

MINUTES OF THE SENATE COMMITTEE ON JUDICIARY

The meeting was called to order by Elwaine F. Pomeroy at
Chairperson

10:00 a.m./~~p.m.~~ on March 28, 1984 in room 514-S of the Capitol.

~~All~~ members ~~were~~ present ~~except~~ were: Senators Pomeroy, Winter, Burke, Feleciano, Gaar, Gaines, Hein, Hess, Mulich, Steineger and Werts.

Committee staff present: Mary Torrence, Office of Revisor of Statutes
Mike Heim, Legislative Research Department
Jerry Donaldson, Legislative Research Department

Conferees appearing before the committee:

Frances Kastner, Kansas Food Dealers Association & Regency Condominium Association
Marjorie Van Buren, Office of Judicial Administration
Evelyn Bowers, Kansas Association of District Court Clerks and Administrators
Bud Grant, Kansas Chamber of Commerce and Industry
Jim Foster, Boeing Computer Services
Rick Dodds, Boeing Computer Services
Representative Dennis Spaniol
James R. Green, Data Processing Management Association
Wayne Hundley, Office of the Attorney General
Janet Stubbs, Home Builders Association of Kansas

House Bill 2718 - Small claims court, limit on amount of claim.

Frances Kastner testified the two organizations she is representing today are in support of the bill. A copy of her testimony is attached (See Attachment No. 1). The chairman referred to the food dealers proposed amendment that would allow them to hire a representative to file their claims, and inquired, if the bill is amended this way, how does that person not come under the definition of practicing law? She replied, for example, the Harry's IGA bookkeeper can go down and represent them. If they could do something like that, it would help.

Marjorie Van Buren stated her office is not supporting the bill. Copies of her three handouts are attached (See Attachments No. 2). She explained there will be an increase in caseload; the last time the limit was raised, they saw an increase in small claim cases filed. They are assuming there would be a net increase overall of number of cases; both judicial and nonjudicial time will be needed. They have not taken into consideration any possible large increase in filings that might come about in the possibility of a contractual person filing claims. She noted the net loss of revenues of \$150,000 by the county and state because of the reduction of the fee for limited actions cases is between \$7500 to \$100,000. She also pointed out, as shown in the handout, they have no problem with distributing the brochure as long as they are provided with the money to do it. She referred to Chapt. 20, Section 362, disposition of docket fees, and stated if this bill would pass in this present form, it would be a ten dollar docket fee instead of what is in the statute.

Evelyn Bowers testified they are concerned about this bill for the same reasons Marjorie Van Buren gave. She asked that the docket fees on limited action cases be one docket fee of thirty dollars for Chapt. 61 cases; this would help clerks in limited action cases. Committee discussion with her followed.

Bud Grant testified his organization supports the bill. In hearing from their members there is an interest in increasing limits in small claims courts. He said it is helpful to change limit slightly; don't think we should shut people out of this. He feels one thousand dollars is very reasonable. If the limit goes to \$750, this would be an increase in his eyes.

CONTINUATION SHEET

MINUTES OF THE SENATE COMMITTEE ON JUDICIARY,
room 514-S, Statehouse, at 10:00 a.m. ~~noon~~ on March 28, 1984.

House Bill 3082 - Computer crimes and theft.

Jim Foster explained his handout to the committee (See Attachment No. 3). He pointed out four more states have computer crime laws in addition to those states listed on his handout. The chairman inquired, why carve out separate crimes for this? When the criminal code was revised, it was done deliberate so there wouldn't be a number of specific crimes. Mr. Foster replied, this is a result of an interim study, and this is their recommendation.

Rick Dodds stated they don't believe the existing theft law is suitable, because it requires proof of attempted theft of a person's property. He explained how their information is received, and the technical problem with the law trying to prove they were permanently deprived of their property. A committee member inquired, you are not aware of any action been brought in regard to computer theft? Mr. Dodds replied, no. They are asking consideration of the substantial evidence that is mounting with 32 states passing computer theft bills. The chairman inquired what the language meant in line 66 of the bill? Mr. Dodds replied, when a party affirmatively makes a statement to you on which you rely to your detriment. The chairman inquired, how does that apply to computer theft? Mr. Dodds replied, it isn't entirely clear to me either. Further committee discussion was held with him.

House Bill 2718 - Small claims court, limit on amount of claim.

Representative Dennis Spaniol, the sponsor of the bill, explained the bill to the committee. Following his explanation, the chairman referred to lines 38 through 42, which would permit claims filed for someone else; and inquired, how is that not practicing law? Representative Spaniol replied, this was amended in by the House Ways and Means Committee, it was not a part of his bill. He said he remains neutral on the amendment and would like to see the bill passed. A committee member inquired, does that destroy the bill? Representative Spaniol replied, will not object if the amendment is taken out.

House Bill 3082 - Computer crimes and theft.

James Green testified his association supports the bill, because they feel the current statutes do not cover computer crime. Their chapter board of directors voted unanimously to endorse the explicit defining of computer crime and penalties for computer crime in the state statutes. A copy of his testimony is attached (See Attachment No. 4). Committee discussion with him followed.

House Bill 3021 - Warning for mechanic lien on residential property; time limit.

Wayne Hundley testified his office requested this amendment to the mechanics lien statute. He said under the present system notice is required. He explained the problem and feels the bill is necessary. He stated it will not cure all of the problems; it is a small burden compared to the potential danger. A committee member inquired, if he would object to striking line 84 starting with "except" through line 90? Mr. Hundley replied, probably not; would like to give it some thorough thought.

Janet Stubbs testified her association has worked with the attorney general's office in the past years on legislation. She stated they would have a problem with the suggestion made in lines 84 through 90. Good business practices would alleviate some of the problems. They would have trouble with a subcontractor who furnishes labor. She said they found three days would not alleviate the problem. A committee member inquired, how many cases have there been of contractors who have not paid their bills? She replied, I can't tell you in the last couple of years. Can't give statistics in recent times. She is not aware of the horror stories.

The hearings were concluded on House Bills 2718, 3082, and 3021.

House Bill 2598 - Sale of tobacco products to persons under 18 unlawful.

Senator Gaines moved to reconsider action on House Bill 2598; Senator Mulich seconded the motion, and the motion carried.

The meeting adjourned.

