closing, let me say that Kansas bankers are being forced to scrutinize and deal cautiously with the legitimate users of Kansas Identification Cards. It's not fair to these law-abiding citizens. It's not fair to us. It's not fair to Kansas.

Please help us protect our communities, our customers and our employees. Our experience indicates that law-abiding citizens do not have a problem providing proof of identity. We encourage you to change the process currently used in issuing Kansas identification cards and Kansas Drivers licenses.

Thank you. I will be happy to answer any questions you may have.



K A N S A S

JOAN WAGNON, ACTING SECRETARY

DEPARTMENT OF REVENUE
DIVISION OF VEHICLES

KATHLEEN SEBELIUS, GOVERNOR

TO: Chairman John Vratil
Members of the Senate Judiciary Committee

FROM: Sheila J. Walker, Director of Vehicles

DATE: January 16, 2003

SUBJECT: Senate Bill 16 – Identity Security

Mr. Chairman, members of the committee, I am Sheila Walker, Director of the Kansas Department of Revenue's Division of Motor Vehicles (DMV). Thank you for allowing me to testify on Senate Bill 16.

As you might expect, law enforcement, retailers, bankers and others rely on the Kansas DMV for verification that the person before them is who they say they are. This bill gives the Division the tools to do that.

Under this bill, each applicant shall submit a Social Security number to the Kansas DMV, and we are then required to verify that number, before issuing a driver's license, instruction permit, or ID card. The Social Security number shall remain confidential and will not be placed on the driver's license, instruction permit or ID card unless the applicant requests so in writing. At a one-time cost of \$20,000, we can install numeric keypads to enable applicants to privately enter their own Social Security number, so it does not have to be shared with examiners or overheard by the public. If the applicant does not have a Social Security number, the applicant must submit a sworn statement indicating that he or she does not have one. Of course, applicants do not have to have a Social Security number to drive, but if they provide us one, we will verify it.

This bill endorses the DMV's ability to take the time necessary to verify all information presented, prior to issuing a driver's license or ID card. The applicant is to receive a temporary driver's license, instruction permit or ID card until we are able to verify all facts, including Social Security number, age, identity, and residency. Additionally, no applicant would be able to hold both a valid driver's license and ID card at the same time. Identity verification would include photo comparisons to ensure that the individual applying today is the same one that applied six years ago, and is also designed to catch individuals trying to obtain multiple IDs.

Finally, the bill increases the photo fee from \$2 to \$4, generating \$1.5 million annually, to pay for costs associated with photo comparison software, as well as Social Security, age and residency verification.

Senate Judiciary – SB 16

Page 2

January 16, 2003

While these proposed changes to Kansas' licensing laws are all in line with the national recommendations for tighter security, we recognize the big picture – before the driver's license became proof of identity (enabling Kansans to open bank accounts, write checks, and so on) it was proof that they passed the vision, written, and the behind-the-wheel drive tests. Not only do we have an interest in ensuring identity, driving safety is equally important.

Thanks again for the opportunity to testify on Senate Bill 16. I would be glad to try to answer any questions you may have.



The Kansas Bankers Association

1-16-03

TO: Senate Judiciary Committee
FROM: Chuck Stones, Senior Vice President

RE: SB 16

Mr. Chairman and Members of the Committee,

Thank you for the opportunity to appear before you in strong support of SB 16. SB 16 would help assure that the person represented by a State issued drivers license or ID card is the actual person.

ID THEFT IS A CRIME OF MAJOR PROPORTIONS AND IS BECOMING A NATIONAL SECURITY ISSUE -

Identity theft has been called the fastest growing and largest monetary crime in the US today. The complementary crime of check fraud is a huge problem. Even beyond ID theft is the whole issue of positive identification verification. People try to conceal or change their ID for a wide variety of reasons. There should be a more stringent process to get an official state issued identification card. Individuals and businesses in Kansas and other states rely on these cards as correct identification. Kansas has a duty to do everything within its power to ensure that people to whom it issues any identification card is, in fact, the person they say they are.

The article from Time Magazine attached to my testimony points out that some consumer advocates estimate that as many as 750,000 identities are stolen every year. Most are stolen for personal financial gain, but some are stolen for other larger crimes. The Time article points out that people steal identities to mask their participation in a crime. The article from the ABA newspaper points out that ID theft is growing national security issue and that Congress has recognized that financial fraud and ID theft "continue to play a large role in funding the terrorist cells in this country."

