ployment Act program in the State of Rhode Island has been thrown into chaos.

I realize that the Congress assigned to EDA a very difficult administrative chore in requiring a speedy, accurate, and just allocation and distribution of $4 billion in public works funds in a short period of time. I know that EDA personnel have worked long hours to meet this challenge.

The fact remains that as far as the allocations within the State of Rhode Island are concerned, the program has been badly botched. Recurring, very sizable errors have produced not only uncertainty, but a growing distrust of the allocation process by local government officials.

Confidence in the fairness and equity of the allocation process has been seriously undermined.

The Economic Development Administration is well aware that there are serious problems in the allocation of funds within the State of Rhode Island. It is time, indeed it is long past time, that EDA resolved those allocation problems finally, accurately, and equitably.

It is time that EDA explained the allocation process clearly so that every government official in Rhode Island can know with confidence whether his city or town has been given fair treatment.

Until this is done, the intent of the Congress, to combat unemployment and provide jobs through the construction of needed public facilities, will be frustrated.

COMPUTER-RELATED CRIMES

Mr. RIBICOFF. Mr. President, Brandt Allen, D.B.A., is a professor at the Colgate Darden Graduate School of Business Administration at the University of Virginia, Charlottesville. He is a member of the Financial Executives Institute, the American Accounting Association, and the Society for Management Information Systems, and is the author of several articles on computer fraud.

In the May 1977 issue of the Journal of Accountancy, Professor Allen has published a comprehensive article on the nature, types, and scope of computer-related crime. Professor Allen also proposed recommendations for detecting and preventing computer-related crime.

The Senate Governmental Affairs Committee recently completed a year-long investigation of computer-related crimes, their prevention, detection, and prosecution in Federal programs and private industry.

The investigation led to the issuance of a committee staff report, "Computer Security in Federal Programs," dated February 2, 1977.

In addition, with the cosponsorship of Senators JOHN L. MCCLELLAN of Arkansas, CHARLES H. PERCY of Illinois, HENRY M. JACKSON of Washington, LEE METCALF of Montana, EDWARD M. KENNEDY of Massachusetts, STROM THURMOND of South Carolina, ROBERT P. GRIFFIN of Michigan, PETE V. DOMENICI of New Mexico, H. JOHN HEINZ III of Pennsylvania, and JACOB K. JAVITS of New York, I introduced on June 27, 1977, the Federal Computer Systems Protection Act of 1977.

This measure, S. 1766, is to amend title 18, United States Code, to make a crime the use for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

The legislation, which was referred to the Judiciary Committee, would impose heavy prison terms and stiff fines for electronic burglars who use computers and computer technology to steal or manipulate information, financial instruments, and other property.

Many of the issues raised in the Senate Governmental Affairs Committee inquiry are discussed in Professor Allen's article, "The Biggest Computer Frauds: Lessons for CPA's."

Professor Allen's article is well documented and is written in a manner which persons not expert in the computer field can understand.

Mr. President, I ask unanimous consent that Professor Allen's article, and supporting charts, from the May 1977 issue of the Journal of Accountancy be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

THE BIGGEST COMPUTER FRAUDS: LESSONS FOR CPA'S

(By Brandt Allen)

Today no one argues that computers are "fraud-proof" as some did a decade ago, but there is still much disagreement as to what comprises computer fraud, where it begins and how to prevent it. As a result, the activities of accountants and auditors as they relate to computers and computer security systems often lack direction and focus. Because of the increased incidence of computer frauds, auditors can no longer consider them of concern only to law enforcement agencies. Now the entire accounting profession must be alerted to the proliferation of these crimes and must understand how to recognize them and how to inform management of ways to prevent them.

This article analyzes most of the publicly documented computer fraud cases detected to date (see Appendix, page 62) with special emphasis on the major ones. The latter include those that were long running, were difficult to detect, produced large losses and are representative of frequently detected schemes. Through analysis, it has been possible to determine the major control lapses that seem to invite such schemes. Through analysis, we're also able to speculate about the major undetected computer frauds and where they may turn up.

This analysis focuses on 150 major cases that have been publicized, excluding many others where the data was skimpy. For purposes of this article, computer fraud is defined as any defalcation or embezzlement accomplished by tampering with computer programs, data files, operations, equipment or media, and resulting in losses sustained by the organization whose computer system was manipulated. In most instances, this would encompass all activities in the computer department as well as those departments that directly enter or prepare computer input. Excluded are thefts of computerized information, use of computer time for personal gain, alteration of computer records for nonfinancial gain and schemes where the employer was not the victim. These excluded schemes cover instances where the records of credit bureaus, license agencies and property registers were altered to defraud credit grantors and others dependent on these records. Also eliminated are unusual cases like Equity Funding or Computer Payroll and Accounting Services, Inc., where the service bureau owner absconded with the payroll funds of his client companies.