GUESTS

SENATE JUDICIARY COMMITTEE

NAME	ADDRESS	ORGANIZATION
Philip Ellis	RR #1	McLouth High
Tom Porter	RR 3	McLouth High
Richard Stacker	RR #1	McLouth High
Robt. Carl	RR #1	McLouth High 155
Cheri Dickey	Box 226	McLouth High
Myrcel Martyrowicz	Box 339	McLouth High
Sisu Belinger	Box 134	McLouth High
Denise Peino	RR. 1	McLouth High
Jim Weaver	RR 3	McLouth High
James O. Foster	3801 So. Oliver WICHITA	BOEING
Janet Stubbs	Tapeka	HBAK
Masha Hutchinson	Wichita	Beech Aircraft
Stan Poweroy	McLouth	McLouth High
Sandy Taylor	McLouth	McLouth High School
Michael Smith	McLouth	McLouth High School
Andrew Pheroff	RR #1 McLouth	McLouth High School
F. J. DODAS	3801 S. OLIVER WICHITA, KS.	BOEING
Dale R. Terry	3801 S. Oliver Wichita, KS	BOEING
Tracy Dover	RR #3	McLouth high
Jim Gooch	RR 1 Box 118	McLouth High School
A. B. Swenson	RR 1 Box 39	McLouth High School
Allan Matz	Box 71	McLouth High
David Beebe	RR 3	McLouth High
Jim SPENCER	WICHITA	BOEING
Avis Nelson	Wichita	Boeing Computer Services

GUESTS

SENATE JUDICIARY COMMITTEE

NAME	ADDRESS	ORGANIZATION
Doris M. Diffett	Topeka	Data Processing Mgmt Assoc.
Jae Furgane	Topeka	KASB
Phyllis Anderson	-	BUDGET DIV.
Ed Culbertson	-	"
Maury Kantola	Topeka	Ks Co-op Council
Wayne Hundley	"	A.G.
Mayne VanBuren	"	OJA
Jerry Sloan	"	"
BUD GRANT	1.	KCCJ
Marion C. Humphrey	"	KULL

3-28 '84

Attach. # 1



Kansas Food Dealers' Association, Inc.

2809 WEST 47th STREET SHAWNEE MISSION, KANSAS 66205

PHONE: (913) 384-3838

March 28, 1984

OFFICERS

PRESIDENT
JOE WHITE
KINGMAN

VICE-PRESIDENT
CHUCK MALLORY
TOPEKA

TREASURER AND SECRETARY
LEONARD MCKINZIE
OVERLAND PARK

CHAIRMAN OF THE BOARD
ROY FRIESEN
SYRACUSE

BOARD OF DIRECTORS

J.R. WAYMIRE
LEAVENWORTH
STAN HAYES
MANHATTAN
JOHN MCKEEVER
LOUISBURG
CHARLES BALLOU
CHANUTE
DONALD CALL
CEDARVILLE
JOE ENSLINGER
WICHITA
BOB BAYOUTH
WICHITA
MIKE DONELAN
COLBY
DELL KLEMA
RUSSELL

DIRECTORS AT LARGE

PAUL DART
GARDEN CITY
BILL WEST
ABILENE

AFFILIATE DIRECTOR

BOB MACE
TOPEKA

DIRECTOR OF GOVERNMENTAL AFFAIRS

FRANCES KASTNER

SENATE JUDICIARY COMMITTEE

SUPPORTING HB 2718

EXECUTIVE DIRECTOR
JIM SHEEHAN
SHAWNEE MISSION

Thank you for the opportunity to appear before you today.

I am here in a dual capacity, that of Director of Governmental Affairs for the Kansas Food Dealers Association, and as the Secretary--Treasurer of the Regency Condominium Association where I live.

About a year ago, the Condo Association had to use the small claims systems to recover damages to a roof which was under warranty and which amounted to \$650. Even though we were awarded the limit under Small Claims (\$500) the Association members still had to stand the cost of \$150 for repair which was supposed to be under warranty and the original roofer would not fix so we had to get another contractor to perform the work and pay for it.

Had HB 2718 been in effect, the original contractor would have been liable for the entire amount of the repair work.

Members of the KFDA asked us to seek an amendment which would allow them to hire a representative to file their claims, instead of having to do it themselves, or have a full-time employee responsible for filing claims and following them through. This amendment was added by the House Waysn and Means Committee and we believe it makes HB 2718 a good tool for our members to use in trying to collect on some of their unpaid debts. We all know that anytime a businessman has to absorb a bad debt, or a bad check, that is included into the cost of doing business, which in turn is passed on to honest consumers who pay their bills.

We ask that you recommend HB 2718 favorable for passage.

Attch. 1



3-2 84

Attach #2

State of Kansas
Office of Judicial Administration

Kansas Judicial Center
301 West 10th
Topeka, Kansas 66612

(913) 296-2256

February 28, 1984

To: Mary Galligan, Legislative Research
From: Jerry Sloan, Fiscal Officer
Re: House Bill No. 2718 as amended by the
House Committee on Ways and Means

This bill, as amended, would raise the jurisdictional limit for the small claims procedure from \$500 to \$1,000. It would also raise the docket fee for a small claims action from \$10 to \$15 as well as change the docket fee in Chapter 61 cases to \$15, if the amount of the claim does not exceed \$1,000.

Although the increase in docket fees might slightly reduce the number of filings, the cost estimates in my original fiscal note on this bill (copy attached) are not changed by the amendments of the House committee. We would continue to expect the increase in small claims filings along with the noted costs of \$39,300 for clerical help, \$23,500 for judges on assignment, and \$4,715 for forms modifications.

There would, however, be a change in the revenues generated due to the amendments. Using as an estimate of small claims filings, the number of filings in FY 1983 plus the increase estimated in the earlier fiscal note, we could anticipate 17,793 small claims cases filed. The estimated 14,043 cases under current statutes would generate an additional \$5 per case or \$70,215. The increased case-load of 3,750 cases would generate \$15 additional per case or \$56,250. There appears to be some inconsistency between this bill and K.S.A. 1983 Supp. 20-362(a)(3). However, it appears that of the collection of \$126,465 in new revenues, \$18,750 would go to the counties, approximately \$5,625 would go to the county law libraries, and approximately \$102,090 would go to the State General Fund.

There would be a decrease in revenue generated from Chapter 61 case filings from this proposed docket fee change. In an unscientific survey in one judicial district, it was discovered that 24% of the case filings in Chapter 61 were for claims between \$500 and \$1,000.