THE MYTH OF CONSUMER PROTECTION -

The Legislature is NOT protecting the consumer by ignoring this problem. According to a recent AP story, ID theft is the fastest growing consumer crime and accounts for more than 40% of consumer-fraud complaints. Passing provisions such as this is protecting the consumer.

As you will remember the discussion of last years HB 2296, the bill that increased the penalties for check forgery and fraud, the crime of check forgery and fraud is a huge problem for every citizen, either directly or indirectly.

- According to the Wichita Business Journal, there were **\$8 million worth of check forgeries** written in Wichita in 1999; and detectives in the Topeka Police Department's Financial Fraud Unit tell us they are aware of \$2 million worth of check forgeries written in Topeka in 2000.
- According to a GAO report, "Identity Theft Available Data Indicate Growth in Prevalence and Cost", community bankers report that identity theft attributed to 56% of all check fraud.
- Forgeries involve **multiple victims**: the person whose checks were stolen, the business that cashed the check and the bank where the account is drawn on. All parties potentially face huge losses when checks are forged. In addition, losses occurred by banks and other businesses get passed on to the innocent consumer as the cost of doing business increases.

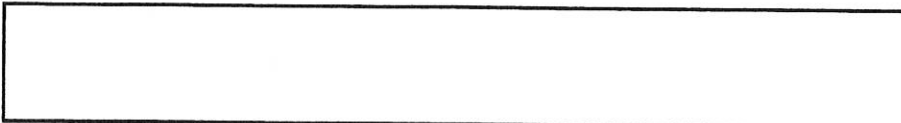
BIOMETRIC WORKS –

Biometric identifiers are the ONLY true identifier of a person. The KBA is among a large number of states where some banks require a thumbprint to cash a non-customers check. In the first year of the program fraud was decreased by approx 60%.

At the national level the Homeland Defense Dept. and the Attorney General office is actively investigating the use of biometric identifiers to help assure the security of the United States.

Biometric identifiers may sound a little out on the edge, but are being used increasingly to stop fraud and as the only true way to ensure identity.

We believe that SB 16 would go a long way in helping reduce this crime and we urge your support.



HOME | FEDERAL COMPUTER WEEK | GOVERNMENT E-BUSINESS | TECHNOLOGY | EVENTS | LINKS | DIRECTORY |

SEARCH THE SITE

Search input field with a 'go' button

Advanced Search

ALSO ONLINE

- Agenda
- Letters Archive
- Online Archive
- Print Editions
- Special Reports
- Milt Zall Archives

NEWS BY TOPIC

- Accessibility
- CIOs
- City
- Columns
- County
- Defense
- Democracy
- E-Government
- Funding
- Homeland Defense
- Industry
- Intergovernmental
- International
- Policy
- Privacy
- Procurement
- Records Management
- Schools
- Seat Management
- Security
- State
- Technology
- Telecom
- Training
- Workforce

READER SERVICE

- Advertise
- Contact us
- Editorial Calendars
- E-mail Newsletters
- Linking to us
- Links Disclaimer
- Online Permission



Ridge: Link driver's license, visa

BY William Matthews
March 15, 2002

Printing? Use this [version](#).
[Email this to a friend.](#)

The Office of Homeland Security is urging states to establish tighter control over foreign visitors by issuing driver's licenses that expire when visas expire.

The office is drafting model legislation to require that driver's licenses issued to non-citizens be tied to visas, homeland security spokesman Gordon Johndroe said March 14. The model is to be sent to the states for consideration by legislatures.

In recent weeks, Tom Ridge, director of the Office of Homeland Security, has been encouraging governors and other state officials to take steps to improve the security and authenticity of driver's licenses.

In a conference call with state officials March 7, Ridge told state emergency management officials that he hopes motor vehicle departments can be electronically linked to databases maintained by the federal Immigration and Naturalization Service. That would enable state workers to check the immigration status of foreign nationals who apply for driver's licenses and issue licenses that would expire when visas expire.

Such capability also could enable the states to help keep better track of visiting foreigners.

INS has asked Congress for \$380 million to build an entry and exit data system to keep track of foreign visitors. The system may include biometric identification information such as fingerprints or eye scans of visa holders. Such information also could be included on driver's licenses.

Ridge's telephone remarks came about 10 days after he urged governors attending a National Governors Association meeting to draft model legislation setting standards for more secure licensing procedures. By coming up with their own standards, Ridge said, the governors would avoid having standards forced on them by Congress.