PREVENTION NECESSARY

As will be seen from the analyses of the computer fraud cases subsequently described in this article, such fraud can often be prevented by a tight system of internal control. Later analyses of these cases will show that certain areas of internal control are weak and in need of improvement. As a result, the CPA should give special attention to the following areas:

1. Transaction controls. The most important area for improvement seems to lie in tightening controls over the generation and flow of input transactions. In all the big cases, perpetrators were able to add bogus transactions or to alter others. Computer users need to perfect means to ensure that all transactions are subject to controls and that the controls are tight. Obvious problem areas, such as adjusting entries and error corrections, should be designed to be controlled by persons other than those responsible for the entries.

2. Rigorous audits. Auditors must give increased attention to the causes of inventory losses. It seems clear that many of the disbursement and inventory frauds were conducted in an environment of large, continuing inventory losses. It appears that the growing crime problem has established the expectation of inventory shrink in many organizations. Inventory frauds or disbursement frauds flourish in this climate; not only does it reduce the organization's diligence but it also tends to foster fraud ideas. Where losses run to the hundreds of thousands or even millions of dollars per year, additional inventory controls and investigations are warranted and can probably be cost justified.

3. Improved responsibility reporting. The most effective internal control for the big cases seems to be improved management reporting systems to alert others to possible fraudulent transactions. Buyers should receive recapitulations of orders placed, received, paid and canceled by time period, by vendor and by type of item. Adjustments and corrections should be highlighted in special management reports. All expense entries should be reported to authorizing management in sufficient detail and clarity to enable the executives to spot unauthorized charges.

4. Program controls. In a well-run computer department, neither programs judged to be critical nor those that access critical programs or data collections are accepted for use in the computer center until they have been subject to independent verification. Once so accepted and approved, they are placed in secure file storage and are available for use only according to schedule. At any time, internal audit can verify that the current program version being used is the one approved for use. All program changes must go through the same sequence.

5. File controls. Every computer user must have a file librarian responsible for the security of all critical program and data files. No files should be released to computer operations except as scheduled. Monitors are necessary to ensure that files are used according to the approved schedule and that all deviations are investigated.

6. Place EDP house in order. Even today many computer centers are run on a crisis basis with few controls, poorly designed systems and unaudited and unauditable software. In too many organizations, edit tests and input controls are relaxed when backlogs grow. Program patches are made in desperation with no review or control. In such an environment it would not be surprising to find computer fraud, and such was the situation in the cases in this study. In

48046

one case, the data files and programing systems were in such bad shape that direct file changes were made repeatedly in order to correct errors. This made it easy for the dishonest employee to make certain other "corrections" to effect his scheme without arousing suspicion. In my opinion, the auditor who discovers a chaotic, poorly controlled data center in his review of internal control is in trouble. He can hardly proceed without additional, and sometimes exhaustive, verification, but it is in just such situations that the additional review is so difficult to perform. The auditor can do a great service for his client and for himself by working to reduce the "management by crisis" conditions found in many computer rooms.

TYPE OF SCHEME

The 150 cases were first sorted into categories by type of scheme and victim organization. In examining Figure 1, page 54, we observe that accounting and inventory control fraud involves average losses of $1.3 million, the largest in the corporate category. Schemes based on fraudulent payments account for almost 40 percent of the cases involving corporations. Fraudulent payments to creditors average $324,000 while fraudulent payments to corporate employees average a $139,000 loss per case. Fraudulent payments in corporations are made to employees (payroll), to other individuals (usually pension or insurance claims) or to creditors or suppliers (disbursements). Losses average well over $100,000 per case. Disbursement frauds are the most costly, primarily because they are more difficult to detect and thus continue longer. Disbursement frauds also are more complex and can be understood and planned by only a few in the company, usually members of management.

In banks and savings institutions, the payment frauds are, with one exception, manipulations of withdrawals. Ordinarily, these involve attempts to withdraw funds from inactive or dormant accounts or efforts to prevent the processing of a check by rendering the MICR (magnetic ink character recognition) codes unreadable. By their very nature, these schemes usually are detected quickly by auditing procedures or internal controls. In one typical case, however, where check processing was blocked on a customer account resulting in a $6.8 million loss, a bank officer was in collusion with an officer of the client company and was in a position to hide the discrepancy in the reconciliation of the bank's account with the regional Federal Reserve Bank.