Atch. 2

Ms. Galligan

-2-

February 28, 1984

Extrapolating this percentage statewide, we might expect that approximately 10,000 cases would be affected by the docket fee change. This would indicate a decrease in revenues of \$150,000. The inconsistency with K.S.A. 1983 Supp. 20-362 again makes it unclear, but it appears that \$50,000 of this decrease would be from the counties' general funds and the remainder from the State General Fund.

JS:dm
Attachment



State of Kansas


Office of Judicial Administration

Kansas Judicial Center
301 West 10th
Topeka, Kansas 66612

(913) 296-2256

January 30, 1984

To: Lynn Muchmore, Director of Budget
Executive Branch

From: Jerry Sloan, Fiscal Officer 
Judicial Branch

Re: House Bill 2718

This bill would raise the jurisdictional limit for small claims procedure from \$500 to \$1,000.

The 1979 Legislature raised the limit for small claims procedure from \$300 to \$500 (see Chapter 187, Session Laws of 1979). At the same time (see Chapter 80, Session Laws of 1979), the jurisdictional limit in Chapter 61 cases was increased from \$3,000 to \$5,000. Following this action, it was found that case filings in both small claims and Chapter 61 increased dramatically, the former by 26.7% and the latter by 18.8%. At the same time, Chapter 60 case filings also increased but at a more normal 3.9%. We could anticipate this historical phenomenon to again occur in small claims filings with this bill.

In FY 1983, 14,043 small claims cases were filed. While the jurisdictional limit increase proposed is more, both in amount and percentage, than the increase that occurred in 1979, if we use a conservative estimate of the same percentage increase in case filings, we would expect about 3,750 more small claims cases. Historically, we would expect this to occur without a decrease in other civil filings.

It is estimated that this increase would require an additional 3 clerical positions, either in additional positions or an equivalent in temporary help. The cost for this additional staff in FY 1985 would be \$39,300. There would also be an impact on judicial work load. Estimating 30 minutes per case of judge time, this would require almost the equivalent of one full-time judge. While this increase would be statewide, it would require the additional usage of retired judges, if available, or more cross-assignments. It is estimated this cost would be approximately \$23,500.

2

Mr. Muchmore
January 30, 1984
Re: HB 2718
Page 2

The additional revenue generated from this filing increase would be \$37,500. Of this amount, approximately \$13,125 would go to the State General Fund and \$18,750 would go to the counties; approximately \$5,625 would go to the county law libraries.

There would also be an additional cost to the counties. Since most district courts order their forms on an annual basis, if this bill were to become law on July 1, the remainder of the existing forms would have to be discarded and new forms purchased. For small claims forms, it is estimated this would cost, in the aggregate, \$4,715.

JS:dm

3-28-84
2

March 28, 1984

To: Marjorie J. Van Buren
From: Jerry Sloan
Re: House Bill No. 2718 as amended

House Bill No. 2718 as amended by the House committee of the whole includes a requirement of creating, printing and distributing a pamphlet to all parties to proceedings pursuant to the small claims procedure act. This, of course, would have a fiscal impact beyond that of my earlier fiscal notes.

In discussions with our Trial Court Specialist, the proposed amendments, which are attached, should be included to clarify the type of booklet that is needed. My following analysis of the cost of this is based on this amendment being included.

As noted in my earlier fiscal notes, I am estimating nearly 18,000 small claims cases to be filed per year. When one takes into account that at least two booklets are required for each case and in the case of multiple defendants, even more, at least 36,000 booklets will be distributed and possibly more. In addition, since a supply of booklets needs to be available in each district court, some overage will be required.

Using an estimate of the amount of material that will be required in such a pamphlet, I requested a cost estimate from the Division of Printing. They approximated the cost of 50,000 booklets at \$10,500. It should be noted that a reduction in the number of booklets would not show a similar percentage decrease in cost since set-up charges would remain the same.

There is one additional administrative problem with complying with this amendment. The effective date of this bill is July 1. Should it become law, we would have to compile this booklet as well as get it printed. From my experience with the Division of Printing, especially around the end of the fiscal year, I would not expect to be able to have printed copies until August or even September. After that we would have to distribute these booklets to the district courts. It would probably be the first of October before we could be in complete compliance.

JS:lfb

0247 prepare, cause to be published and distribute to all clerks of the
0248 district court a pamphlet containing:

0249 [(1) A copy of the small claims procedure act, other than
0250 K.S.A. 60-2713 and amendments thereto; and

0251 [(2) a summary of the ~~rules of evidence and other procedures~~
0252 ~~used in the~~ proceedings pursuant to the small claims procedure
0253 act.

requirements of the

0254 [(b) The clerk of the district court shall distribute the
0255 pamphlet provided for by this section to all parties to proceed-
0256 ings pursuant to the small claims procedure act.

on or after October 1, 1984

0257 [(c) This section shall be part of and supplemental to the
0258 small claims procedure act.]

0259 Sec. 4 6 [7]. K.S.A. 61-2501, 61-2703, 61-2704, 61-2706 and
0260 61-2713 are hereby repealed.

0261 Sec. 5 7 [8]. This act shall take effect and be in force from and
0262 after its publication in the statute book.

#2

H. B. 3082

BY COMMITTEE ON COMMUNICATION, COMPUTERS, AND TECHNOLOGY

- o REPRESENT BOEING MILITARY AIRPLANE COMPANY, WHICH INCLUDES BOEING COMPUTING SERVICES COMPANY.
- o AT OUR BMAC FACILITY IN WICHITA WE HAVE:
 - 7 COMPUTER CENTERS
 - 1,000 + TERMINALS
 - 150,000 + DATA FILES
 - 2 DISHES THAT BEAM DATA VIA SATELLITE
 - ARE PART OF THE LARGEST PRIVATELY OWNED TELECOMMUNICATIONS NETWORK IN THE WORLD.
- o AT BMAC WE PROCESS VARIOUS CLASSIFICATIONS OF DATA WHICH ARE ASSETS OF THE COMPANY:
 - MILITARY CLASSIFIED
 - UNCLASSIFIED MILITARY
 - BOEING LIMITED/PROPRIETARY
 - COMMERCIAL SENSITIVE
- o WE ARE ASKING THAT COMPUTER SCIENCE AND LAW BE DESIGNED TO DEAL WITH CHANGING TECHNOLOGIES AND SOCIETIES.
- o REASONS BOEING IS SPONSORING HOUSE BILL 3082:
 - PROPER LEGISLATION TO GET OFFENDERS OFF THE STREETS.
 - ALLOW A COMPANY TO RECOUP SOME OF ITS LOSSES.
 - BMAC COMPUTING POWER HAS INCREASED OVER 1300% OVER THE LAST 5 YEARS.
 - STORAGE CAPACITY HAS INCREASED OVER 1900% TO APPROX. 450 BILLION WORDS.
 - CURRENT STATUTES LACK SPECIFIC DEFINITIONS IN THE COMPUTING AREA.
 - ADDITIONALLY CURRENT STATUTES LACK PENALTIES OR RECOURSE CONSISTANT WITH THE VALUE OF THE DATA.
 - MORE AND MORE VITAL COMPANY AND GOVERNMENT PROPRIETARY DATA RESIDES IN THE COMPUTER NETWORK.

