

HB

520

FISCAL NOTE

Revision Date: _____

REQUEST

Bill/Resolution No.: HR 520
 Title: "An Act relating to
 criminal use of a computer."
 Sponsor: Repr. Haves
 Requestor: House Judiciary
 Date of Request: 1/26/84

FISCAL DETAIL

Agency Affected: Department of Law
 Program Category Affected: Admin. of Justice
 BRU, Program or Subprogram(s) Affected: Prosecution

EXPENDITURES/REVENUES: (Thousands of Dollars)

	FY 84	FY 85	FY 86	FY 87	FY 88	FY 89
OPERATING						
100 PERSONAL SERVICES						
200 TRAVEL						
300 CONTRACTUAL						
400 SUPPLIES						
500 EQUIPMENT						
600 LAND & STRUCTURES						
700 GRANTS, CLAIMS						
800 MISCELLANEOUS						
TOTAL OPERATING	-0-	-0-	-0-	-0-	-0-	-0-
CAPITAL						
REVENUE						

FUNDING: (Thousands of Dollars)

GENERAL FUND	-0-	-0-	-0-	-0-	-0-	-0-
FEDERAL FUNDS						
OTHER						
TOTAL						

POSITIONS:

FULL-TIME	-0-	-0-	-0-	-0-	-0-	-0-
PART-TIME						
TEMPORARY						

SOURCE OF FUNDS TO OFFSET FISCAL IMPACT OF BILL:

N/A

ANALYSIS: Attach a separate page for analysis

Prepared By: Richard I. Peaves, Director Phone: 465-3672
 Division: Administrative Services Division Date: 2-1-84
 Approved by Commissioner: Norman G. Gorsuch Date: 2-1-84
 Agency: Department of Law

Distribution (by Agency preparing fiscal note):

- Legislative Finance
- Legislative Sponsor
- Requestor
- Office of Management and Budget
- Impacted Agency(ies)

12/1/83

Fiscal Note
Analysis
HB 520

February 1, 1984

This bill addresses a limited area of criminal activity where a person uses a computer system or a computer network to commit a crime. Because existing statutes already cover most of the criminal acts set out in the bill, enactment of this legislation will have little, if any, fiscal impact on the Department of Law's operations. This bill's provision making it a crime to use a computer to obtain information with no legal right to do so concerning the credit information of a person clarifies and strengthens existing law.



POUCH V
JUNEAU, ALASKA 99811
(907) 465-4990

Alaska State Legislature
HOUSE OF REPRESENTATIVES

REPRESENTATIVE
CHARLIE BUSSELL
CHAIRMAN

Committee on Judiciary

HB 520
TABLE OF CONTENTS

- A. House Bill No. 520
"An act relating to criminal use of a computer."
- B. Sectional Analysis
Keith B. Levy, Legislative Counsel.
- C. Fiscal Note/Analysis
John Valensi, Information Resource Planning and Review, Department
of Administration.
- D. Position Paper of Support
James R. Shea, Deputy Commissioner, Information Resource Management.
Lisa Rudd, Commissioner, Department of Administration.
- E. Letter of Introduction to Representative Joe Hayes
Maureen S. Frisch, Regional Manager, TRW, Inc.
- F. Letter of Introduction to Representative Charlie Bussell
Maureen S. Frisch, Regional Manager, TRW, Inc.
- G. A Presentation on Computer Crime Legislation
TRW Information Services Division, TRW, Inc.
- H. "Credit Data"
TRW NEWS, TRW Information Services Division, TRW, Inc.
- I. A Report on Computer Fraud
TRW Information Services Division, TRW, Inc.
- J. Computer Crime Fact Sheet and Presentation
D. Barry Connelly, Senior Vice-President, Associated Credit Bureaus, Inc.
- K. Pertinent Local News Clippings
Anchorage Daily News

MEMBERS:
REP. JOHN LISKA, VICE CHAIRMAN; REP. RAMONA BARNES, EMERITUS;
REP. JOE HAYES; REP. HUGH MALONE; REP. DON CLOCKSIN; REP. RON WENDTE

STATE OF ALASKA
THE LEGISLATURE

POUCH Y - STATE CAPITOL
JUNEAU, ALASKA 99811
907-465-3800

LEGISLATIVE AFFAIRS AGENCY

MEMORANDUM

January 30, 1984

SUBJECT: Sectional analysis of HB 520

TO: Representative Charlie Bussell
Chairman, House Judiciary Committee

FROM: Keith B. Levy *KBL*
Legislative Counsel

You have requested a sectional analysis of HB 520, "An Act relating to criminal use of a computer." HB 520 creates the offense of criminal use of a computer (AS 11.46.575), a class C felony. A person commits the offense by knowingly accessing or causing to be accessed a computer for certain purposes listed in the statute. Those purposes include fraud, obtaining property illegally, obtaining or altering credit information, and altering a computer or computer program.

KBL:ojb
J3/014

STATE OF ALASKA 1984 LEGISLATIVE SESSION
FISCAL NOTE

Revision Date: _____, 1984

Page 1 of 2

REQUEST

Bill/Resolution No.: HB 520
 Title: An Act Relating to Criminal
Use of a Computer
 Sponsor: Hayes, Barnes, Liska, Furnace
 Requestor: _____
 Date of Request: _____

FISCAL DETAIL

Agency Affected: Dept. of Administration
 Program Category Affected: General Government
 BRU, Program of Subprogram(s) Affected:
Information Resource Management

EXPENDITURES/REVENUES: (Thousands of Dollars)

	FY 84	FY 85	FY 86	FY 87	FY 88	FY 89
OPERATING						
100 PERSONAL SERVICES						
200 TRAVEL						
300 CONTRACTUAL						
400 SUPPLIES						
500 EQUIPMENT						
600 LAND & STRUCTURES						
700 GRANTS, CLAIMS, ETC						
800 MISCELLANEOUS						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL	0.0	0.0	0.0	0.0	0.0	0.0
REVENUE	0.0	0.0	0.0	0.0	0.0	0.0

FUNDING: (Thousands of Dollars)

GENERAL FUND						
FEDERAL FUNDS						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

POSITIONS:

FULL-TIME	0	0	0	0	0	0
PART-TIME	0	0	0	0	0	0
TEMPORARY	0	0	0	0	0	0

SOURCE OF FUNDS TO OFFSET FISCAL IMPACT OF BILL:

ANALYSIS: Attach a separate page for any Analysis.

Prepared By: John Valensi *JValensi JRS*
 Division: Information Resource Planning and Review

Phone: 465-2200
 Date: January 23, 1984

Approved by Commissioner: Lisa Rudd *LJR*
 Agency: DEPARTMENT OF ADMINISTRATION

Date: 1/24/84

Distribution (by Agency preparing fiscal note):
 Legislative Finance
 Legislative Sponsor
 Requestor
 Office of Management and Budget
 Impacted Agency(ies)

12/1/83

House Bill 520
Fiscal Note Analysis
Prepared by the Division of
Information Resource Planning & Review
Department of Administration

January 23, 1984

The Department of Administration concurs with the intent of this Act. The following modifications are suggested, however, in order to broaden the applicability of the Act:

Sec. 11.46.575(a) (1) be modified to read:

"(1) devising or executing a scheme with the intent to deceive or defraud another person, business, or government entity;"

Sec. 11.46.575(a) (2) be modified to read:

"(2) obtaining money, property, or services with the intent to deceive or defraud another person, business or government entity;"

Sec. 11.46.575(a) (3) be modified to read:

"(3) obtaining information with no legal right to do so concerning another person or business;"

Sec. 11.46.575(a) (4) to be modified to read:

"(4) introducing false information into a computer system or computer network with no legal right to do so and with the intent to damage or enhance the data record of a person or business;"

POSITION PAPER

HB 520

This bill defines certain elements of computer stored data as private and classifies attempts to access, use or modify that data as criminal acts.

The Department of Administration supports this bill as an aid and clarification to administering disciplinary action in the area of data security infringements.

A recent incident pointed out the necessity for clearer statutory instructions in the area of non-authorized data access. This bill represents a step toward clarifying those instructions and lays a base for future statutes if deemed necessary.

James R Shea

James R. Shea, Deputy Commissioner
Information Resource Management

1/26/84

Date /

Lisa Rudd

Lisa Rudd, Commissioner
Department of Administration

1/26/84

Date

TRW Inc.

Executive Offices
One Space Park
Rancho Beach, CA 90278
213.535.2175

TRW

January 23, 1984

The Honorable Charlie Bussell
Member, Alaska State Legislature
Pouch V (MS 3100)
Juneau, Alaska 99811

Dear Representative Bussell:

We are writing to urge your support of House Bill 520, as introduced by House Speaker Joe L. Hayes.

This legislation would enact a computer crime statute for the State of Alaska and protect consumers from unauthorized access to and manipulation of sensitive computer-based information.

TRW's Information Services Division is one of the country's largest consumer credit reporting operations. We maintain credit information on more than 90 million consumers. We service these consumers through 21 offices and 80 independent credit bureaus, including Credit Data of Alaska, Inc.

We are keenly interested in this issue as it affects consumer credit history information, and we believe that this legislation is in the best interests of the consumer.

I have attached additional information on this issue and a brief description of our consumer credit reporting services.

Once again, we respectfully encourage your support of this measure. Thank you.

Sincerely,



Maureen S. Frisch, Regional Manager
TRW Inc. Government Relations

Attachment: as stated.



TRW Inc.

Executive Offices
One Space Park
Redondo Beach, CA 90276
213.535.2175

November 30, 1983

The Honorable Joe L. Hayes
Member, Alaska State Legislature
Box 1821
Anchorage, Alaska 99510

Dear Representative Hayes:

Tony Phister of the Credit Bureau of Alaska, Inc., suggested I contact you regarding our desire to sponsor legislation in your state dealing with the issue of computer crime. Our hope is that you will agree to author such legislation during your 1984 legislative session.

TRW's Information Services Division is one of the country's largest consumer credit reporting operations. We maintain credit information on more than 90 million consumers and service consumers through 21 offices and 80 independent credit bureaus serviced by TRW.