Driver's licenses became a source of concern after the Sept. 11 terrorist attacks because most of the terrorists used such licenses — obtained

["Driver's licenses get another look"](#) [Federal Computer Week, Jan. 21, 2002]

["ID card plan assailed"](#) [Federal Computer Week, Feb. 18, 2002]

["System proposed to track foreigners"](#) [FCW.com, Jan. 31, 2002]

Advertis



Do it c

There are
things you
don't see
To stay f
the govern
IT comm
turn
FCW.COM
breaking



Identity Theft ^{*} ↙

Evolving Into a National Security Issue

By John Ginovsky

Raise your hand if you, or anyone you know, have had a credit card or other bank account abused by a complete stranger — in other words, have become a victim of identity theft.

The odds are, your hand is raised.

That's the experience of Robert Douglas, an identity theft expert who's talked with thousands of people around the country, and who has advised numerous banks and federal agencies about the subject.

"When I talk to groups and ask if anybody has been a victim or knows a victim, it's always more than 50 percent of the [attendees], and sometimes substantially more," Douglas said.

(Douglas, who is CEO of American Privacy Consultants Inc., Alexandria, Va., will speak on this subject during the ABA Regulatory Compliance

Conference, June 2-5, in New Orleans. For more information, call 1-800-BANKERS.)

Since Sept. 11, identity theft has taken on a much more sinister, much more serious aspect than before.

"Congress is aware that financial fraud and identity theft ... continue to play a large role in funding the terrorist cells in this country," Douglas said during ABA's recent teleconference, "Identity Theft: Protect Your Customers and Your Bank."

"And it's no mistake that one of the first [private

sector entities] on Sept. 12 that President Bush called upon to act in this regard was the financial services industry," he added.

To that end, Douglas stressed, "This issue needs to become just

that this is going to become a priority in the banking industry."

Douglas generally advises banks to concentrate on four "T's" when putting into place an effective anti-identity theft program.

■ Teach awareness — "Employees need to know

why this is important, why this is a priority, from financial losses to the institution and also to the damage it's doing to American

See Identity Theft/Page 2

ID THEFT

as important as sales and marketing in banks. Compliance departments and security departments need more resources. Mostly they need more direction from the board of directors on down,

TipOff



AMERICAN BANKERS ASSOCIATION®

World-Class Solutions,
Leadership & Advocacy
Since 1875

Identity Theft Help

The Federal Trade Commission has unveiled a new form to help victims of identity theft.2

Credit Union Monitor

ABA's Keith Leggett explains why federal credit unions should directly compensate their boards.3

Grassroots Lobbying

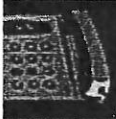
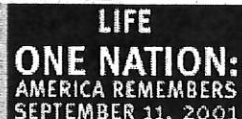
ABA's Sharon Raymond discusses the importance of bankers' involvement in political advocacy.5

NewsBriefs2-3
Editorial6

Consumer Connection ...6
ViewPoints7

Ask Don7
Technology Update8

Welcome!

[N Netscape](#) [Mail](#) [Maps](#) [IM](#) [Search](#)[★ Academy Awa](#)**Big Savings For Small Businesses!****JOIN NOW!**

TIME.com

nation

Wednesday, Jan. 23, 2002

Identity Theft: Could it Happen to You?

New statistics suggest it may be only a matter of time. A security expert offers tips on protecting yourself

BY [JESSICA REAVES](#)

Imagine this: Someone out there knows your name, your credit card information, your bank account numbers and your social security number. They are pretending to be you — running up outrageous bills, even committing crimes — and as far as your banks, creditors and various authorities are concerned, they *are* you.

It may sound like the plotline of a hackneyed Hollywood thriller, but hundreds of thousands of Americans may have already been victims of identity theft. Last year alone, the Federal Trade Commission logged more than 85,000 complaints from people whose identities had been pirated. That may only be the tip of the iceberg; some consumer advocates suggest as many as 750,000 identities are stolen each year.

See pgs 2

What, exactly, is identity theft? How does it happen? And how can you protect yourself against this growing trend? TIME.com spoke with Ted Claypoole, a technology lawyer concentrating in financial services and security at the firm of Womble Carlyle Sandridge and Rice in Charlotte, North Carolina.

TIME.com: You don't seem particularly shocked by these figures.

Ted Claypoole: No, I'm not. It's actually frighteningly easy to steal someone's identity in this day and age. And the key is in the numbers that have come to identify all of us.