#5

PAGE 2

- ASSISTANCE IN HELPING US PROTECT OUR COMPUTER SYSTEMS AGAINST:
 - PHYSICAL ABUSE
 - DATA CORRUPTION
 - FRAUD
- OUR INTENT IS TO PREVENT THE INVASION OF OUR RIGHTS AND WHEN VIOLATED, PROVIDE EVIDENCE TO SHOW THAT OUR OBLIGATIONS IN PROTECTING THE RESOURCES HAVE BEEN CARRIED OUT.

MARCH 28, 1983 "COMPUTER WORLD"
18 STATES WITH COMPUTER CRIME LAWS

- | | |
|------------------------|------------------------------|
| 1. ARIZONA.H.B.2212 | 10. MISSOURI.S.B.559 |
| 2. CALIFORNIA.H.B.66 | 11. MONTANA.H.B.621 |
| 3. COLORADO.H.B.1110 | 12. NORTH CAROLINA.H.B.S.397 |
| 4. DELAWARE.H.B.730 | 13. NEW MEXICO.H.B.S.8 |
| 5. FLORIDA.H.B.1305 | 14. OHIO.H.B.437 |
| 6. GEORGIA.S.B.198 | 15. RHODE ISLAND.H.B.5775 |
| 7. ILLINOIS.H.B.H.1027 | 16. UTAH.H.B.183 |
| 8. MICHIGAN.H.B.4112 | 17. VIRGINIA.H.B.439 |
| 9. MINNESOTA.S.B.381 | 18. WISCONSIN.H.B.744 |

Computer World 3-5-84

Va. lawmakers pass categorical computer crime bill

By Paul Korzeniowski
CW Staff

RICHMOND, Va. — The Virginia state legislature overwhelmingly passed a computer crime bill that renders obsolete current legislation and clearly defines categories of computer crime. The bill awaits the signature of Gov. Charles S. Robb, after which it will become effective July 1.

Sponsored by the Virginia League of Savings Institutions, the bill divides offenses into five categories: computer fraud, trespassing, invasion of privacy, threat to security and forgery. "The law clearly labels categories of crime that previously didn't exist," said Daniel R. Burk, an attorney with Thomas and Fiske P.C., the Alexandria, Va., law firm

that represented the league. "It is designed to stop anyone who uses a computer for an illegal activity."

Minimum sentences for persons convicted under the new law range from a \$500 fine to a five-year prison term.

"There is a wide range of sentences which helps to ensure that the punishment fits the crime," accord-

ing to Burk.

To draft the bill, Burk studied computer crime bills currently in place in 21 states. "We wanted to ensure that the bill had comprehensive, clear language," he said.

One issue that the new bill does not address is illegal copyrighting. "We may explore that issue next year," Burke noted.

#

Mass. Crime Bill Classifies Electronic Data as Property

BOSTON — A piece of legislation that sponsors hope will encourage Massachusetts businesses to prosecute computer criminals more aggressively is nearing approval in the Criminal Justice Committee of the commonwealth's House of Representatives here.

The bill would amend the state criminal code to classify electronic impulses as property, opening the door for offenders to be prosecuted under state larceny statutes for the value of information that is recorded electronically.

The bill is in its third reading in the House Criminal Justice Committee after being given a reading on a voice vote without debate last week. It is intended to fill "a rather broad gap [in the law] that needs to be addressed," according to Rep. Paul White (D-Boston), chairman of the committee and the bill's cosponsor.

"This will protect the computer

industry substantially because it will not be exposed to potential losses [since] our law did not cover areas like this," White said. He noted that losses from theft of computer data are "awfully hard to get because the companies seem hesitant to talk too much about being ripped off on a regular basis. But we get the feeling that there has been substantial loss over the years."

White said the matter gained legislative attention after a 1981 state Supreme Court decision that a person who stole a magnetic tape could be prosecuted only for the value of the tape itself, not the electronic impulses contained on it.

The bill will go to the House floor after the third reading. "I think it will pass," White said. "We just have to engage in some education with some of our colleagues who get confused about something as highly technical as this."

Computerworld

May 9, 1983

NEWS

Concern mounts over misuse of medical records

By David Olmos
CW Staff

CHICAGO — In the thick of last year's mayoral race here, damaging information about Republican candidate Bernard Epton's medical history was revealed, perhaps influencing the election results.

Some health care groups fear the potential for similar disclosures of supposedly confidential medical records — whether those of politicians or the general public — is becoming more likely. The growing use of computerized medical records in U.S. hospitals is posing an Orwellian threat to patients' privacy, according to one top health care official.

"Never before has the privacy of health records been so endangered," said Dr. Stuart A. Wesbury Jr., president of the American College of Hospital Administrators (Acha), in a recent report that warned of the "potentially serious threat" posed by increased computerization.

New demands for information by the federal government and insurance companies have prompted the college and other health care groups to call for stronger safeguards for computerized medical records. The 28,000-member college is the nation's largest organization for health care workers.

Last October, the government began new payment procedures in which hospitals are paid predetermined rates for the care given Medicare patients, Wesbury said. This has made it necessary for hospitals to correlate patient information and financial information "as never before."

The new payment structure has made it virtually impossible for a hospital to function efficiently without its own in-house computer system, service bureau or other outside time-sharing service, Wesbury noted.

The new Medicare payment procedures raise the likelihood that access to information will be available

not only to doctors and nurses, but also to data processing and accounting department personnel, he said. An average of 75 people in each hospital now have access to patient records, according to research by the college.

The government and insurance companies are not the only organizations seeking patient information, Wesbury continued. Many employers are now establishing their own health insurance plans and are seeking patient data before making payments. An employer conceivably could gain access to medical information that the employee wanted kept confidential, he said.

Health organizations are recommending that hospitals implement policies on data security to help protect patient privacy.