Frauds shown as payments to other individuals for state and local governmental agencies were for welfare payments, unemployment insurance and job corps programs.

In summary, in most types of organizations automated systems that pay money from the organization to suppliers, employees and others are the most troublesome.

All the cases in the accounting inventory control category shown in Figure 1 are based on changes made in accounting and subsidiary records without an immediate change in physical assets or cash payout. Several of the corporate cases had the same pattern: inventory clerks or managers entered fraudulent transactions into computerized inventory systems; this, in effect, deleted items from inventory or assigned responsibility for the items to someone or someplace else. Then items would be stolen, bringing the physical count into line with inventory records. In the bank and savings and loan cases, various schemes were employed. The simplest schemes were thefts from inactive accounts accomplished by transferring funds to accounts of the perpetrators. Several other cases involved crediting perpetrators' accounts while charging the offset to various expense and adjustment accounts. In one case, service charges to customers were overbilled, with the overage flowing into the programer's account.

In cases involving the manipulation of incoming funds, the number of cases and size of losses for corporations were less significant. There are several reasons for this. Most corporations can and do exercise tight control over customer remittances; the process is more easily audited. Payments to a firm are generally made by check and are not easily cashed. Manipulations of receivables or deposits, the so-called "lapping" schemes," require constant attention and manipulation of accounts. These schemes are also risky; the stolen amount is always hidden in the accounts, awaiting detection. In only two cases was there a potential for large losses.

FIGURE 1.—AVERAGE LOSSES IN COMPUTER FRAUDS

[In thousands of dollars]

Type of fraud	Corporation	Bank/savings and loan	State and local government	Federal Government
Payments to employees	$139(3/8)	$3(1/1)	$14(3/4)	$33(22,29)
Payments to other individuals	133(2,4)		487(6/9)	
Payments to creditors	324(5/5)	[1] 252(8/12)		56(25,30)
Accounting/inventory control	1,300(10/10)	195(12/12)	[2] (—/1)	
Collections/deposits	43(2,6)	157(8/9)		
Billings	6(2,6)			
Miscellaneous	[2] (—/2)		[2] (—/2)	
Average loss totals	621(25,41)	192(27,34)	329(9/16)	45(47,59)

[1] 1 case of $6,600,000 deleted from figures to avoid distortion.
[2] Amount of loss unknown.

Note: The average loss figure is based upon x cases out of y total cases in that category where (x/y) is shown just to the right of the average. Losses in some cases were unavailable or were eliminated for other reasons.

FIGURE 2.—THE VICTIMS OF COMPUTER FRAUDS

Method of computer manipulation	Corporation	Bank/savings and loan	State and local government	Federal Government
Transactions added	16	9	9	48
Transactions altered	8	12		
Transactions deleted	3	4		
File changes	5	3	5	
Program changes	6	8		
Improper operation	4		1	
Miscellaneous, unknown	4	1	1	11
Totals	46	37	16	59

Note: Case totals do not add up to 150 because some are classified in more than 1 category.

In each instance, the perpetrators had discovered how to permanently eliminate the receivables from the accounts through unauthorized adjustment of entries. In certain corporate receivables frauds, the billings were manipulated—and reduced—before the basic sales transactions were recorded in the accounts.

The analysis revealed a significant number of deposit frauds in banks, which yielded much higher average losses. The basic scheme is really the same as that for receivables collection in a corporation: deposits intended for one account are pocketed or credited to another; then the former is made good later by diverting another deposit intended for still another account. Also in this category are check-kiting schemes where deposit tickets or records were altered so that uncleared deposits could be immediately withdrawn.

It's probably misleading to draw any conclusions from the fact that corporations had the largest average fraud losses per case, because only the major cases are publicized. No doubt there were many smaller detected computer frauds in corporations that were simply settled by dismissal; it's the bigger cases that are brought to court and thus reported. Banks, on the other hand, probably report a much higher percentage of their fraud cases because they're federally regulated, insured and required to report their losses. As in corporations, possible computer frauds in state and local governments appear to be underreported and the losses understated.