Your online identity consists of numbers and other information that describes you — it's not really you, of course, but to anyone online it is

7-5

you. In other words, if someone can use your social security number, which is really the key to identity theft, and find your financial information, like a bank account number or credit card number, they can begin to build an identity of someone online who has a lot of your characteristics.

So what pieces of information are particularly key to identity?

There are three basic ways to authenticate oneself: One is something you know. Two is something you have. Three is something you are.

Something you know is easy: it's a password, a personal identification number that no one else should have. Something you have is an ATM card or an ID card at work. Something you are can be your handwriting, your fingerprint or your DNA sample, depending on how detailed you want to get. Some very advanced systems use GPS to pinpoint where you are, but that's a different level of technology. *

Anyone who understands identity theft knows these things — so if they can get hold of this information, they can fake your identity.

Many people are particularly concerned about using credit cards to make online purchases. Is it safer to use credit cards in person than online?

I don't see a bigger problem with using a credit card online than using it offline. It's just as big a risk to make a credit card transaction at a restaurant as it is to make a transaction on a trusted web site.

What's the motive behind identity theft? I can imagine people wanting to steal money, but beyond that I'm at a loss.

You're right, the purpose is generally to steal money, or account information, or credit, or someone's good name.

Another reason people steal identities is to mask their participation in a crime. The more convincingly a criminal can establish he is someone else, the more likely it is the authorities won't come after that criminal. *

Okay. Now for the important information. What can any of us do to shield ourselves from identity theft?

There are things that are standard, generally accepted methods of keeping information secure that lots of people don't follow.

- Using credit cards is generally safer than allowing access into other accounts. The credit card system has safeguards built in to protect users from fraud. If someone steals your credit card number, you're out 50 bucks and

7-6

5

some hassle. With a debit card, you could be cleaned out completely. Using cash is also not a bad thing.

- Never give out your social security number. Except for government or big-ticket items, no one should be asking for that number. Credit card numbers and social security numbers should never be used to make charitable contributions.
- Never give out any information about yourself over the phone, particularly to anyone who's called you.
- Try to avoid writing your bank account numbers on anything.
- Rip up pre-approved credit card notices, because that's one of the ways this can happen — they'll take the notice, change the address, and build credit using your name and identity.
- Read your bank statements. You'd be amazed by how many people just toss those statements without checking for strange transactions.

Some people are going to read this and start worrying about shredding every piece of personal information that comes across their desk. How nervous should this threat make us?

There's no reason to be paranoid; there's just reason to be careful. If someone wants desperately to target you, they can probably get a lot of information about you — so you just need to minimize the criminal's opportunities to get that information. You can make yourself a harder target, and that's probably your best defense.



[Click here to return to the original story](#)

Thieves pilfering personal identities

1:05 a.m.
1/24/2002

By David Ho
The Associated Press

WASHINGTON -- Identity bandits victimized thousands of people last year, stealing their financial information and branding some with criminal records. This fast-growing crime accounts for more than 40 percent of consumer-fraud complaints.

The Federal Trade Commission said Wednesday that identity theft complaints far exceeded other areas of fraud, such as deceptive Internet auctions and lotteries. The figures come from a government database of more than 200,000 complaints collected in 2001 from more than 50 law enforcement and consumer groups.

Privacy advocates say the number of people victimized by identity theft may be as high as 750,000 a year.

"We've seen an explosion in this crime and it's not going away," said Beth Givens, director of the Privacy Rights Clearinghouse, a San Diego-based consumer group.

Givens said consumers should look at their credit reports twice a year, shred personal documents before throwing them away, and cleanse wallets of old receipts and printed Social Security numbers.

However, she cautioned, "You could take all the preventative steps and still become a victim."

One identity thief's actions made the world believe that Chicago lawyer Ted Wern wasn't only a deadbeat, but a criminal.

"He took my name and information and started running amok with it," Wern said.

He thinks the thief went through his mail or garbage for the information in 1998.

Using Wern's name and Social Security number, the ID thief applied for

7-8
7

and got at least four credit cards and ran up nearly \$50,000 in bills. The thief also opened a checking account with a Georgia bank and wrote thousands of dollars in bad checks.

Then, whenever the thief was pulled over for a traffic violation without a license, he started giving out Wern's information, building a litany of charges, including a drunken driving arrest in Ohio.

He was released, but that encounter led authorities last year to arrest Terre A. Stevens for the identity fraud crimes. This month he was sentenced to six months in prison and four years of probation, according to court officials in Mansfield, Ohio.

"I am angry, but in many cases theft of your identity is something you can't control," Wern said. "You have to just do your best to clear it up."