Confidentiality of patient records "is a problem, but it is solvable," according to Peter Wagemann, director of the Institute for Medical Record Economics, Inc., a

Boston-based research organization serving the health care industry. The institute has recommended that every staff person with access to patient information be required to sign a statement of confidentiality, with violations punishable by reprimand or dismissal.

Wesbury said he was alerted to the security issue last August after a widely publicized incident in which computer hackers gained access to patient files at the Memorial Sloan Kettering Cancer Center in New York.

That kind of incident "perks up your ears," he said. "What if you have someone who really knows what they're doing and has more sophisticated hardware and software?"

The American Medical Records Association, in a statement on confidentiality and security of health records, urged hospitals using computers to adopt security safeguards such as limiting access to patient records, controlling access by pass-

words, establishing user input and output limitations, using numbers instead of names for both patients and health care providers and maintaining backup files on magnetic disk or tape.

One group is addressing the problem of access to medical information by creating model state legislation. A drafting committee of The National Conference of Commissioners on Uniform State Laws, a quasi-governmental body comprised mainly of lawyers appointed by the nation's governors, has completed a preliminary draft of a Health Care Information Act.

According to Alan Bennett, a Washington lawyer and reporter for the drafting committee, the legislation, which involves records on paper as well as in computers, contains provisions to protect access of certain medical records, prohibit disclosure of data without patient consent and place restrictions on access by law enforcement agencies.

NEWS

Three suspended for tapping school's system

By Patricia Keefe
CW Staff

SAN DIEGO — A series of break-ins into the computer system at a specialized math and science high school here last month has resulted in the suspension of three students and a beefing up of system security.

Officials of the San Diego School Department and Gompers Secondary School decided against filing criminal charges with local police, even though four students allegedly deleted grades and altered other students' homework filed on the school's Digital Equipment Corp.

minicomputer system.

Initially, the students confined their activities to changing passwords so teachers couldn't access their programs. No data was lost, however, because the teachers had maintained hard-copy backup, according to Albert Cook, the assistant

superintendent of schools here.

Although Gompers officials are reportedly now planning to educate students and their parents about the ethics and legalities of system violations, Cook said new students are regularly given an orientation regard-

ing the ethics of computer science, including tampering.

Three of the students involved attended Gompers, while a fourth attended Patrick Henry High School, which also has a computer science program. Three of these students have been suspended from the computer science program for the remainder of the year, Cook said.

Their activities were discovered after the chairman of the Gompers computer science program realized that phone lines used by students to do computer science homework at night were being used during the day. After setting up a monitoring system, the chairman learned that a student at another school, using information supplied by his brother at Gompers, figured out the passwords needed for full access to the Gompers computer system. The two brothers then circulated the passwords among other students.

School officials still aren't sure how many students ended up with the ability to access the system. Although the students claimed the passwords were relatively simple, the teachers say the students were extremely lucky to have guessed them, Cook said. The only security precautions the school can take, according to John Crane, director of DP for the San Diego schools, is to change the passwords, which has been done. There is no need for anything more since the Gompers system is not connected to any school administration computers, he added.

Workers Allegedly Set 'Logic Bomb'

Associated Press

LOS ANGELES — Two computer programmers have been accused of trying to sabotage their company's computer system with "logic bombs," destructive programs set to go off at a specified time.

"The logic bombs would have deleted inventory and payroll information, shut down the computer system and then erased any trace of the destructive commands, so the pair could have gone undetected," said District Attorney Robert H. Philibosian.

Both men were charged with two counts of computer fraud and one count of conspiracy to commit computer fraud. Both charges are felonies.

(CALIFORNIA COMPUTER CRIME STATUTE)

The Value of Legislation

by Congressman Bill Nelson

With the advent of electronic funds transfer systems and automatic teller machines, you can well appreciate that familiarity with computers is rapidly becoming common experience for tens of millions of Americans. Many security managers are concerned daily with the broad problem of ensuring the security and accuracy of computer operations in the business communities of our nation.

I would like to address part of this problem—the part that can be played by making computer-assisted crime a violation of federal law.

Computer-assisted crime is the way we should refer to this particular type of wrongdoing. But I doubt that the simpler, less accurate term "computer crime" will disappear from popular reports of the issue. Nevertheless, what we are

talking about is not crimes committed by computers, but crimes committed by people with the assistance of computers. This includes crimes committed by people at a computer keyboard and crimes that take advantage of the ability of computer systems to bypass the human controls that existed in traditional accounting and auditing procedures.

The federal government, particularly the Pentagon and Bureau of the Census, has many computers—more than 16,000 in the entire federal establishment. The private sector has some 56,000 large, general purpose computers and 213,000 smaller business computers. Another 570,000 minicomputers and 2.4 million desktop computers are also in use in the private sector. My own congressional office has a powerful minicomputer with 256 K of core memory and 60 megabytes of disk memory, a tape drive for backups, and its own emergency power supply.

The computer-assisted crime problem poses major difficulties for the future because computers will be increasingly available to our society to assist whatever work we have to perform. And where people work daily with a powerful tool such as a computer, some will overstep the boundaries between legitimate and criminal uses of these devices.

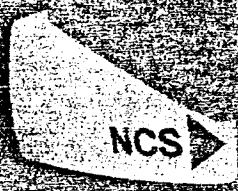
Daily newspaper headlines cite rising computer criminal activity. Recently reported was the story of a former Federal Reserve employee who used a stolen password to tap into confidential Federal Reserve System computer files. The assistant US attorney on the case was able to prosecute under the federal wire fraud provision only because the perpetrator used a telephone and dialed across state lines to commit the act. Had he confined his activity to within state, the prosecutor would most likely have had to rely on a general theft statute—resulting in only a \$100 fine for the theft of the actual computer time stolen, without consideration of the information's value.

The 414s, a group of teenage hackers in Milwaukee, were recently in the headlines when they made incursions into more

Congressman Nelson gave this speech at the ASIS conference on Theft & Diversion of High Technology, October 31 and November 1, 1983, in Washington, DC.

SECURITY MANAGEMENT

THE RIGHT STUFF




The very nature of the experimental and secret aircraft tested at Vandenberg Air Force Base demands the best security system money can buy. That's why Vandenberg chose National Control Systems for the optimum in security.

National Control Systems pioneered the concept of a "Disributed Data Base" to assure full security operation at each door even in the event of a central computer breakdown or communication failure.

NCS has a full range of products from an individual door application to the most sophisticated computer directed systems—and NCS creates and supports its own software.