Computer crime and the unauthorized access to sensitive consumer credit information have become significant concerns to many companies. Unfortunately, existing state statutes are not adequate to deal with this growing problem, and we have successfully sponsored legislation in the states of California and New York to address the issue of computer crime as it relates to consumer credit history information.

The Honorable Joe L. Hayes
November 30, 1983
Page Two

To better familiarize you with TRW, our consumer credit reporting services, federal credit reporting laws, and the need for computer crime legislation, I have attached an information packet. I have also included the text of the California Penal Code (subsection 502) on this subject. The code itself deals with the broad subject of computer crime. The law was amended to include the unauthorized access to and manipulation of a consumer's credit history.

I hope you agree that this is an important legislative and consumer issue. We are most anxious to see similar legislation enacted in your state. To further discuss this with you, I will call your office within the next two weeks.

Thank you for your consideration of this matter.

Sincerely,



Maureen S. Frisch, Regional Manager
TRW Inc. Government Relations

cc: Tony Phister
Credit Bureau of Alaska, Inc.

Leo Spiekerman
TRW Information Services Division

Attachment: as stated.

A PRESENTATION ON
COMPUTER CRIME LEGISLATION

Prepared for
MEMBERS OF THE LEGISLATURE
THE STATE OF ALASKA

December, 1983

THE NEED FOR COMPUTER CRIME LEGISLATION

INTRODUCTION

Several issues related to the information services industry have led to the need for computer crime legislation.

The computer industry has created a consumer market that has put machines in the hands of hobbyists, and controls in the data processing industry have been reduced thru time-sharing options and other productional facets. While we see individuals invading systems in the news and entertainment mediums, the point is being raised that it will not be long before true criminals are involved in other areas. Unfortunately, this has become a reality. Little publicity is given to these cases of computer crime because they are not always turned over to law enforcement agencies. This is because computer crime statutes, for the most part, are either not in place or insufficient to result in prosecution. With little chance of achieving successful prosecution, or even getting to court, it is not surprising that many companies do not report computer crime.

Because of growing problems and concerns about unauthorized access to and manipulation of computer-based information, it is necessary to enact legislation. After unsuccessful attempts at the national level, it has become necessary to have progressive state legislatures implement legislation on a state-by-state basis.

UNAUTHORIZED ACCESS TO CREDIT INFORMATION

The credit industry has evidenced criminal behavior thru unauthorized access in three basic scenarios:

1. Consumer victimization via stolen access codes.
2. File manipulation.
3. Investigation and collection agency activity using stolen access codes.

Each of these scenarios is elaborated on separately to illustrate the impact of this activity and the need for up-to-date legislation.

Consumer Victimization

Attachment A, "For Sale: Credit Ratings," describes a process of victimization. The act of a consumer obtaining a good credit rating was facilitated by stealing subscriber access codes. The individuals that were selling these packages telephoned legitimate credit grantors subscribing to the credit agency. These individuals represented themselves as calling from the credit agency, usually using the pretext of clearing up a billing problem, or being from the security department. During the conversation the access code is requested and usually provided. This access code enables access to the credit data base to facilitate the process. The buyer of the good credit history uses the good accounts and requests other credit cards. The buyer runs up bills with no intent of paying. The good consumer is left with the issue of clearing up his or her credit history once it has been discovered that someone has used the individual's history.

File Manipulation

Attachment B illustrates the issue of file manipulation. File manipulation is achieved by bribing someone to modify the information contained in files within the bureau or subscriber's premises and the submission of false credit information.

Unfortunately, not all bureaus have controls to prevent this access and many incidents of information modification occur. Once the bad credit history is deleted or modified, the individual applies for new credit accounts. (Controls exist within the TRW system to prevent and/or isolate attempts of this type.)

Even if consumer victimization and file manipulation efforts are successful, most law enforcement agencies will not pursue the case until there has been a loss to a credit grantor.

Investigation and Collection Agency Activity (Attachment C)

Private investigators, lawyers, and repossession agents may, in isolated cases, have a legitimate purpose to access a credit data base; however, most of the major credit agencies do not allow these individuals to subscribe due to the control features required to monitor permissible access. Unfortunately, there have been many cases where individuals wanting this information have either stolen access codes or derived the access code from credit profiles sent to them by other subscribers with the access code on them.

Some collection agencies have acquired access codes in a similar manner. Although collection agencies have legitimate reasons to access a credit bureau, and they are subscribers, some do not use their own access code. The stolen access code is often utilized to reduce costs and increase commissions and agency profits.

A GROWING PROBLEM

According to recent statistics (Modern Office Procedures - March 1983, "Defending Your Computer Room Against Disaster") the average bank robbery is less than \$3,000. The average "white collar" embezzlement nets less than \$30,000. But the average computer crime is estimated to exceed \$600,000, with little chance of detection, prosecution or conviction.

Education has become a key element in the fight against this area of criminal activity, and the United States Department of Justice has opened a specialized four week computer fraud school for F.B.I. agents. The Department of Justice, Sacramento, California, operates a two week course specializing in the same subject. Other municipalities as well as private organizations are currently holding seminars to combat problem areas of detection.

The challenge is to actively prosecute computer crime suspects. A challenge in the sense that the current laws regulating computer access are extremely lacking. Following, are three examples of TRW incidents that illustrate the need for computer crime legislation:

Example #1

An organized ring of credit criminals was established in a large metropolitan area. Although this example was taken from the Western Region, there is an indication that an identical ring is operating in the Eastern Region. One member of the ring provided computer password information to another who used it to gain access to our system. The suspect then retrieved hundreds of credit reports. Through a relocation and file merge system, the suspect was able to alter negative credit information into what appeared to be a positive profile.

The fee charged for this service varied, however, it averaged about \$600 per report. This particular case is being actively prosecuted at the writing of this report. The section selected for prosecution was 502 P.C. (California).

Example #2

A collection agency/private investigative firm gained access to computer password information on several Information Services Division subscribers. As such, unauthorized access was made into our system and a total of \$65,000 worth of credits were applied for from various east coast subscribers. While working the investigation of this matter, several New York agencies were contacted and each declined investigative jurisdiction. Most felt that it was a civil or federal problem, in that no computer crime bill existed.

Subsequently, the F.B.I. was contacted and consented to continue the investigation. A suspect was identified and prosecution is being actively pursued.

Example #3

A coast-to-coast organized crime ring obtained several thousand blank credit cards. Later, they obtained illegal access into credit systems and retrieved thousands of credit profiles of potential victims. By viewing the reports, account number information was obtained and later embossed on the stolen cards. The total amount stolen from creditors is unknown at this time, but it is believed to exceed \$1,000,000. Investigation is continuing.

Crimes by these individuals were made possible through the illegal access to computer files. In each case the criminal simply called a TRW operator and relinquished certain password information which then caused the computer to be accessed.

It is acutely apparent that much has been done in the area of detection, but legislation is now needed for active prosecution.

CALIFORNIA'S COMPUTER CRIME LEGISLATION

SB 648 (California Penal Code 502), of which a copy is attached, was introduced in the California Legislature in March of 1981. This bill modified the penal code to make it a crime to intentionally access or cause to be accessed any computer system or network for the purpose of damaging the credit rating of any person. The bill was sponsored by an individual in the San Diego District Attorney's office, Fraud Division, in response to a situation in San Diego in which an individual's credit file was sold for the purposes of obtaining credit under fraudulent circumstances. (Similar legislation has been enacted in New York.)

Legislative justification for the bill goes on to say:

"The credit granting sector of private industry is being deluged with false and fraudulent applications for credit. It is not uncommon for individuals and organized groups to systematically apply for multiple credit cards, loans, etc. utilizing fictitious and false names, biographical information, and credit histories. These fraudulent applications are carefully created to fit within the credit grantors' criteria for issuance of credit - such policies which are well known to the applicants. Sophisticated wrinkles are added such as the use of telephone answering services, which have been provided a prepared script to read in case of inquiry by the credit granting agencies. The answering service tells the inquiring party 'that the applicant has been employed at a high salary for five years; that the applicant has successfully paid off a loan on a expensive automobile, etc.'

Under existing law, the credit grantor must suffer a loss before this activity can be filed as a felony. This ridiculous posture does nothing to prevent repeated attempts to obtain credit by fraudulent means. It is likewise discouraging to the credit grantors, who having discovered these activities, bring them to the attention of law enforcement and discover that this conduct is at most a misdemeanor. (Section 532a, California Penal Code)"

ONE STEP TOWARD A SOLUTION

Because of the tremendous growth in computer-based information services and concerns about the unauthorized access to and abuse of this information, it is necessary to adopt legislation. It has become clear that a national computer crime bill has little chance of passage. Some states, though, have passed legislation in this area, and, it is hoped that similar legislation can be passed in other states to facilitate interstate criminal prosecution and standardize penalties.

TRW's Information Services Division is prepared to support your state's activities to enact needed computer crime legislation. We recommend adopting statutes similar to those enacted in the States of California and New York (California's statute is attached).

11/1983

CALIFORNIA PENAL CODE - SUBSECTION 502

Definitions; computer system or network; intentional access to defraud or extort, or to obtain money, property or services with false or fraudulent intent, representations or promises; malicious access, alteration, deletion or damage; violations; penalty

(a) For purposes of this section:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer system or computer network.

(2) "Computer system" means a machine or collection of machines, excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contained computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(3) "Computer network" means an interconnection of two or more computer systems.

(4) "Computer program" means an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network.

(6) "Financial instrument" includes, but is not limited to, any draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(7) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(8) "Service" includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network.

(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.

(c) Any person who maliciously accesses or causes to be accessed any computer system or computer network for the purpose of obtaining unauthorized information concerning the credit information of another person or who introduces or causes to be introduced false information into that system or network for the purpose of wrongfully damaging or wrongfully enhancing the credit rating of any person shall be guilty of a public offense.

(d) Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

*** (e) Any person who violates the provisions of subdivision (b) *** (c), or (d) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars (\$5000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

*** (f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction.

auditors commended Sandia's corrective actions and stated that it appeared that the problems had been solved. However, it would not pay those responsible for the laboratory to become complacent. Without continual policing, the problem will return. The auditors recommended periodic random sampling of computer files to check on unauthorized use of the system. #

FOR SALE: CREDIT RATINGS

While evidence is still not clear, it seems possible that a data theft gang has been operating in southern California. It appears that the ring has allowed those with poor credit ratings to use someone else's good rating as the basis for opening charge accounts and obtaining loans.