It cost the average victim more than \$1,000 to clean up the mess left by identity thieves, the FTC said.

The high number of identity theft complaints last year may partly reflect the FTC's increasing emphasis on investigating this kind of fraud and its use of toll-free numbers to receive those complaints, said Howard Beales, the agency's director of consumer protection. Consumers can call toll free (877) FTC-HELP or (877) ID-THEFT.

After identity theft, the top consumer fraud complaints of 2001 were problems with Internet auctions and deceptive trial offers and charges from Internet and computer services.

Credit card fraud accounted for 42 percent of identity theft complaints, followed by scams where telephone or utility accounts were created in a person's name without his or her knowledge.

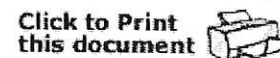
In some cases, hackers have been able to penetrate big corporations' databases and download credit card numbers and other data.

The District of Columbia had the highest rate of identity theft in 2001 with 77 victims for every 100,000 people. California and Nevada followed with 45 and 41 victims per 100,000 people, respectively.

Sue Ann Mills, 52, had her identity stolen from her home in Columbus, Ohio, when two burglars broke in and stole her purse, which contained her driver's license and Social Security card.

She called to cancel her credit cards, but not before the young thieves attempted and failed to use her cards to buy PlayStation video game consoles. They were never caught.

"It's a very scary situation," she said. "They don't want your furniture or your crystal, they want your identity."



For Immediate Release
Office of Homeland Security
January 7, 2002

Specifics of Secure and Smart Border Action Plan

ACTION PLAN FOR CREATING A SECURE AND SMART BORDER THE SECURE FLOW OF PEOPLE

1) Biometric identifiers

Jointly develop on an urgent basis common biometric identifiers in documentation such as permanent resident cards, NEXUS, and other travel documents to ensure greater security.

2) Permanent Resident Cards

Develop and deploy a secure card for permanent residents which includes a biometric identifier.

3) Single Alternative Inspection System

Resume NEXUS pilot project, with appropriate security measures, for two-way movement of pre-approved travelers at Sarnia-Port Huron, complete pilot project evaluation and expand a single program to other areas along the land border. Discuss expansion to air travel.

4) Refugee/Asylum Processing

Review refugee/asylum practices and procedures to ensure that applicants are thoroughly screened for security risks and take necessary steps to share information on refugee and asylum claimants.

5) Handling of Refugee/Asylum Claims

Negotiate a safe third-country agreement to enhance the handling of refugee claims.

6) Visa Policy Coordination

Initiate joint review of respective visa waiver lists and share look-out lists at visa issuing offices.

7) Air Preclearance

Finalize plans/authority necessary to implement the Preclearance Agreement signed in January 2001. Resume intransit preclearance at Vancouver and expand to other airports per Annex I of the Agreement.

8) Advance Passenger Information / Passenger Name Record

Share Advance Passenger Information and agreed-to Passenger Name Records on flights between Canada and the United States, including in-transit flights. Explore means to identify risks posed by passengers on international flights arriving in each other's territory.

9) Joint Passenger Analysis Units

Establish joint units at key international airports in Canada and the United States.

10) Ferry Terminals

Review customs and immigration presence and practices at international ferry terminals.

11) Compatible Immigration Databases

Develop jointly an automated database, such as Canada's Support System for Intelligence, as a platform for information exchange, and enhance sharing of intelligence and trend analysis.

7-10 9

COORDINATION AND INFORMATION SHARING IN THE ENFORCEMENT OF THESE OBJECTIVES

23) Integrated Border and Marine Enforcement Teams

Expand IBET/IMET to other areas of the border and enhance communication and coordination.

24) Joint Enforcement Coordination

Works toward ensuring comprehensive and permanent coordination of law enforcement, anti-terrorism efforts and information sharing, such as by strengthening the Cross-Border Crime Forum and reinvigorating Project Northstar.

25) Integrated Intelligence

Establish joint teams to analyze and disseminate information and intelligence, and produce threat and intelligence assessments. Initiate discussions regarding a Canadian presence on the U.S. Foreign Terrorist Tracking Task Force.

26) Fingerprints

Implement the Memorandum of Understanding to supply equipment and training that will enable the RCMP to access FBI fingerprint data directly via real-time electronic link.

27) Removal of deportees

Address legal and operational challenges to joint removals, and coordinate initiatives to encourage uncooperative countries to accept their nationals.

28) Counter-Terrorism Legislation

Bring into force legislation on terrorism, including measures for the designation of terrorist organizations.