Through its technical services group NCS customers and dealers are given the most complete factory support found of any affiliate.

For the Right Stuff in security systems, call or write us today.

NCS 

NATIONAL CONTROL SYSTEMS, INC.

3001 S. Madison Blvd., Oconomowoc, WI 53151 (414) 281-0500

than fifty business and institutional computers, among them the Los Alamos nuclear weapons laboratory. This year in my own state of Florida, a health insurance claim agent generated more than \$240,000 in fraudulent claims to herself and family members. That case was successfully prosecuted under the comprehensive computer crime law I sponsored as a state legislator in 1978. Since we passed the Florida law, approximately twenty states have followed suit, adding varying degrees of protection against computer-assisted crime to the state criminal codes.

The examples given point to the inadequacies of our existing judicial system and penal codes in handling this type of case. Prosecutors are unable to make effective cases against computer criminals because the forty or so federal laws that could be applied were designed to control other kinds of criminal activity. Testifying at a recent Senate subcommittee hearing, John Keeney, deputy assistant attorney general of the Department of Justice Criminal Division, described the current legal dilemma well. He suggested that in relying on statutory restrictions dealing with other offenses, the law enforcement officer and the prosecutor must create "a theory of prosecution that somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement, or even the illegal conversion of trade secrets." Obviously, such application can be awkward and the results far from perfect.

Legislation is obviously in order to strengthen the powers of federal prosecutors so those who illegally penetrate computer systems can be brought to justice. Thus, I have introduced the Federal Computer Systems Protection Act of 1983 to make crimes by computer a specific federal offense. H.R. 1092 would make it illegal to tamper with the computers of the federal government, the computers of financial institutions guaranteed by the federal government, and computers operating in interstate commerce or using interstate facilities. (See summary of H.R. 1092's provisions at right. This legislation could give federal prosecutors an efficient tool to combat the growing threat of computer-assisted crime to the national economy and to national security.

We need a national statute to defend our federal government computers from unauthorized entry, to protect the developing electronic funds transfer system, to preserve the integrity of the Federal Reserve System, and to safeguard

The Federal Computer Crimes Act of 1983—A Summary

The Federal Computer Systems Protection Act of 1983 would make crimes by computer a specific federal offense. Such crimes must now be prosecuted under other federal fraud and theft statutes. "This bill will give prosecutors a clear-cut basis for prosecuting anyone who steals information from a computer or who alters or destroys information in a computer maliciously or for personal gain," states the bill's sponsor, Congressman Bill Nelson (D-FL). H.R. 1092 is a revised version of H.R. 3970, which Nelson sponsored in the 97th Congress with 44 co-sponsors. The new bill broadens the definition of a computer system and makes other changes recommended by experts in the computer and computer crime fields.

H.R. 1092: "A bill to amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce."

PENALTIES: Fines of up to \$50,000 or twice the value of the property stolen or imprisonment for up to five years, or both, for . . . "whoever uses, or attempts to use, a computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or knowingly convert to his use or the use of another, if the computer—

- (1) is owned by, under contract to, or operated for or on behalf of: (A) the United States Government; or (B) a financial institution; and the prohibited conduct directly involves or affects the computer operation for or on behalf of the United States Government or financial institution; or
- (2) operates in, or uses a facility of, interstate commerce."

And provides for fines up to \$50,000, or imprisonment for up to five years, or both, for "whoever intentionally and without authorization damages a computer described (above) or intentionally and without authorization causes or attempts to cause the withholding or denial of the use of a computer, a computer program, or stored information."

JURISDICTION: "In a case in which Federal jurisdiction over an offense as described in this section exists or may exist concurrently with State or local jurisdiction, the existence of Federal jurisdiction does not, in itself, require the exercise of Federal jurisdiction, nor does the initial exercise of Federal jurisdiction preclude its discontinuation."

DEFINITIONS:

Computer "means an electronic, magnetic, optical, hydraulic, organic, or other high-speed data processing device or system performing logical, arithmetic, or storage functions, and includes any property, data storage facility, or communications facility directly related to or operating in conjunction with such device or system; but does not include an automated typewriter or typesetter, a portable hand-held calculator, or any computer designed and manufactured for, and which is used exclusively for, routine personal, family, or household purposes and which is not used to access, to communicate with, or to manipulate any other computer."

Property "means anything of value, and includes tangible and intangible personal property: information in the form of computer processed, produced, or stored data; information configured for use in a computer; information in a computer medium; information being processed, transmitted or stored; computer operating or applications programs; or services."

Use "includes to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer, or, with fraudulent or malicious intent, to cause another to put false information into a computer."

Computer medium "includes the means of affecting or conveying data for processing in a computer, or a substance or surrounding medium which is the means of transmission of a force or effect that represents data for processing in a computer, or a channel or communication of data for processing in a computer."

Financial Institutions are "(A) a bank with deposits insured by the Federal Deposit Insurance Corporation; (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank; (C) an institution with accounts insured by the Federal Savings and Loan Corporation; (D) a credit union with accounts insured by the National Credit Union Administration; (E) a member of the Federal home loan bank system and any home loan bank; (F) a member or business insured by the Securities Investor Protection Corporation; and (G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934."

business computers in a world where a computer terminal may be on every desk in every home.

We have tried to draft this bill to avoid discouraging the legitimate inventiveness of computer programmers. We recognize the need for interaction between people and computers on a day-to-day basis. Limiting access and other necessary security measures must not prevent computers from being used to their fullest potential in government or the private sector. Employees must have ready access to computers to do their jobs with a minimum of security hassle, just as they previously needed access to a typewriter, a telephone, or a library. H.R. 1092 is intended to allow that freedom, while providing the protection of legal prosecution of the willful or malicious wrongdoer.

The bill has received generous support both from my congressional colleagues and from many experts in the industry. We currently have 110 cosponsors and look forward to hearings before the House Judiciary Subcommittee on Civil and Constitutional Rights in the near future. Subcommittee Chairman Don Edwards, of California, has recently appointed a special counsel to assist in the preparation of those hearings. As soon as pos-

sible, you will be notified of the date and time for the hearings, so ASIS can participate and attend.

Hearings have been held in both House and Senate committees to review the computer-assisted crime problem in general. Although none of these hearings legislatively addressed H.R. 1092, many witnesses testified to its viability and the need for such a statute. Representing ASIS, Mr. Criscuoli and Mr. Bequai recently appeared before Senator Cohen's Subcommittee on Oversight of Government Management, of the Governmental Affairs Committee, and addressed the need for federal legislation. Mr. Criscuoli reaffirmed your support of my legislation, and Mr. Bequai emphasized the deterrence and educational quality of the bill. (See page 25 for the ASIS testimony.) I look forward to working with you in the future to press this bill forward.