METHODS OF COMPUTER MANIPULATION

Figure 2, this page, and Figure 3, page 56, illustrate how the computer system was manipulated. Several things are clear from these tabulations. Manipulation of transactions is by far the most frequent method: adding unauthorized transactions, such as phony purchase orders and warehouse receipts in the case of disbursement frauds; altering transactions, such as posting deposits or payments on account to some other account; or not processing a transaction at all, such as payments on long term certifications of deposit. Sometimes a combination of methods is used, as in the cases of pension fraud where a termination triggered by a death notice is not processed (transaction deleted) and then an address change (unauthorized transaction added) is used to channel the payments to the schemer.

Schemes involving direct charges to matter files by the use of utility programs or direct terminal entry via file maintenance were found less frequently. In several cases, transactions had to be added or altered in order to accomplish the file change. I classified these schemes as file changes if a one-time, unauthorized transaction resulted in a recurring fraudulent activity, such as the misappropriated pension payments. If an unauthorized transaction had to be added each time a fraudulent activity was triggered, this was classified as a transaction, even though the effect of the transaction was to change a master file.

Direct manipulation of master files can be difficult to prevent because of the difficulty of establishing file maintenance and change controls:

In one case, a programer/systems analyst used his ability to make direct changes to master files to change the price on items he

was purchasing just before the billing run; later he'd return the price to its correct condition. In another, a programer transferred funds from inactive accounts to his own and his associates by using a utility program and by carefully making all switches within a file control block. The change was made between the end of one quarter and the beginning of another, further compounding the auditor's decision problem.

FIGURE 3.—THE SCHEMES USED IN COMPUTER FRAUDS

Method of computer manipulation	Payments to employees and other individuals	Accounting inventory control; disbursements	Billings collections deposits	Miscellaneous
Transactions added or altered	49	49	17	
Transactions deleted	2	3	2	
File changes	6	3	1	2
Program changes	2	7	5	
Improper operation	4	1		
Miscellaneous, unknown	2	11	2	2
Totals	56	69	27	4

Note: Totals do not add up to 150 because some cases are classified in more than 1 category.

Computer frauds caused by program changes or patches have been discovered in only a few cases. This method has been used to hide overdrafts on checking accounts, to accumulate fractional cents on interest calculations, to skip over accounts at billing time in order to inflate service charges and to mispost accounting transactions fraudulently. Computer users appear to be particularly vulnerable to program patches, as can be seen in the following recent case:

A programer at a large savings and loan association attempted what could have been the perfect computer fraud. At this institution, the on line teller terminals accessed only a temporary customer file during the day; after all tellers had balanced out, the day's transactions were posted to the permanent files and the temporary file was then refreshed for the following day's business. This two-file system was used for security reasons and is the preferred approach for advanced, on line systems. The programer had patched the program so that any withdrawals against his personal account, when posted to the permanent file, would be actually charged to an inactive account. On the following day he would remove his withdrawal slip from the documents sent to the computer center from the branches and substitute one drawing on the inactive account. With the program patch removed, it would have been impossible for auditors to discover the perpetrator. Fortunately, the scheme never got off the ground; the programer erred in keying the inactive account number on his first effort. He was caught the next day.

Frauds caused by improper computer operation were almost always payroll frauds, where extra checks were printed or where unauthorized use of computer terminals was employed to enter fraudulent payroll data, thus leading to excessive payments.

UNDETECTED COMPUTER FRAUDS

One cannot help inferring that a significant amount of fraud and embezzlement goes undetected. Since so many cases are uncovered only by chance or because the perpetrator simply gives up or makes a stupid mistake, one may well conclude that most fraud goes undetected. I believe this is true for computer fraud as well. Furthermore, it's possible to determine the most likely undetected cases simply by applying the pattern of non-computer-related frauds to computer users. Other cases appear probable, considering the buying, selling, employment or functional activities of various types of organizations.

First, it should be clear that a large number of undetected computer frauds simply follow the patterns found in these detected cases. Thus, there is much undetected corporate inventory and disbursements fraud, much undetected welfare fraud in federal, state and local government agencies and many undetected funds transfers in banking institutions. Theft from inactive accounts in savings institutions is a good case in point. This scheme was the most frequently reported in this analysis, and yet many more probably go undetected. Officers of such institutions depend heavily on the computer to block attempted withdrawals from dormant accounts, yet this control can easily be circumvented by the computer thief. Long running dormant account thefts can easily be masked by blocking or diverting quarterly statements and then sending adjusted statements in their places. Beyond this, my guesses as to undetected schemes are the following:

1. *Pension frauds.* There were a couple of cases in this study where pension payments were discovered being made in the names of deceased individuals. But the number of pensioners in this country, the number of pension-paying organizations and the ease of the scheme suggest that computerized pension fraud in the United States is a hidden problem of major significance. There are probably thousands of deceased pensioners on computer files whose monthly checks are being diverted to white collar criminals.