29) Freezing of terrorist assets

Exchange advance information on designated individuals and organizations in a timely manner.

30) Joint Training and Exercises

Increase dialogue and commitment for the training and exercise programs needed to implement the joint response to terrorism guidelines. Joint counter-terrorism training and exercises are essential to building and sustaining effective efforts to combat terrorism and to build public confidence.

###

Return to this article at:

<http://www.whitehouse.gov/news/releases/2002/01/20020107.html>

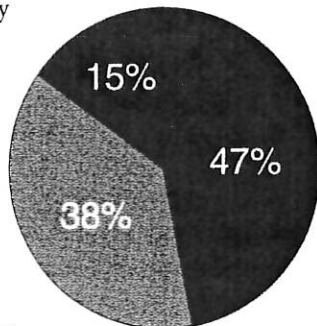
Click to Print
this document



But while community banks have pushed forward despite a slumping economy, issues on the horizon promise new challenges. Chief among these is the increasingly complex legislative and regulatory environment in which they must maneuver. Last year, brought more regulation, including new customer identification rules as outlined by the USA PATRIOT Act and enhanced corporate governance responsibilities as dictated by the Sarbanes-Oxley Act (see story, page 26).

In addition to these new guidelines, community bankers were once again called upon to defend their disclosure practices as it relates to consumer privacy and data sharing (sparked, in part, by recent legislative action in California) as well as weigh in on the ever burdensome CRA examination process. A recent

What impact, if any, would significantly further stock market declines have on lending demand at your bank?



47% say it will result in a decreased demand for loans

38% say it will result in increased demand for loans

15% say it will have no impact

Source: Phoenix Management Services

Community bankers report that identity theft attributed to more than half (56 percent) of all check fraud.

Source: GAO report, "Identity Theft Available Data Indicate Growth in Prevalence and Cost."

What are the top-five management issues community bankers consider important to their institution's continued success:

- 1) Retaining key employees—91%
- 2) Developing new sources of revenue—86%
- 3) Expanding services for small businesses—68%
- 4) Offering Internet banking services—68%
- 5) Measuring customer profitability—68%

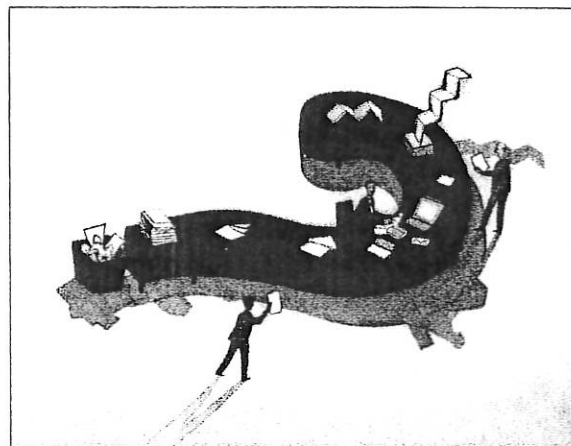
Source: Grant Thornton Survey

survey conducted by ICBA and Grant Thornton revealed that community banks can expect related costs for CRA compliance to more than double when they cross the \$250 million in asset threshold and move into the large bank category.

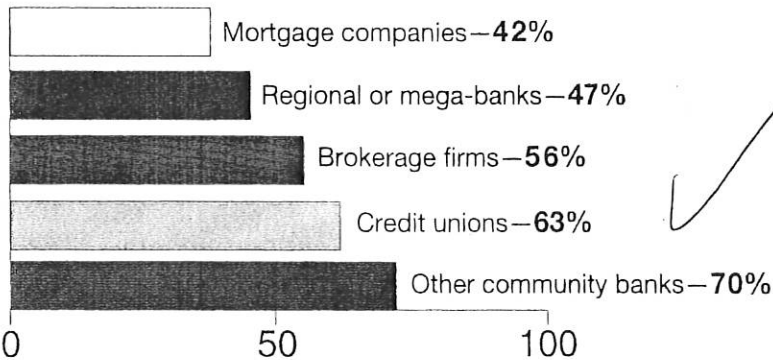
In the final analysis, 2002 proved once again that despite the obstacles facing the industry, community banks continue not only to survive but also thrive. Let's all hope that 2003 is at least as good. ■

* Figures are for banks with assets of \$100 million to \$1 billion. Source: FDIC

Nicole Swann is Independent Banker's senior editor.



What competitors do community bankers view as their biggest threat?



Source: Grant Thornton Survey