The endorsements from your own Society, financial institutions, trade associations, and private computer security experts have been most encouraging. The American Bankers Association, in a letter to Subcommittee Chairman Don Edwards, said, "We feel H.R. 1092 is an important step in defining the issues and the scope of the computer crime prob-

lem, and an important ingredient in appropriately controlling the information powers of computers as well as deterring abuses. . . . Our Association considers computer-related crime to be a serious threat to society and particularly to the safety and soundness of financial institutions. . . . The American Bankers Associations supports H.R. 1092."

Representatives of the Federal Bureau of Investigation, the Department of Labor, and the General Accounting Office have all voiced support for a federal statute addressing this unique legal problem.

During a recent hearing before the Science and Technology Subcommittee on Transportation, Aviation, and Materials, John L. Hancock, senior vice president of Wells Fargo Bank, San Francisco, stated, "Current legislation, which is now pending at the federal level, should be enacted to better define computer crimes." He supported his comments by suggesting that through implementation of such a law, prosecution (of computer-assisted crime) would be facilitated and public awareness (of the problem) would be heightened—an obvious and potential deterrent to the commission of computer crimes would be in place.

Finally, passage of federal computer crime legislation would serve as a pace-

PUT YOUR FORCE ON COURSE.

Now there's a cost effective, universally applicable basic training program for the private security officer. Private Security Training Institute's slide and videotape courses have been produced by security training professionals. And unlike most programs, which are merely watered down versions of public law enforcement programs, the P.S.T.I. courses specifically address your needs, from basic security techniques to human relations, and more.

We can also customize one of our current programs for you or design a program for your very specific needs. Because we are a division of a nationally recognized full service security firm, we can also provide a complete line of security training consulting services.

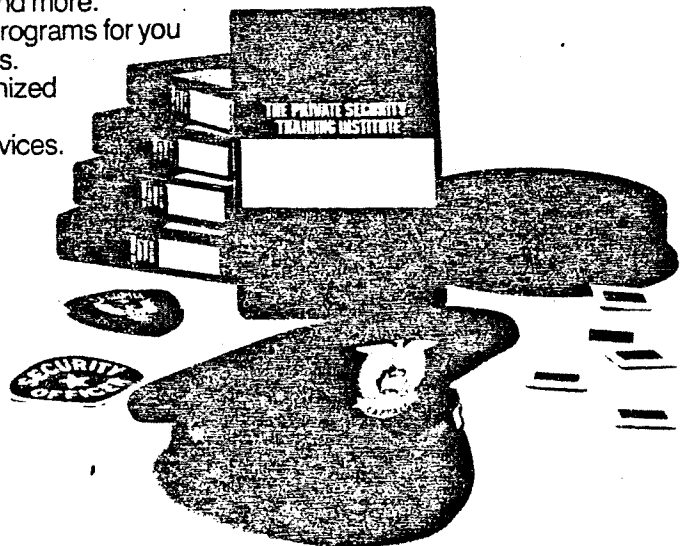


For more information or a brochure, contact Mr. Scott Edmonston, CPP, Director.



THE PRIVATE SECURITY TRAINING INSTITUTE

92 State Street, Boston, Massachusetts 02109
In Mass: 1-800-392-6289
Outside Mass: 1-800-225-6146



setter or guide for other industrialized countries. I was delighted to learn that a copy of the legislation had been forwarded to the governments of Germany and Italy for review. While our nation is certainly a leader in computer tech-

nology, we must remember that the usefulness of computers, as well as the potential for disastrous international crimes, will affect the entire world.

I hope with your assistance and the help of my colleagues, the business com-

munity, and law enforcement agencies, we will be able to enact federal computer-assisted crime legislation that will stand the test of time—even in an industry that is advancing and changing every day.

ASIS

About the Author . . . *Congressman Bill Nelson (D-FL) previously served in the Florida state legislature, where he sponsored that state's computer crime bill. It became law in 1978, making Florida the first state to enact a computer crime law.*

SESSION OF 1984

SUPPLEMENTAL NOTE ON HOUSE BILL NO. 3082

As Amended by House Committee on
Communication, Computers and Technology

Brief of Bill*

H.B. 3082 establishes, as part of the Kansas criminal code, the crimes of computer theft and computer crime. Computer theft includes wrongfully obtaining or exerting control over the property or services, both of which the bill defines with respect to computers, of another person with intent to deprive such person of property or services. Computer crime is defined as knowingly and fraudulently or without authorization using, damaging or destroying any computer, computer system, computer network, software, programs, documentation or data.

Commission of computer crime or theft causing a loss of less than \$100 is a class A misdemeanor; a crime causing a loss exceeding \$100 constitutes a class D felony.

The House Communication, Computers and Technology Committee amendments were to clarify certain language.

* Bill briefs are prepared by the Legislative Research Department and do not express legislative intent.

2
[As Amended by House Committee of the Whole]

As Amended by House Committee

Session of 1984

HOUSE BILL No. 3082

By Committee on Communication, Computers and Technology

2-22

0021 AN ACT relating to crimes and punishments; concerning com-
0022 puter crime and computer theft; classifying certain acts as
0023 misdemeanors and felonies.

0024 *Be it enacted by the Legislature of the State of Kansas:*

0025 Section 1. (1) As used in this section, the following words
0026 and phrases shall have the meanings respectively ascribed
0027 thereto:

0028 (a) "Use" means to instruct, communicate with, store data in,
0029 retrieve data from, or otherwise make use of any resources of a
0030 computer, computer system or computer network.

0031 (b) "Computer" means an electronic device which performs
0032 logical, arithmetic or memory functions by the manipulations of
0033 electronic or magnetic impulses and includes all input, output,
0034 processing, storage, software or communication facilities which
0035 are connected or related to such a device in a system or network.

0036 (c) "Computer network" means the interconnection of com-
0037 munication lines, including microwave or other means of elec-
0038 tronic communication, with a computer through remote termi-
0039 nals, or a complex consisting of two or more interconnected
0040 computers.

0041 (d) "Computer program" means a series of instructions or
0042 statements in a form acceptable to a computer which permits the
0043 functioning of a computer system in a manner designed to
0044 provide appropriate products from such computer system.