The crime apparently involved unauthorized access to a credit bureau data base to obtain financial information about individuals with a clean credit history. Good credit ratings are sold to people who have problems obtaining credit. The bad credit risk purchases information that will allow him to assume for credit purposes the identity of someone who has the same name but a better financial record. Information supplied includes such things as social security number, bank account number, and driver's license number.

This suspected crime came to light when an individual with a good credit rating became aware that his identity was being used by another. He contacted a number of different law enforcement agencies and informed them about the alleged crime. To date, investigative efforts have been hampered by the fact that, although everyone acknowledges that a crime has indeed taken place, no one has been able to figure out who has jurisdiction. Meanwhile, a number of questions remain unanswered:

- How was the data obtained from the supposedly secure files of the credit bureau?
- Who obtained the data?
- Is it an inside job?

These questions will remain unanswered until jurisdiction problems can be ironed out and further information developed. #

STUDENT CRACKS SCHOOL DISTRICT'S COMPUTER SYSTEM

A high school senior in Tucson, Arizona was successful in breaking into the school district's computer system. However, he is beginning to have regrets about his actions. Since his successful intrusion, security measures have been tightened, and his access to the computer has been reduced.

The student, Joel Snyder, first realized that he could break the system's security code when he was accessing the computer through a remote job entry terminal at his high school. He was quoted as saying that anyone with a knowledge of assembly language could easily circumvent the system's security features. The passwords protecting student grades and other information were unimaginative.

His attempt to gain access to another user's password was successful. As a result, Snyder felt he should inform the authorities about the security risks involved. However, officials tended to doubt that Joel Snyder had actually cracked the system. They were willing to acknowledge that he had obtained access to passwords, but they were never sure how he had done it.

In his attempt to publicize the security weakness, Joel appeared at a school board meeting and brought the matter to the attention of the board. This action had some results. System security was soon tightened. Students are now allowed to access the system only from RJE stations (not by dialing up from a modem), only during certain hours, and only while a teacher is present.

While he has proven that he has more than a passing knowledge of computers and their security features, Snyder does not plan a career in data processing. His first college choice is Stanford University, where he plans to major in liberal arts.

Although Joel Snyder's reasons for breaking security were not malicious, his action shows the ease with which intelligent students can circumvent security features in today's systems. Obviously, there are basic weaknesses in most security provisions. #

SEP 3 1976 *R/L*

U.S. Charges Six Fixed Reports On Credit-Risk Buyers For Fee, Fed False Data Into Computers

Authorities Believe Plot May Have Led To Millions Of Dollars In Unpaid Bills

LOS ANGELES (AP) —With the aid of a file clerk, six men sought out persons with poor credit records and for fees of up to \$1,500 improved their credit reports in the computer banks of the country's largest consumer credit bureau, a federal indictment charges.

The credit records were kept in the computers of TRW Credit Data in Anaheim, Calif. The company maintains credit files on about 50 million Americans living in 20 cities.

The files are used by banks, credit card companies, and other businesses seeking

information concerning the credit worthiness of customers.

Authorities said the alleged scheme may have produced millions of dollars in unpaid bills and caused untold legal problems for firms that rely on credit information.

The six men are charged with conspiracy in the indictment returned Thursday by a grand jury. All six also are charged with at least one count of making false loan-application statements.

A TRW Credit Data file clerk, Kathleen Bennett, was named as an unindicted co-conspirator. Federal authorities said she is to be a government witness.

According to the indictment, Miss Bennett was paid \$50 each time she improved the computerized credit records of people solicited by the ring.

Some Information Deleted

This allegedly was done by deleting bad payment records, information about bankruptcies, and other unfavorable material. In some cases, material indicating a good credit history was inserted, authorities said.

The indictment listed 26 persons who paid between \$300 and \$1,500 to have their credit records altered, but authorities said as many as 150 persons may have paid for such falsifications between August, 1974, and March, 1975.

With their improved credit records, these people obtained banks loans, credit cards, and credit at retail stores, authorities said, and many of them subsequently defaulted on payments.

FBI agents uncovered the plot and broke up the ring 18 months ago, authorities said. It took the FBI, a Justice Department Organized Crime Strike Force, and the U.S. Attorney's office nearly 1½ years to obtain the evidence needed to present the case to a grand jury.

Seven Counts In Indictment

Charged in the seven-count indictment were Philip Kostoff, 31, the alleged ring-leader; his brother, Paul Kostoff, 35; Ronald C. Rossi, 41; John R. Dubbs, 41; Kenneth L. Stevenson, 39, and Sean Shanahan, 35. All live in Orange County, where Anaheim is located.

The indictment alleged that Philip Kostoff hired the other defendants to locate persons who wanted their credit ratings improved and also recruited Miss Bennett.

Authorities said TRW Data Credit, a division of Cleveland-based TRW, Inc., cooperated in the investigation and is lightening its security.

APR 6 1982 *EJL*

Authorities seize stolen computer reports

ORANGE — Detectives, armed with search warrants, last week seized several thousand credit reports that were allegedly stolen from TRW computers in Orange.

The records were seized by police during raids at three Los Angeles area companies — H.E.L. Locksmiths of Van Nuys, Searchers Investigations and Searchers Security Co., Los Angeles.

Police said entry into TRW's

computer bank was made via telephone and teleprinters, using that company's codes.

No charges were filed against the officers of the three companies.

The search warrants served Thursday and Friday culminated a three-month investigation into what police said is "the best of our knowledge, the first known reported crime of this particular type in California and the country."

Gil Hamblet, TRW's vice president of industry and public affairs, said the company first noticed the illegal access to their computer records six months ago.

He said the material relates to the pay habits of Southern California residents and does not include any other personal information, except their names, addresses and previous addresses.

The Van Nuys firm is an automobile repossession company

and the two Los Angeles companies are private investigators who work for attorneys and corporations.

"Such records are used to obtain credit information on individuals," Detective John Carson said. "The records are also used in skip tracing."

Carson said the material is now being inventoried, and it will probably be a week before the police and the district attorney will be ready to file charges.

Los Angeles Times
LARGEST CIRCULATION IN THE WEST
LOS ANGELES CAL.
D. 1,000,945 S. 1,234,115

APR 7 1982 *EJL*

3 Firms Probed in Theft of TRW Computer Data

Two Los Angeles private detective agencies and a Van Nuys vehicle repossession firm have been accused of massive electronic theft of credit information from a computer at TRW, Orange County authorities said Tuesday.

Police said the three firms gained access to the nationwide credit reporting agency's computer by obtaining codes issued to TRW subscribers. No dollar value has been set on the alleged theft.

Investigators said Tuesday that H.E.L.P. Locksmiths, the repossession company, had been using the code for six months. Searchers and Securities and Searchers Investigators, the detective agencies, had been using them since 1972, police said.

Orange police Detective Roger Braham said no charges have been filed, but investigators are examining thousands of records—mostly computer printouts—seized from the three firms in raids last week.

Gil Hamblet, vice president of public affairs for TRW's Information Services Division in Orange, said the firm's own security surveillance system first spotted the illegal information request entries in January.

Officials of the three companies that allegedly obtained the information illegally could not be reached for comment Tuesday.

APR 6 1982

Authorities seize stolen computer reports

ORANGE — Detectives, armed with search warrants, last week seized several thousand credit reports that were allegedly stolen from TRW computers in Orange.

The records were seized by police during raids at three Los Angeles area companies — H.E.L.P. Locksmiths of Van Nuys, Searchers Investigations and Searchers Security Co., Los Angeles.

Police said entry into TRW's

computer bank was made via telephone and teleprinter, using that company's codes.

No charges were filed against the officers of the three companies.

The search warrants served Thursday and Friday culminated a three-month investigation into what police said is "to the best of our knowledge, the first known reported crime of this particular type in California and the country."

Gil Hamblet, TRW's vice president of industry and public affairs, said the company first noticed the illegal access to their computer records six months ago.

He said the material relates to the pay habits of Southern California residents and does not include any other personal information, except their names, addresses and previous addresses.

The Van Nuys firm is an automobile repossession company

and the two Los Angeles companies are private investigatory who work for attorneys and corporations.

"Such records are used to obtain credit information on individuals," Detective John Carson said. "The records are also used in skip tracing."

Carson said the material is now being inventoried, and it will probably be a week before the police and the district attorney will be ready to file charges.

Los Angeles Times
LARGER CIRCULATION IN THE WEST
LOS ANGELES CAL.
D. 1,000,945 S. 1,234,113

APR 7 1982

3 Firms Probed in Theft of TRW Computer Data

Two Los Angeles private detective agencies and a Van Nuys vehicle repossession firm have been accused of massive electronic theft of credit information from a computer at TRW, Orange County authorities said Tuesday.

Police said the three firms gained access to the nationwide credit reporting agency's computer by obtaining codes issued to TRW subscribers. No dollar value has been set on the alleged theft.

Investigators said Tuesday that H.E.L.P. Locksmiths, the repossession company, had been using the code for six months. Searchers and Securities and Searchers Investigators, the detective agencies, had been using them since 1972, police said.

Orange police Detective Roger Braham said no charges have been filed, but investigators are examining thousands of records—mostly computer printouts—seized from the three firms in raids last week.

Gil Hamblet, vice president of public affairs for TRW's Information Services Division in Orange, said the firm's own security surveillance system first spotted the illegal information request entries in January.

Officials of the three companies that allegedly obtained the information illegally could not be reached for comment Tuesday.

TRW NEWS

INFORMATION SERVICES DIVISION OF TRW INC. • 505 CITY PARKWAY WEST • ORANGE, CALIFORNIA 92688

FOR RELEASE:

TRW Information Services Division

CONTACT:

Credit Data

A CAPSULE DESCRIPTION

TRW Information Services operates and markets one of the nation's largest, computerized consumer credit reporting services called Credit Data. TRW has credit information on more than 86 million consumers, and serves 24,000 subscribers at 35,000 locations.