2. Inventory and disbursement frauds in state and local governments. Disbursement and inventory frauds were found to be big problems for automated systems in corporations and federal government agencies; the same must be true for state and local governments, but no cases of this type were found in my collection. It seems clear that they weren't included because they haven't been detected, perhaps because auditing of these agencies is not as thorough. When you consider the number of state and local governments in existence, the amount of purchasing they do and the size of their inventories, this must be considered another hidden problem.

3. Insurance claims fraud. From the cases to date it might be concluded that there is no computer-related fraud in insurance companies. This can't be so. The nature of the business in this industry is money collecting, investing and paying; there are many individual accounts, many transactions, a high degree of automation, the dollar magnitude is high and much of the industry depends primarily on good faith—such as medical insurance claims processing. Few industries have such a high potential for computer fraud and so few detected cases to date.

4. Corporate billing frauds. While there were a few detected cases of this type in my collection, the total was surprisingly small considering the vast amount of billing activity in the corporate sphere. The large number of employees who have access to billing transactions and the case of manipulation suggest that much fraud here goes undetected, particularly that effected by deleting, blocking or altering transactions.

5. Federal government program frauds. If the results of this survey can be believed, there have been no dishonest computer programers in the federal government. This hardly seems possible. Considering the potential for abuse in such agencies as the Department of Health, Education and Welfare, the Department of Defense, the Internal Revenue Service and the Agriculture Department and in programs such as revenue sharing, it may be concluded that a significant number of payment frauds generated by unauthorized program patches go undetected in the federal government.

6. Loan frauds in commercial banks. Commercial banks, as opposed to savings institutions, also appear surprisingly clean in the survey. For many reasons, the chances of operating successful funds transfers are lower for demand accounts than for savings accounts, but the opportunities for loan frauds are greater in commercial banks. It seems impossible that computer-assisted loan frauds are not a giant problem for commercial banks. My guess is that many are out there waiting to be detected.

PERPETRATOR'S JOB POSITIONS

Some of the most interesting observations to be made from computer fraud cases come from looking at the job positions of the perpetrators. As shown in Figure 4, this page, there was much collusion, particularly in those cases initiated by data entry personnel. Line 1 of Figure 4 should be read as follows: There were 15 cases involving data entry personnel; 4 of these acted alone; 5 colluded with 1 other employee, 1 colluded with 2 others and 3 with more than 2 employees; 1 colluded with a nonemployee and 5 colluded with at least 3 nonemployees; the average loss per case for those 4 employees working alone was $8,000 and it was $727,000 per case for all cases in this category.

The distinction between data entry/terminal operators and clerk/tellers is essentially that the latter category deals directly with customers, suppliers and others; the former do not.

FIGURE 4.—AVERAGE LOSS, JOB POSITION OF PERPETRATOR, INDIVIDUALS INVOLVED

Job position of primary perpetrator	Total	Inside				Outside			Average loss (thousands)	
		Prepetrator alone	1	2	>2	1	2	>2	Alone	Tota
1. Data entry/terminal operator	15	4	5	1	3	1		5	$8	$727
2. Clerk/teller	16	11	3	1	1	2	1	1	37	58
3. Programer	15	10	4	1		3		1	20	53
4. Officer/manager	21	18		3				1	274	314
5. Computer operator	9	5		2	1		1	1	33	37
6. Other staff	5	4		1					48	92
7. Computer operator	5	3								696
8. Unknown	3									2,400

Note: All but 4 of the Federal Government cases were excluded because of missing information in those case descriptions.

The higher the rank or position of the perpetrator, the less likely is one to find collusion; thus, managers were found to work alone much more often than keypunchers or teller operators. Perhaps this is because the higher the rank, the broader the job responsibilities and the greater the knowledge of company operations and controls. Thus, there is less need to collude for purposes of gathering knowledge or to effect frauds via transaction generation, etc. Also, the higher the rank, the greater the loss. For example, officers and managers, working alone, stole $274,000 on the average, whereas other staff took $43,000 and clerk/tellers $37,000.

Something of a surprise was the fact that the computer specialists were caught taking much less when working alone than were nonspecialists; operators took $23,000, programers averaged $20,000 and data entry personnel only $8,000. It seems that ordinary managers and clerks have learned to use the computer to steal much more readily than have the computer specialists.