0045 (e) "Computer software" means computer programs, proce-
0046 dures and associated documentation concerned with the opera-
0047 tion of a computer system.

0048 (f) "Computer system" means a set of related computer
0049 equipment or devices and computer software which may be
0050 connected or unconnected.

0051 (g) "Financial instrument" means any check, draft, money
0052 order, certificate of deposit, letter of credit, bill of exchange,
0053 credit card, debit card or marketable security.

0054 (h) "Property" includes, but is not limited to, financial in-
0055 struments, information, including electronically produced data
0056 and computer software and computer programs in either ma-
0057 chine or human readable form and any other tangible or intangi-
0058 ble item of value.

0059 (i) "Services" means computer time, data processing and
0060 storage functions.

0061 (2) Computer theft is: *use*

0062 (a) Wrongfully obtaining or exerting unauthorized control
0063 over the property or services of another person, or the value
0064 thereof, with intent to deprive such person of such property or
0065 services;

0066 (b) by color or aid of deception, obtaining control over the
0067 property or services of another person, or the value thereof, with
0068 intent to deprive such person of such property or services; or

0069 (c) appropriating lost or misdelivered property or services of
0070 another person, or the value thereof, with intent to deprive such
0071 person of such property or services.

0072 (3) In any prosecution for computer theft, it is a defense that
0073 the property or services was appropriated openly and avowedly
0074 under a claim of title made in good faith ~~even though the claim is~~
0075 ~~untenable.~~

0076 (4) Computer crime is knowingly and fraudulently or know-
0077 ingly and without authorization obtaining the use of, using,
0078 altering, damaging or destroying any computer, computer system
0079 or computer network, or any computer software, program, docu-
0080 mentation ~~or~~, data or property contained in such computer,
0081 computer system or computer network.

0082 (5) Computer theft or computer crime which causes a loss of
0083 less than \$100 is a class A misdemeanor. Computer theft or
0084 computer crime which causes a loss of \$100 or more is a class D

#3

0085 felony.

0086 (6) This section shall be part of and supplemental to the
0087 Kansas criminal code.

0088 Sec. 2. This act shall take effect and be in force from and
0089 after its publication in the statute book.

3-28-84

Attach. # 4

DATA PROCESSING MANAGEMENT ASSOCIATION

Testimony of

James R. Green, Kaw Valley Chapter President
Data Processing Management Association (DPMA)

before

Senate Judiciary Committee

March 28, 1984

The Kaw Valley Chapter is one of 280 chapters of the Data Processing Management Association. DPMA was founded in 1951, and with over 45,000 members in the U.S. and Canada is the largest professional association in the field of information management. It is governed by standards of conduct and an enforceable code of ethics.

At its February meeting, the chapter board of directors voted unanimously to endorse the explicit defining of computer crime and penalties for computer crime in the state statutes. This is especially important as the U.S. Congress does not seem in any hurry to address these matters at the federal level.

While neither the board nor the general membership (83 members in the greater Topeka area) have reviewed HB3082 in great detail, it appears to do a very good job of addressing the very real and present problem of computer crime.

Though none of us are attorneys, HB3082 appears to correct the two major problems with current statutes: 1) many products of the computer age can be misappropriated by persons not the owner or producer without depriving the original owner of their use; and 2) many products of the computer age may not be covered at all because of their intangible nature.

I personally cannot think of a proper and ethical use of a computer that would be made illegal by this bill, and yet it is broad enough to address all the weaknesses of current statutes outlined in the newspaper article in a recent Topeka Capitol Journal article. It also seems to cover "hacking", that is, unauthorized use of computers, whether or not it is done with the intent to harm or for personal gain. I am not that knowledgeable about electronic fund transactions, but the inclusion of credit and debit cards in the definition of "property" should be a great help in that area.

The chapter proposes no specific changes in the wording of HB3082, but would be available at any time to discuss changes proposed in the future.



Handwritten signature/initials

Moore Business Forms, Inc.

Crime laws criticized

WASHINGTON (AP) — A Justice Department report said Sunday that existing criminal laws weren't sufficient to deal with crimes committed against automated banking machines and in other electronic financial transactions.

The department's Bureau of Justice Statistics said there was growing concern that so-called electronic fund transfers "provide an electronic environment that is potentially fertile for criminal abuse."

The bureau said that only 22 states had laws addressing computer crime or electronic fund transfer, that virtually all those laws were enacted in the last five years, and that there was little information on how effective they were. There are also several federal laws in the area.

The bureau's report said electronic crimes had the same consequence as traditional theft but "the existing criminal law does not in many cases directly address the unique elements of electronic fund transfer crimes."

The report noted that theft statutes typically prohibited the taking of physical property but it was not clear whether an electronic command making a fund transfer constitutes "taking" under those laws. The report said it was also uncertain whether the contents of a computer memory constitute property. Finally, the bureau noted that fraud

statutes called for willful misrepresentation to a person, but it was unclear whether computers are legally considered persons.

The report said the use of automated teller machines had grown from 4,056

"The existing criminal law does not in many cases directly address the unique elements of electronic fund transfer crimes"

— Justice Department report

terminals in 1975 to 35,721 terminals in 1982, when they handled more than 2 billion transactions and \$240 billion.

Automated clearing houses handled 40 million transactions in 1976 and 300 million transactions in 1981.

Wire transfers grew from 23 million transactions involving more than \$42 trillion in 1975 to 700 million transactions involving \$137 trillion in 1981.

"The growth of electronic fund transfer use to date will, however, pale in comparison to its expected future growth, especially as banking laws are changed to accommodate the information age and as computer and communications technology becomes more

advanced," the report said. The bureau identified four basic types of crime directed at automatic teller machines:

- Unauthorized use of a stolen bank card. The bureau noted that many card holders make the mistake of keeping their personal identification numbers with their card.

- Fraud committed by a legitimate cardholder who because the machines do not use sophisticated verification procedures, like fingerprints or voice prints, can make withdrawals and later claim they were not responsible for the withdrawal.

- Insider manipulation ranging from the theft of cards by bank employees to computerized alterations of accounts.

- Physical attacks on the machines themselves to obtain the large amount of cash they contain or on cardholders immediately following a cash withdrawal.

In the case of wire transfer, the bureau said that the system was susceptible to errors made by authorized employees, to fraudulent computer instructions by unauthorized employees of financial institutions, and to illegal manipulation by outside criminals who use their own computer systems to skirt security arrangements and manipulate transactions.