TRW collects and stores factual credit information on consumers and provides that information to credit grantors that subscribe to the service including banks, retailers and finance companies. The TRW Updated Credit Profile contains credit account information provided by subscribers including positive and negative information about retail credit card accounts, bank charge card accounts, lines of credit, secured loans and finance company accounts. The Profile also includes selected public record information limited to tax liens, judgments and bankruptcies. TRW does not collect information on checking and savings accounts, race, religion, sex, salary, personal lifestyle or criminal records.

Open current credit accounts remain on the Profile indefinitely. Closed or paid accounts are removed within seven years. Adverse credit information remains on file for a maximum of seven years, with the exception of bankruptcies, which remain for a maximum of 10 years.

HISTORY

The development of consumer credit reporting agencies was a direct result of the rapid growth in the use of credit and need for consumer credit repayment information. As more and more businesses began extending credit to consumers, there was an increasing need for information on how those consumers repaid their credit obligations with other creditors. To meet this need, individual businesses began to collect their customer repayment information and exchange it within branches of their own company or within their industry. This credit information was kept in paper files in a central location. As the volume of credit information grew, the job became too large for individual businesses.

Credit bureaus soon developed, meeting businesses' need for a central repository of credit repayment information that provided credit grantors with a more complete picture of consumers' repayment habits. The Michigan Merchants Credit Assn. in Detroit was one such bureau, which was founded in 1932 by Norman Jordan, and taken over by his son, Harry ("Bud") Jordan, in 1956. The company was incorporated in Michigan in August of 1960 as the Credit Data Corp. and used file cabinets and 3" x 5" cards to store consumer credit information. In 1965 Credit Data initiated and installed the first computerized, on-line credit reporting system. It was acquired by TRW Inc. in November 1969 and became TRW Credit Data.

HOW CREDIT GRANTORS USE CREDIT REPORTS

TRW provides credit information to bona fide credit grantors who have a legitimate business need for the information. When consumers apply for

credit, they generally authorize a credit grantor to obtain information on their credit history. Credit grantors use TRW's service when considering applications for credit, or when reviewing their current accounts. Credit grantors apply their own evaluation criteria to the information TRW supplies in determining whether to grant or deny credit. In addition to the information on a Credit Profile, credit grantors also take into consideration information not supplied by TRW, such as the consumer's employment, income, other assets and outstanding debts. TRW does not make the decision to grant or deny credit.

HOW AUTOMATED CREDIT REPORTING WORKS

TRW provides credit information to credit grantors that assist them in the credit granting decision. In turn, they provide TRW with a record of their past and present credit account information. This is usually done on a monthly basis. Since the majority of TRW subscribers have their accounting function computerized, they typically provide the information via magnetic tape, copied directly from their billing records used to notify their customers. These tapes are sent to TRW's data center in Anaheim, Calif., where they are entered into the TRW computer system. This regular receipt of credit information provides TRW with an automatic updating of the credit account information in the files. Public record information is gathered directly from court records, converted to a computerized format and entered into the computer system in the same manner as credit information from credit grantors.

THE CREDIT PROFILE

The TRW Credit Profile contains up-to-date credit information on consumers' credit accounts, items of public record, inquiries, and a consumer's identifying information. (A sample Credit Profile is included in this package.)

--Identifying Information: the consumer identifying information is limited to the consumer's full name (including generation, such as "Junior" or "Senior"), address, social security number, age or year of birth, and spouse's initial. The consumer's place of employment, as indicated by the consumer on a credit application, may also be contained in the Profile.

--Credit Account Information: includes the name of the company reporting the account, the date the information was reported, the date the account was opened, the type of account, terms, the original balance or credit limit, current account balance, amount past due and the status of the account, such as "current account" or "30 days past due."

--Inquiries: whenever a request is made for a copy of the Profile, that request, or "inquiry," is automatically recorded on the Profile and is retained for a period of one year. Inquiries include the name of the inquiring company and the month, day and year of the inquiry.

--Public Record Information: includes the name and location of the court from which the data was obtained, a description of the item, such as "judgment" or "state tax lien," the docket number and/or page number where it was located, date and the status of the item, such as "judgment

of their Credit Profile from TRW, through TRW's 21 Consumer Relations offices across the country. They should include the following information in their request:

- : Full name (including generation, i.e., Jr., Sr., III, etc.)
- : Addresses for 5 years
- : Social Security Number
- : Year of birth
- : Signature

If the consumer has been denied credit within the past 30 days, there is no charge for the Profile. Consumers should indicate the company that declined them credit or include a copy of the declination letter with their request. If they have not been denied credit within the past 30 days, there is a \$8 fee. (\$5 in Maryland). The request should be mailed to the TRW Consumer Relations office closest to their home (See list of TRW locations). Eighty-six percent of the consumers who request their Credit Profile from TRW do so by mail.

Consumers may also make a personal visit to TRW offices during business hours to receive a copy of their Credit Profile and speak to a trained representative, who will explain its contents. To make an appointment for a personal visit, consumers should call the TRW Consumer Relations office closest to their home. Fourteen percent of the consumers who contact TRW make a personal visit to TRW's Consumer Relations offices.

TRW reinvestigates any item on a consumer's Credit Profile that the consumer disputes. This is done by contacting the source of the information to verify its accuracy. If there is any item on the Credit Profile that

--Designations: each item of credit or public record information is assigned a general designation of "positive," "negative" or "non-evaluated," depending on the status of the account or public record item. A paid satisfactory account, for example, would be designated as a positive item. These designations -- selected through the consensus of credit grantors that use TRW's service -- are provided as a service to credit grantors. TRW does not provide a general credit rating -- such as "A-1" or "Triple-A Credit" -- on an individual.

--Payment Profile: is another service to credit grantors that provides them with an immediate comprehensive picture of the consumer's payment history for the last 12 months. An account that has been current for the last 12 months, for example, would be indicated in the Payment Profile as a series of "C's," representing "current." A 30-day, or one month past due, would show on the Payment Profile as a "1" in the column for that month.

--Consumer Statement: if the consumer so chooses, a consumer statement of 100 words or less regarding any item that TRW has reinvestigated and with which the consumer is still dissatisfied may also be included on his or her Profile.

(A more extensive explanation of status comments, association codes, types of accounts, and items of public record is included on the back of the sample Credit Profile).

DISCLOSURE TO CONSUMERS

Consumers may obtain a copy of their Credit Profile anytime by writing to TRW directly. Approximately 500,000 consumers a year request a copy

Billing Act, summarized below, are the three most important laws for consumers to be aware of.

FEDERAL FAIR CREDIT REPORTING ACT

Gives you the right....

...to know what credit information is held that pertains to you, without charge if you've been denied credit within 30 days

...to know who has received a report on you in the past six months

...to have information pertaining to you, which you dispute, reinvestigated and corrected or removed if inaccurate or unverifiable

...to place a statement in the credit reporting company's records if you continue to dispute the accuracy of an item after reinvestigation

...to have an updated report sent to those credit grantors who have received a report pertaining to you in the last 6 months

...not to have adverse information pertaining to you over 7 years, or 10 years for bankruptcies, kept or reported

EQUAL CREDIT OPPORTUNITY ACT

Gives you the right...

...to be judged on an equal basis with all other credit applicants

the consumer disputes, the nature of the dispute should be indicated in the column provided on the Credit Profile and returned to TRW. TRW will reinvestigate the disputed item with the source of information. If the item cannot be verified, it will be deleted from the record. TRW notifies the consumer of the result of that reinvestigation by sending the consumer an updated copy of the Credit Profile. Of the approximately 500,000 consumers a year who request copies of their Credit Profile from TRW, less than one-third dispute information on the Profile.

Consumers may add a consumer statement to their Credit Profile regarding any item which TRW has reinvestigated and with which they are still dissatisfied. This statement will tell the consumer's side of the story in his or her own words, and will be included with all inquiries to the consumer's Credit Profile. TRW will work with consumers to formulate the statement, which should be limited to 100 words or less and should not include libelous comments.

SAFEGUARDS

TRW's contract with subscribers specifies the Credit Profiles be used only in accordance with the permissible purposes outlined in the Federal Fair Credit Reporting Act. TRW has extensive security procedures, including safeguards for protecting the computer equipment, computer center, information files, systems programming and access to the TRW system.

CREDIT AND FEDERAL LAW

There are a number of federal laws that pertain to credit. The Fair Credit Reporting Act, Equal Credit Opportunity Act, and Fair Credit

...to have joint accounts reported for both spouses separately after
June 1977

...to have your income considered without regard to sex or marital status

...to have child support and alimony payments regularly received counted
as income, if requested

...not to be asked questions about birth control or child bearing plans

...to obtain a credit card in your own name if you are a married woman

...to know the reasons you have been denied credit

FAIR CREDIT BILLING ACT

Gives you the right...

...to file a written complaint with the credit grantor within 60 days after
the bill you question was mailed to you

...to receive an acknowledgement from that credit grantor within 30 days
after that, and a settlement within 90 days

...to forestall collection of the account until the dispute is resolved and

...to prohibit that credit grantor from reporting negative information
regarding the disputed amount to credit reporting agencies until the dispute
process is completed

OTHER CREDIT REPORTING AGENCIES AND INDEPENDENT BUREAUS

TRW is one of the largest of five major, U.S. computerized credit reporting agencies. The others are TransUnion (Chicago); Credit Bureau Inc., a division of Equifax (Atlanta); Chilton (Dallas); and Pinger (Houston).

There are many more smaller, independently owned credit bureaus nationwide that provide an important service to their communities. TRW has contractual agreements with 28 such bureaus to provide them with the latest data handling technology and enhancements, while at the same time allowing them to retain independent control of their operations, as well as access TRW's data.

"The 1980's will be to computer bandits what the days of Prohibition were to Al Capone - wide open with little fear of apprehension or prosecution." This analogy was offered by August Bequai, a Washington attorney and nationally recognized expert on computer crime. He went on to say that the legislative and criminal justice system "is thoroughly unprepared to deal with the problem of computer fraud." Its safe to say that the computer felons are at least a century ahead of the criminal justice system ostensibly designed to stop them."

Several issues are apparent in the information services industry that has led to this situation and the requirement for computer legislation.

The computer industry has created a consumer market that has put machines in the hands of hobbyists as well as reduced controls in the data processing industry thru time-sharing options and other productional facets. The computer industry starting with ENIAC in 1946 was projected to grow to 500,000 computers in 1990. By 1970 there were 140,000 computers. Little did anyone realize that the microcomputer boom would be producing 1,975,000 units in 1982. One of these home computers can be as powerful as that first computer. The home hobbyist has dial-up capability to many public data bases, mail services and other computers. The Government Services Administration has developed a community bulletin board to facilitate information exchange about microcomputers.

Today more than 50% of the U.S. labor force is engaged in some aspect of the information industry. Over 90% of business related jobs involve contact with a computer.

While we see "Hackers" invading systems in the news media and entertainment media, the point is being raised that it will not be long before true criminals are involved. Unfortunately they are already here! Little publicity is given to these cases because

JAN 24 04 11:13 TRW-130 ORANGE PUS

they are not always turned over to law enforcement because computer legislation, for the most part, is either not present or insufficient to result in prosecution. With little chance of achieving successful prosecution, or even getting to court, it is not surprising that many companies do not report computer crime except as necessary. The cost benefit analysis of doing so is lop sided to provide only a negative image in the market place.

The types of computer-related crimes fall into the following categories:

- 1) Theft of Data: Involves the misuse of confidential business or personal data
- 2) Unauthorized Use: Use of another's computer for personal use.
- 3) Vandalism: Involves both the computer and programs.
- 4) Sabotage: Involves the destruction (partially or in total) of an EDP system.
- 5) Economic Crimes: The computer is used for manipulating or misappropriating company assets; embezzlement; wire fraud; securities fraud and any other dishonest financial scheme.
- 6) Espionage: Use of the computer to gain valuable property or data.

No one really knows how much computer abuse there is. Donn Parker of SRI is probably the most knowledgeable on the subject. He has reviewed 849 reported cases over the last 11 years. He has observed that there is no general agreement as to the meaning of the

terms computer crime or abuse. His case analysis, on the attached chart, revealed a number of unreported cases. He found that few victims were willing to disclose the incident. His findings are based on reports by the news media and, as such, contribute to the leveling off effect. In the Spring 1983, Computer Security Journal he states: "We do not need statistics of total incidence and loss to motivate us to take prudent care of assets and to implement generally accepted safeguards and security practices. Let us get back to the job of protecting business and government from computer abuse, based on the fact that it is occurring and has changed the nature of business crime, that losses can be very large, and that reasonable scenarios of potential loss demonstrate the existence of serious vulnerabilities."

His analysis of losses show that the degree of loss is significantly different. In the area of bank fraud the manual perpetration averages \$19,000 whereas the computer assisted crime nets \$450,000. While accurate statistics involving dollar amounts and the number of crimes are impossible to obtain most law enforcement experts say they are increasing at an alarming rate and expect these statistics to grow. This premise is apparent as automation in every sector of business and government increases. K. Lydon in "Security World," Sept. '82, stated "Computer crime losses are estimated at between \$300 million to \$3 billion per year. It is difficult to detect and unpopular to report. The average computer crime is \$400,000 to \$500,000. About 85 to 95 percent goes unreported." For this reason it is imperative that computer legislation be established. After unsuccessful attempts at the national level it has become necessary to have progressive state legislatures implement legislation on an individual basis.

The record for prosecution of computer crime cases is poor. A. Bequal at the "Compacts '83!" conference in England stated that fewer than 5% of all securities-related frauds in the U.S. are referred by the police for prosecution. Law enforcement has adopted many programs to train themselves in this new technology, but have been confronted with laws that leave them ill-equipped to prepare a prosecutable case. Our criminal statutes were designed for another era dominated by paper.

JAN 24 04 11 16 TRW-13D ORANGE P03

The laws presently being applied in computer crime cases are:

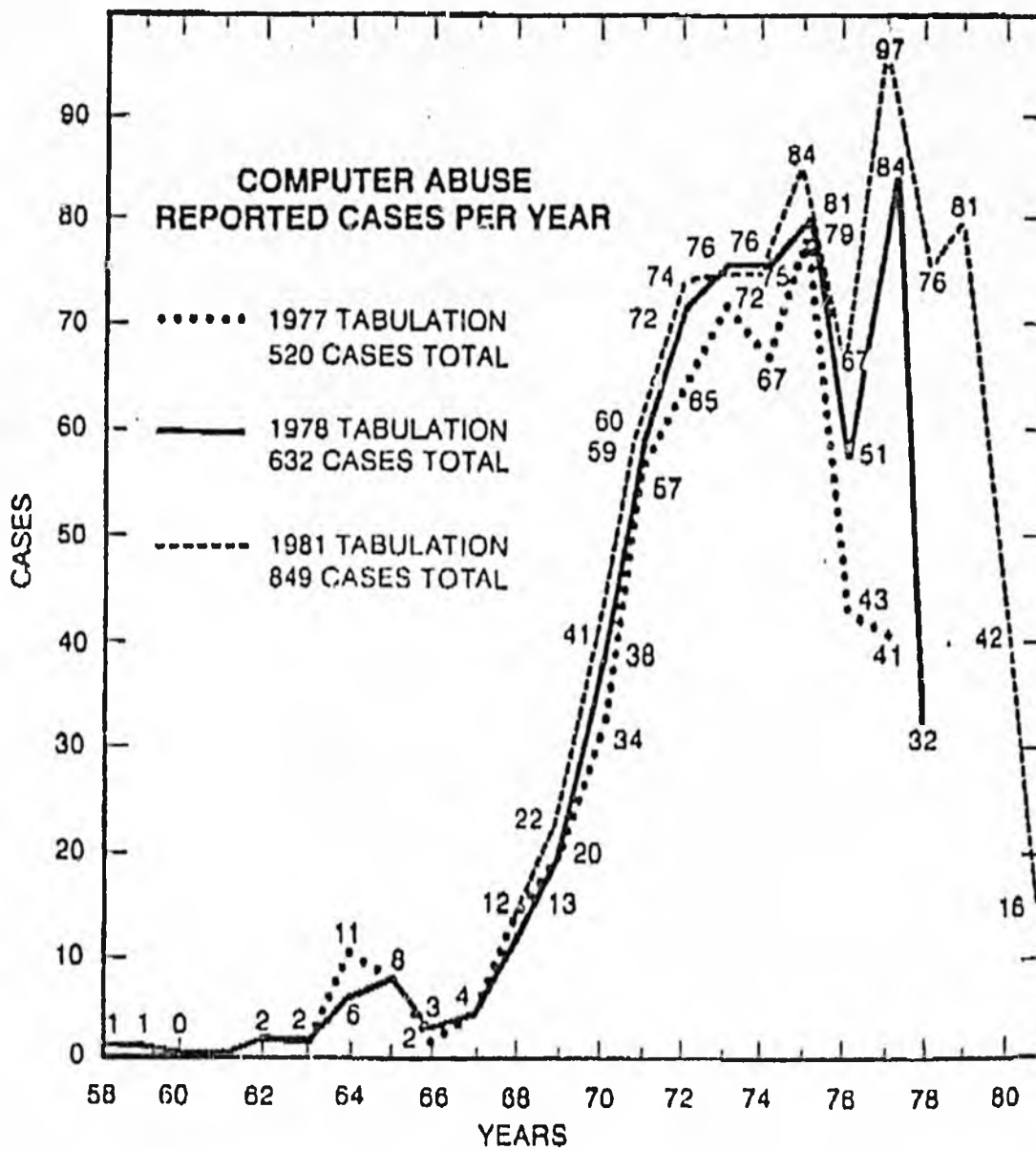
- o Wire Fraud Statutes: These acts relate primarily to transmittals by "means of wire, radio or television" in interstate or foreign commerce. They are difficult to apply to electronic transmissions.
- o Bank Fraud Statutes: These statutes pertain only to bank "insiders" and the taking or concealment of funds. It is difficult to extend the definition to electronic formats.
- o Mail Fraud Statutes: The perpetrator must use the paper based U. S. Postal System. Most criminals use electronic access.
- o Title III of the Omnibus Crime Control Act: This Act is aimed at the interception of wire or oral communications. Data communications is probably not applicable under the Acts definition.
- o Counterfeiting & Forgery Statutes: These statutes are of limited value since a paper format is rarely made or forged.
- o Robbery Statutes: Application is to forcible attempts to steal property from Federally insured or regulated institutions.
- o Extortion Statutes: These statutes can be used if force or fear is used to obtain property. It could be applied to terrorists.

Although computer criminals have been prosecuted under the statutes, more definitive law is required. Such legislation has been enacted under California PC502 and New York.

The California law has resulted in several arrests in the last law year with prosecutions pending. Law enforcement has found no difficulty in applying the law since it relates to computer technology.

In relation to my initial statement, regarding hackers in the newspaper and entertainment media, the Computer Security Institute analyzed this phenomenon in their latest conference. It was stated that "Hackers begin with the perception of information as a public asset and use it freely when and where it is available." It was pointed out that they are not deterred by raising the cost of penetration. The hacker is perfecting his skill. The CSI newsletter points out "The lesson we must learn from the hackers is that "it" can be done and is being done today." What we in the business and legislative arena must learn is that there must be updated and effective legislation to cope with the issues of a computer age.

FIGURE 1
Computer Abuse Case File History





Associated Credit Bureaus, Inc.

16211 Park 10 Place • PO Box 218300

Houston, Texas 77218 • (713) 492-8155

JAN 31 1984

COMPUTER CRIME FACT SHEET

1. The manipulation of and unauthorized access to sensitive computerized data has become increasingly widespread, particularly with the advent of the home computer. Multiple news articles and Congressional hearings have highlighted the problem.
2. Computer crime has grown in scope and severity to the point that many American businesses now carry related insurance protection.
3. Unauthorized access to computer data can have far-reaching effects beyond those encountered by the actual recordkeepers. Consumers, especially, may be unwitting victims in the possible manipulation of medical, bank, education and credit records.
4. Technology has moved more quickly than legislation creating laws to punish manipulators of computer data. State statutes outlining stiff penalties for manipulation of or unauthorized access to computer data are necessary to help protect business and consumers.



Associated Credit Bureaus, Inc.

1984 STATE LEGISLATIVE PROGRAM PARTICIPANTS

Computer crime, ACB Members, ATTN: TONY PFISTER

has become increasingly prevalent, especially with the growth in popularity of home computers. The U.S. Congress has already shown an interest in the subject by holding a series of hearings featuring computer "hackers" and security experts as witnesses. In addition, a great deal of publicity has appeared on the subject.

For those reasons, our 1984 State Legislative Program, in which your state association's leadership has elected to participate, takes on a new dimension. In previous years we have concentrated on explaining credit reporting and collections to your legislators. That remains an important and necessary task, but this year we're encouraging you to go a step further and assume an advocacy role in the area of computer data security. Specifically, you should promote the passage of legislation establishing strong penalties for tampering with computerized records.

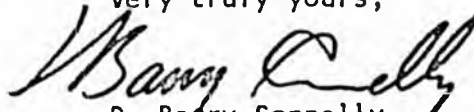
The need for this type of legislation is twofold. First, in most states no options exist for prosecuting employees or others who tamper with credit or other computerized records. Second, by recognizing and acting on the problem we further establish our industry as one which is willing to utilize proper legislative channels to bring about change necessary to protect the millions of consumers affected by our industry. By supporting legislation to further secure all types of computerized data, you can anticipate building a strong coalition of support with other industries which depend upon safe data storage.

With or without our industry's participation you can anticipate that there will be computer crime legislation introduced in your state. We think an active, positive approach will serve your interests far more effectively than a reactive approach.

The enclosed material will be of help to you in explaining this important issue to your legislators, either by mail or in person. Please let us know about your success in this endeavor.

Best personal regards.

Very truly yours,


D. Barry Connelly
Senior Vice President

Enclosure

Computer-Fraud Coverage Grows As Insurers Solve Policy Problems

By JOANNE LIPMAN

Staff Reporter of THE WALL STREET JOURNAL

An oil company paid millions of dollars to gather highly confidential geophysical information and then fed the data into a computer. Now it wants insurance against electronic theft of the data by competitors or damage to its storage system by teen-age computer hackers. Is such coverage available?

The answer is yes, some insurers say. But the kinds of coverage available vary widely, and most insurance companies are still at work developing their policies. A few insurers cover theft of trade secrets and such items as customer lists. Others cover only the cost of reproducing erased or damaged information. All agree there are problems to overcome: Losses are hard to calculate and potentially staggering, for example, and premiums can be very high. But everyone also agrees that once the problems are solved, business will be hot.

Computer-fraud coverage "is the most sought-after insurance in the crime area these days," says Christopher Barr, vice president of National Union Fire Insurance Co. "The computer is the fad of the 1980s—and computer insurance is the fad topic of the insurance world."

So far, only about \$20 million of electronic-crime policies have been sold and most of them cover transfers of money and securities, according to Dean P. Felton, a vice president of Marsh & McLennan Cos. But he figures that amount will increase geometrically, reaching \$100 million in the next three years.

Demand is already rising. Shand, Morahan & Co., a subsidiary of Alexander & Alexander Securities Inc., says inquiries about its policy have doubled in the past six months, to 75 a week. Applications for the coverage have risen 20% to 30%, says Grant R. Hubbard, a Shand Morahan vice president. St. Paul Fire & Marine Co., Fireman's Fund Insurance Cos., Chubb & Sons Inc. and others report a similar increase in interest.

A New Twist in Coverage

Insuring computer data against theft and damage is a new twist in electronic-crime coverage. One of the first computer-crime policies, introduced by Lloyd's of London in 1981 and quickly copied by several American insurers, applied only to financial institutions and covered only money and securities transferred by electronic means.

That kind of policy was inspired by the exploits of Stanley Mark Rifkin, who was charged with swindling Security Pacific Bank of Los Angeles out of \$10.2 million in 1978. According to prosecutors, he posed as an international bank officer, got the computer codes required to transfer money to a Swiss bank, and then bought 19 pounds of Russian diamonds with the proceeds. Back then, the case was hailed as the ultimate electronic scam.

But a new type of computer crime is

drawing attention now, and its immediate target is information rather than money. Insurers can reel off tales of computer treachery. There's a company, for example, whose client file was pilfered electronically by a competitor. In another case, a prankster gained access to computerized motor-vehicle records, wiping out penalties given poor drivers. Recently, the Federal Bureau of Investigation has arrested teen-agers who allegedly broke into computers belonging to the Defense Department, a New York City hospital and an electronic-mail service.

Crimes like these make companies very nervous. Chubb, for instance, says it has sold computer-fraud policies to an aerospace

Insuring computer data against theft and damage is "a new area, and there are no hard and fast decisions on who is liable for what," says a State Farm executive.

company worried about piracy of its designs and a book publisher concerned that an outsider could steal unpublished books. Shand Morahan says travel agencies, county governments, department stores and stockbrokers have shown interest in its policy.

Computer-data coverage varies from insurer to insurer. St. Paul Fire & Marine covers the cost of reproducing erased or damaged information, including footwork or research. That means that if a client list is erased, the insurer will pay for the extra time and work required to recreate it. But "snooping" isn't covered. As a result, if a competitor steals the client list electronically without damaging the data, no payment is made.

Chubb's policy does cover snooping. If information is stolen and used by someone, the policy covers the full amount spent to develop the data. Thus, if a new automobile design is stolen from a manufacturer's computer and the new car becomes uncompetitive as a result, Chubb will cover such costs as research and promotion. If the car is still marketable but sales are hurt because the design is no longer exclusive, a smaller payment will be negotiated.

Shand Morahan may offer the most ambitious policy. It promises to cover all computer-fraud-related costs, up to \$30 million for a single incident. It will even cover the cost of inventory stolen by electronic means. Such cases have occurred in the past. In the early 1970s, Jerome Schneider was convicted of procuring more than \$200,000 of telephone equipment from Pacific Telephone & Telegraph Co. in Los Angeles.

But many insurers are still trying to de-

termine formulas for insuring computerized data. "It's a new area, and there are no hard and fast decisions on who is liable for what," says Wesley Ooms, assistant vice president of State Farm Mutual Insurance Co., which doesn't offer any computer-fraud coverage.

One problem is that insurers like to stick with quantifiable losses. That makes them reluctant to cover less-concrete costs, like loss of confidentiality and confidence among customers.

There are other problems. While no claims have been made yet, they may be devastating when they come. "We don't expect them to be numerous," says Ralph W. Wheeler Jr., an executive at Aetna Casualty & Surety Co., "but we expect a catastrophe when it happens." Mr. Hubbard of Shand Morahan believes losses among his company's customers will "always be in excess of seven figures."

With the potential for losses like these, premiums can be enormous. They tend to run between \$25,000 and \$100,000 a year, depending on the size of the business and how secure its computer system is. But coverage can cost a large bank as much as \$4 million over three years, according to Mr. Wheeler of Aetna. If the company has a backup computer or other alternate system, insurance costs are usually lower.

Giving Hackers Ideas

Most companies are reluctant to talk about their computer-crime coverage for fear of giving hackers and competitors ideas. "Nobody's going to admit carrying this coverage," says Mr. Hubbard, of Shand Morahan. "It's the same thing as kidnap coverage."

But law firms, which computerize data about cases, and airlines, which computerize everything from accounts receivable to reservations, are among the kinds of companies looking into coverage. "Anyone who uses information-systems technology is going to have to look at this type of insurance," says Don Karmazin, vice president of computer and communications services at United Airlines.

United is self-insured, but it plans to study coverage carefully as it becomes more readily available. "It has been talked about in the industry," Mr. Karmazin says, "especially with all the notoriety that these teen-age computer whiz kids have been getting."

McGraw-Hill Inc. has computer-crime coverage, but it says all its risks still aren't covered. Its policy covers the cost of recreating damaged information, but if an electronic trespasser reads—but doesn't damage—an unpublished stock appraisal from McGraw-Hill's Standard & Poor's Index or an unreleased article from its BusinessWeek magazine, no payment is made.

"We hit the stumbling block," says John J. Bott, corporate risk manager. "It's a gray area. We're going round and round on this at least once a month."

For Fun or Foul, Computer Hackers Can Crack Any Code

Many Just Like the Challenge,
Others Like to Show Off;
The Cookie Monster Caper

By ERIC LARSON

Staff Reporter of THE WALL STREET JOURNAL

SAN FRANCISCO—When their computer started talking dirty, the computer staff members at U.S. Leasing International Inc. knew they had a problem.

The company's typically well-behaved machine had this to say to one of the machine's operators: "The Phantom, the system cracker, strikes again. . . . Soon I will zero (delete) your disks and your backups on System A. I have already crashed your System B. Have fun trying to restore it, you fobscuity)." Some other suggestions were made about what the operator could do with various pieces of computer equipment.

The culprit turned out to be a bright 20-year-old man who had secretly fiddled with the company's machine by telephone from Los Angeles to show off his computer knowledge.

That is the darker side of "hacking," as computer fiddling is known. At the Massachusetts Institute of Technology, where the term is said to have originated, hacking usually has a lighter side. Richard Stallman, a professional programmer at MIT, says a hacker originally was one who knew computers inside out, got a nonprofessional amount of fun out of them and could appreciate the irony and the beauty of a program. He refers to himself as a professional hacker.

'Electronic Vandalism'

Outsiders now use the term to describe all kinds of computer yahoos who electronically invade other people's computers, usually just for the challenge. "I call it electronic vandalism or technological trespassing," says Donn B. Parker, a computer-security consultant with SRI International in Menlo Park, Calif.

For business it's a growing problem, thanks to the proliferation of home computers and computer expertise. "People don't realize the extent to which their systems are being broken into," says Clifton H. Garrott, the Los Angeles deputy district attorney for electronic crimes, who prosecuted the U.S. Leasing case.

At the lighter end of the hacking spectrum are those computer jokesters who use such hacker classics as the "Cookie Monster" program. A San Francisco programmer's version went like this: At brief intervals his program would interrupt another user's work and flash "Cookie" on his screen. The machine would then grow more frantic, sending whole lines of "Cookie" across the unsuspecting user's terminal, finally letting loose with a primal scream: "Gimme Cookie!" If the user tried to stop the program, the machine would bristle: "Don't do that, Monster not like that." The only way to stop the Monster was to feed it a cookie—that is, type the word "cookie."

The Nixon Variation

At MIT, hackers once substituted former President Richard Nixon for the Cookie Monster; the alleged Mr. Nixon demanded immunity from prosecution.

Many hackers just like to browse the electronic byways of the country, exploring a digital never-never land entered through the telephones beside their computers or terminals they aren't supposed to have access to. Recently, the University of Michigan and Ann Arbor, Mich., police captured an electronic peeping Tom, who for about a year had wandered among the files on one university computer system out of curiosity. He was a former student. "We decided to prosecute because we take this very seriously," says Aaron Finerman, the director of the university's computing center. University policy says a student can be expelled and a staff member fired for that kind of thing. The culprit pleaded guilty to a misdemeanor.

To satisfy a need to browse, Geoffrey Goodfellow, now a part-time systems analyst for SRI, once broke into a major computer time-sharing network. "I like to see how things work," he says. "In order to see things work, you have to have carte blanche to look around." Browsing, in fact, helped him get his job at SRI. While loitering once in an SRI computer, he says, he left an electronic note saying he would do some programming free if SRI would give him a computer account that would let him use the computer. SRI gave him an account, and the affiliation grew from there, he says.

Browsing hackers get help from the underground network of electronic bulletin boards suspended in computer circuits around the country. By leaving messages at these, hackers can swap passwords, identification numbers and computer phone numbers to help them get into forbidden systems. Last year, one such bulletin board carried detailed instructions for getting into a key computer system operated by Pacific Telephone & Telegraph Co. in Los Angeles.

"TAP," an underground newsletter will

a mailing address on 42nd Street in New York, also offers hacking tips. Its March 1983 issue gives the telephone number and other entry details for a Princeton University computer. It also tells how to get free credits on certain arcade video games including Pac-Man, using none-too-subtle methods, such as smacking the machines. TAP got started in 1971 to help "phone phreaks" crack phone-company security. But computer hacking is "getting to be more and more" a part of the publication, says an editor who calls himself Cheshire Catalyst.

"If people have the hardware and the general expertise and they've somehow connected with this gray market, all they lack is the motivation," says Doug DeVries, the manager of computer security at Hewlett-Packard Co.'s corporate data center.

To patch into other people's computers, some hackers use such high-technology techniques as looking over the shoulder of a legitimate user to get his password, or rummaging in a company's trash barrels for computer printouts bearing valuable access codes, a tactic called "trashing." "You'd be surprised what you can find in the trash bins," says Mr. Garrott, the deputy district attorney.

Guessing the Password

Computer passwords, which let you into particular accounts, are often easy to guess. They tend to be wives' names, dogs' names, first names and birthdays. Some computers come with standard passwords, which their owners neglect to change. A common one is "SYSLIB," for system library.

"It isn't hard to get lucky," says Michael Chastain, 20, a senior at the University of California at Berkeley, studying math and computer science.

He got lucky when he was 15. A friend gave him a password to an account on a Berkeley computer. "It happened at the right time. "All I wanted to do in life was get access to one of the university's systems. Once I got it, all I wanted to do was beat the Adventure game," in which the player electronically seeks treasure in a cave. "Then all I wanted to do was beat their security." He did, illicitly gaining "super-user" status—computer privileges typically only given to a few key staff members. He didn't go any further. "I turned myself in," he says. "I didn't want to go on to bigger and better security violations and get caught doing something serious."

Die-hard hackers say there isn't any harm in any of this, provided data never get destroyed and no one gets hurt. The malicious hackers, says MIT's Mr. Stallman, may simply be rebelling against antisocial "fascist" computers that seek to keep users out. "I call him a person who has been alienated by the hostile atmosphere he perceives in most computer systems," he says. "He reacts to it with anger, which is perfectly justifiable, in my opinion."

Occasionally, a hacker goes on to do obvious damage, as in the U.S. Leasing case. Profanity was sprinkled throughout its system. Important inventory files, which allowed a leasing subsidiary to keep track of its equipment, were destroyed. And the company spent thousands of dollars restoring the computer to operation.

The culprit was Lewis De Payne, who went by the code name "Roscoe." He led a kind of computer-access gang in Los Angeles that included a woman and a couple of youngsters. With the help of telephone officials, police captured Mr. De Payne, who pleaded no contest in Los Angeles municipal court to reduced charges of computer fraud and conspiracy to commit computer fraud. He spent about six months in the county jail.

To get the computer's phone number and a key password, Mr. De Payne used a terribly sophisticated technique: He asked for them. Posing as a software trouble-shooter, he called the company and said he needed to do some program maintenance over the phone. His repair was supposed to correct a problem that other computers had, in fact, been having. An unsuspecting computer operator gave Mr. De Payne what he wanted.

Although Mr. De Payne won't discuss the case, he says: "You can basically extract any information from a person if they're ignorant of what that can do." Improperly trained people, he says, "are the weakest link."

Mr. De Payne continued the ruse and made the repair. When it didn't work, U.S. Leasing called the local offices of the computer manufacturer and learned the firm had no such employee. U.S. Leasing immediately ordered its legitimate users to change their passwords. Some didn't, leaving an open window for Mr. De Payne.

Early the next morning, the computer left messages that would make a sailor blush, such as: "I just wanted to tell you to go take a flying (obscenity)."

"At that point, we knew we had a very serious problem," says John Whipple, the company's vice president for data-processing services.

The company quickly sealed its computers from outside access. It wasn't worried about the lost data because it had complete backup tapes. Its main fear was that somehow the intruders had devised a program that would let them back into the machine even after all the passwords had been changed. That kind of software sleight of hand is called a "trap door." U.S. Leasing spent about 24 hours of valuable computer and staff time reconstructing its files, Mr. Whipple says.

Why had Mr. De Payne done it? In the court records, a written statement by his psychiatrist says in part: "He wanted to demonstrate that he had a profound knowledge of computers and their functions." In Mr. De Payne's own statement, he says: "It gave us a sense of pride to be able to show each other that we could 'crack the security' of the computer"

Playing the Game

For some hackers, security means only challenge. "It's as if you're playing a game," says MIT's Mr. Stallman. "When they (security people) start playing that game, they shouldn't be surprised when other people play the other side."

Partly as a result, companies are about as willing to talk about the specifics of computer security as families are to discuss incest. They don't want to throw down a challenge for some wise guy. They don't want stockholders or bankers to know that some kid busted into their files. SKK Inc., of Rosemont, Ill., one of a growing number of companies selling computer-security products, plays to this fear in a brochure for its ACF2 software-protection package: "When some sharpie makes a fool out of your computer . . . whose face appears on the news?"

But no system can ever be fully secure, security experts say. SRI's Donn Parker likes to quote "Jackson's Law": "With a big enough hammer, you can break anything." Steven E. Weiland, the principal research manager for the Center for Bank Data Security in Rolling Meadows, Ill., says, "If someone really wants to get in, they get in."

Which can give you a nightmare. Consider "WarGames," an MGM/UA Entertainment Co. film to be released in June. Here's the plot: A kid likes to tap into the computers of a video-game maker so he can play the games before they hit the market. One day he unwittingly patches into a Defense Department doomsday computer and starts the world on its way to World War III, all the while thinking he is playing some neat new game.

We won't say how the movie ends.

Crime on a chip

Beware the logic bombs, data diddlers and hackers

BY MURIEL DOBBIN
© 1983, Baltimore Sun

LOS ANGELES — Logic bombs, data diddling, obscene messages and illegal access to defense secrets are just the tip of a computer crime iceberg that federal and California officials are working full time to control.

Already established in the annals of computer crime are the Phantom, who cost a San Francisco corporation \$250,000 by feeding obscene messages into its machines, a teen-ager who acquired computer access to secret Defense Department information, and Cap'n Crunch, one of the original "phone phreaks" from whom today's electronic pirates are descended.

"The magnitude of the problem of computer vulnerability is only now being realized. What we are seeing is the tip of a nasty iceberg," said Clifton Garrott, an assistant district attorney who heads the electronics crime division in Los Angeles.

The U.S. Justice Department has commissioned a team of electronics experts at Stanford Research International, a California foundation, to carry out a study of computer crime in 18 states.

Rep. Ronald Wyden, D-Ore., introduced this month a computer crime prevention bill, said to be the first of its kind, as an initial step to combating the problem.

The Wyden bill would set up a task force to assess the dimensions of computer crime nationally. It also would create a clearing house to provide guidelines and aid for small businesses that are especially sensitive to computer criminals.

Charles Wood, management systems consultant at Stanford Research International, pointed to the timeliness of the movie *WarGames*, in which a teen-ager accidentally keys into a Pentagon computer and puts the world on nuclear alert.

"It is conceivable," he said. "The question is whether it is reasonably possible."

Garrott, who in three years of heading California computer crime-fighters has seen such offenses rise sharply, recalled that it was a teen-age boy who was reported recently to have used a computer at the University of Southern California to gain access to a Defense Department system. The extent of the youth's success, said Garrott, had not been established because nobody at the Pentagon would talk about it.

"What we must remember," said Garrott, "is that a computer is no more than an electronic filing system, which will do what anyone tells it to do."

A so-called intelligent computer, which could draw on its own experience when dealing with different sets of facts, is still at least seven years away, according to Garrott.

Meanwhile, he said, not only corporations but people have to learn to cope with the growing threat of computer abuse.

"Our credit ratings, our taxes, our bank accounts, our telephone bills are all to be found on computers, and there is evidence

that increasing access is being gained to credit bureau machines where ratings are listed. New personalities can be built over existing ones, but it is the real person who gets the bill," he said.

He classified hackers, as computer criminals are called, as the successors of phone phreaks such as Cap'n Crunch, who used to use a device called the "blue box" to make long-distance calls without paying for them.

Hackers, he said, are "brilliant in a very limited way. They are not sociable. They flunk out of school and they can communicate only through the world of electronics," he said.

They are people like Lewis DePayne, whose computer name was "Roscoe" or "the Phantom." He led a criminal computer gang in Los Angeles that included two teen-age boys and a woman known as "Susan Thunder."

"Susan Thunder loved computers so much that she would prostitute herself to get money to buy computer equipment," said Garrott.

DePayne eventually spent five months in jail for computer fraud after he had planted obscenities in the computers of a California company.

An even darker side of computer abuse was uncovered at a hospital, where it was found that hackers had gained access to the computerized records of patients in intensive care and had doubled the dosage of their medications.

"If a nurse had not noticed the difference, we could have been dealing with a case of mass murder," Garrott said.

What worries the computer crime fighters is that such offenses often are discovered by accident.

"It's too often a fluke that it's found out at all," Garrott said.

He told of the bank employee who decided use a computer to triple the withholding for state and federal taxes of the bank staff and apply for the refund to be

paid to himself. He was unsuccessful only because an auditor wondered if the withholding was too high and investigated.

There was also the case of Sarah the bank teller who programmed the bank computer to pay her unearned overtime and was successful for months until it occurred to a bank official that an enormous amount of overtime was being paid to a low-level employee.

What was significant about the case of Sarah was that after she had made restitution of the money, she was not fired. She was given a better job at a higher salary on the condition that she told nobody how she had diddled the data.

"That attitude on the part of corporations is passing," said Garrott, who explained that it originally stemmed from reluctance on the part of many firms to admit their own management inefficiency. "It does point up the need for new and tougher computer safeguards," he emphasized.

But until computer precautions are improved, he said, there will continue to be cases where data is changed or "diddled," and corporations risk financial disaster as a result of the planting of "logic bombs" which result in a computer erasing all the information in its records on a given time and date.

"The trouble is that people think computer crime is funny when it can be both disastrous and tragic," Garrott said.

Yet even the official admitted computer crime can be funny. As in the classic case of the cookie monster in the computer. That took place in San Francisco, where interference by hackers led to repeated interruption of a firm's programming with the word "cookie" appearing on the screen.

It would wind up with "gimme cookie." And it turned out that the only way to appease the electronic monster was to "feed" it by typing in the word it wanted, which was "cookie."

Criminal Use Of Computers Seen Growing

By ROBERT E. TAYLOR

Staff Reporter of THE WALL STREET JOURNAL

WASHINGTON — Richard Shanklin has found another use for the versatile home computer: credit-card fraud.

From his parents' home in Fairfax, Va., the 30-year-old Mr. Shanklin used his computer to get into the files of Credit Bureau Inc. in Atlanta. Authorities say he used information about other people's credit-card accounts to order about \$50,000 worth of computer and electronic gear from mail-order businesses.

A grand jury indicted Mr. Shanklin on 15 charges. After plea bargaining, the prosecutors dropped all but one charge of credit-card fraud. Mr. Shanklin pleaded guilty, and he faces a jail term.

The ease with which he gained access to the files is alarming to Assistant U.S. Attorney Lren Hershey, who prosecuted the case. He calls the home computer "the burglary tool of the electronic age." Several computer experts consider that an exaggeration, saying they haven't heard of another case like Mr. Shanklin's. But while computer pranks gain far more attention, experts expect the use of home computers in fraud and similar criminal activity to grow.

"The rip-offs are likely to be more frequent and larger," says Arthur Gillis, a computer-security specialist who is president of Computer Based Solutions Inc. of Atlanta. "The numbers are against us," he says, because people are learning about computers faster than adequate security precautions are being developed.

Danger From Insiders

The most serious threats of misuse, most experts say, come not from outsiders, but from insiders. Most computer thefts are embezzlements. In one case, a consultant, Stanley Mark Rifkin, used computer codes to transfer \$10.2 million from the Security Pacific Bank of Los Angeles to his account in Switzerland. He served three years in jail.

Computer buffs have shown that they can use their wits, their terminals and their telephone lines to gain unauthorized access to private data banks. The most dramatic examples have been carried out by a group of youths in Milwaukee who call themselves the 414's, after the city's telephone area code.

They have penetrated dozens of computer systems, including a data base at the U.S. nuclear-weapons research laboratory in Los Alamos, N.M., and the radiation-therapy records at Memorial Sloan-Kettering Cancer Center in New York.

While computer intrusions are generally ascribed to sport rather than greed, the case of Mr. Shanklin shows the possibilities of financial gain.

Computers' Weak Point

Mr. Shanklin apparently broke into the computer data bank by exploiting a weak point common to most systems: human carelessness. Federal authorities believe he posed as a Credit Bureau employee to obtain from a J.C. Penney clerk the codes used to enter the computer's credit files.

Dan P. Miller, a vice president at the Credit Bureau's Maryland subsidiary, says anyone who gets inside the computer's data base can read the company's files on about 90 million people from 24 states—including their credit account numbers, credit histories and unused balances.

Authorities say Mr. Shanklin, in ordering electronic gear by telephone, used credit accounts of people who had recently died. Investigators also say he obtained credit histories of Hollywood personalities, including actress Linda Blair. The grand jury charged that Mr. Shanklin obtained credit reports on at least 80 individuals.

When federal investigators went to Mr. Shanklin's home, they say they found seven antennas on the roof. The amount of computer and electronic gear packed into his bedroom was reminiscent, Mr. Hershey says, of the movie-set bedroom of the youth in "WarGames," a movie that raises the specter of a home-computer penetration of the U.S. missile defense system.

Deliveryman Grows Suspicious

According to the government, Mr. Shanklin picked up some of the goods he ordered at a freight depot, but he had other purchases shipped to his home. A United Parcel Service deliveryman grew suspicious, according to the prosecutor, after taking packages for several individuals to the home in a few days and seeing Mr. Shanklin sign for all of them.

Thomas Maloy, the Credit Bureau's director of public relations, says the company has "taken the appropriate steps" to prevent a similar unauthorized foray into its records, but, citing security concerns, he won't explain what they are.

Mr. Gillis, the computer-security expert, says security can be provided in several ways. Software can require a user to give a series of codes before getting access to data. It also can limit the amount of computerized information that is open to each authorized user. The central computer can be linked only to private telephone lines or programmed to give access to only specific computer terminals.

The most sophisticated safeguards identify authorized users by scanning their fingerprints, voiceprints or even the blood vessels in the retinas of their eyes, says Jim Schweitzer, Xerox Corp.'s manager of system security technology.

But such safeguards may be too expensive or cumbersome for some users. A private phone line to a computer is likely to

cost at least \$1,000 a month, Mr. Gillis says; so it isn't practical for most low-volume users.

In the absence of the more sophisticated security measures, Mr. Gillis says, doesn't take a genius" to break in to a data bank. All it takes, he says, is an understanding of how computers work. Computer users can beat the simpler safeguards by trying random variations of codes and passwords until they find the right ones.

But even the best security is vulnerable to human frailty. A common problem, says Mr. Schweitzer, is that authorized users don't safeguard their passwords and access codes. Theode C. Langevin, working in New York brokerage house, used the password assigned to a former colleague at the Federal Reserve Bank to tap into the Federal Reserve's secret money-supply files. Mr. Langevin pleaded guilty and faces a sentence of up to five years and a \$1,000 fine.

Many crimes that rely on computers, though, could have been committed with old-fashioned tactics. Mr. Schweitzer contends, for instance, that Mr. Shanklin could have found enough information in a credit-bureau or department-store trash bin to charge purchases to someone else's credit card.

Audit concludes state computers are vulnerable

By KARIN DAVIES
Daily News reporter

JUNEAU — The state computer system is poorly protected against tampering by unauthorized individuals, a recently released state audit says.

Because the computer security system is inadequate, someone who puts his mind to it could play with state records — including personnel, payroll and permanent fund dividend files, said James Shea, Department of Administration deputy commissioner of information resource management.

The Department of Administration's lack of policies, procedures and standards for computer operations "leaves the system open to errors and inefficiencies," the Legislative Audit Division said.

"In the worst case, the absence of adequate access controls over production files could expose application systems to errors, fraud and sabotage," the audit said.

Anyone with a current state computer account can change, replace or delete backup programs for the central accounting system, the report said.

The department has asked

the legislature for \$280,000 in the 1984-85 budget year to beef up security systems for central state computers in Juneau and Anchorage, Shea said. The money would pay for a security system and two people to maintain it.

Shea said computer tampering has become a concern nationwide as "computer literacy" increases. Recently, a state employee was disciplined for gathering the information that would have allowed him to enter files that were off limits to him.

House Speaker Joe Hayes, R-Anchorage, recently introduced legislation making it a felony to use computers to illegally obtain or alter information, steal money or to defraud or deceive someone.

A better computer security system would cut down on the number of checks and audits of records that the state would have to perform, Shea said.

The department also plans to comply with suggestions that rules for operating the state computer system be written, distributed and enforced, Shea said.

Several other procedural corrections will be made as well, according to a department response to the audit.

Computer meddling leads state to ask for more security

ADW
12/23

The Associated Press

JUNEAU — Allegations that a state employee tampered with a computer in an effort to gain access to the names of permanent fund dividend recipients has prompted officials to request a new, \$240,000 computer security system, a spokeswoman said Thursday.

Frances Rose, a public information officer with the state Department of Administration, said the employee's name would not be released because he was not charged with any crime.

"He was suspended for 15 days, reduced two steps in rank and had his security clearance lifted," she said.

"If he had been successful, I presume he would have been fired straight out."

The employee is accused of trying to "get information he did not need," or the names of permanent fund dividend recipients, she said.

"I guess he thought he would solicit things from people after they got their checks," Rose said.

"This is the first time this kind of thing has happened. ... It's straight out of 'War Games' (a film about computer tampering)."

A system of "passwords" had been used by the state to safeguard computer information, "but I guess it's not foolproof," she said.

"There's a recognized need that we have to beef up our security," she said.

"We have a proposal in the fiscal '85 budget that would fund the installation of a new computer security system.

"The one they have in mind would cost \$240,000 and include creating a data security office and an officer to monitor computer use," Rose said.

Gayle Horetski, an assistant attorney general, said Thursday the case was not referred to the Department of Law so there was no criminal prosecution.

"Computer tampering is something of a gray area and we're working now on legislation that would tighten it up," she said.