The anomaly of the $727,000 average loss per fraud perpetrated by data entry personnel and cohorts is explained by the nature of the cases here. Several were large welfare frauds, one with over $2.5 million of fraudulent payments to bogus recipients, and several others were large inventory frauds. The cases in this category come as close to being "organized crime" situations as any observed in this project. The majority of deceptions by "unknown" perpetrators or outsiders were inventory frauds; one of these apparently involved organized crime.

The perpetrator was considered an "outsider" if he is unknown and could have conducted the scheme without specialized knowledge or access.

For example, an unknown person or group stole over $2 million from New York banks by depositing bogus checks designed so they could never clear the bank's computer. The checks were printed as if they were drawn on a New York bank, but with a California bank's MICR encoding. The checks were ping-ponging back and forth between New York and California well after the normal clearance time; by then, the funds had been withdrawn.

Comparison of the perpetrator's job position with the method used to manipulate the computer system confirms that the majority of the schemes involve employee actions very similar to those of his job position: data entry personnel and tellers manipulated transactions and programers manipulated programs as shown in Figure 5, this page. Management, staff and computer operators engaged in several types of schemes, but the majority involved tampering with input transactions.

Comparison of perpetrator's job position and type of scheme yielded little pattern in the data. All types of employees operated payroll, disbursement and accounting/inventory frauds. About all that can be said from the analysis was that just about anyone could be involved in a fraud scheme.

Figure 6, page 60, suggests differing degrees of control in different types of organizations. Corporate computer frauds were perpetrated by all types of employees from officers to keypunchers. In banks and savings and loan associations, the primary fraud position was one of management; branch managers and teller supervisors were frequently responsible for the crimes. In state and local governments, the primary job position involved data entry; here again, most of these cases were welfare frauds whree bogus recipients or payments were simply added to the transaction flow at the time of computer input.

AN OUNCE OF PREVENTION

Many of the fraud cases cited here could have been prevented by a revision of the company's organizational structure. Employees should be given positions that do not conflict or overlap with the responsibilities of others in the organization. And all employees should be consistently observed and reviewed to prevent opportunities to commit fraud.

Separation of responsibility. Perhaps half the fraud cases summarized in this article would have been impossible had separation of responsibility in data processing been practiced and enforced. In many of these cases, employees who had no responsibility for transactions were still able to generate, tamper with or delete them. Separation of responsibility in a computer environment means separation of the following functions:

1. Input data generation.
2. Input control.
3. Computer operation.
4. Programing and maintenance.
5. Output control.
6. Data, program file control (librarian).

FIGURE 5.—JOB POSITION OF PERPETRATOR, METHOD OF MANIPULATION

Job position	Transactions added	Transactions altered	Transactions deleted	File changes	Program changes	Improper operation	Miscellaneous unknown
1. Data entry/terminal operator	9	4		1			1
2. Clerk/teller	9	6		1			
3. Programer					14		1
4. Officer/manager	8	4	3	1	3	1	1
5. Computer operator	1	4		1		3	
6. Other staff	1		1	1			2
7. Outsider (nonemployee)	3	1					1
8. Unknown		1		2			

Note: All but 4 of the Federal Government cases were excluded because of missing information in those case descriptions.

It is essential that programers not have access to input transactions, real data or program files and that they not operate the computer. Computer operators must not be able to change programs or gain access to data files except according to job scheduling, and they should not be able to enter or change input data. In keeping with time-honored auditing principles, certain responsibilities should be kept separate and controls or checks are necessary to make sure that data is not manipulated as it is generated and processed.

Employee surveillance. Bankers have always tried to monitor the financial situations of their employees—and for good reason. All computer users should realize that all data center employees and particularly those managers and staff who work with the data center should be closely supervised. All systems where employees or associates have personal accounts (banks, insurance companies, brokerage houses, etc.) should be given special attention.

THE BIGGEST DETECTED COMPUTER FRAUDS

From the 150 computer fraud cases included in this survey, 15 were selected and are listed in Figure 7, page 61, as "the biggest." These cases all involved schemes that ran for more than a year, were operated by employees of the victim organization and are typical of the schemes discovered to date. Excluded from this list are half a dozen cases each with losses greater than $1 million. They were not included because they ran less than a year, the victim was not the employer or the fraud methodology was atypical.

The most important observation to be made from these cases is that they are common. None are creatures of the computer; they have all been tried before. Four of the cases were disbursement frauds where bogus vendors, together with the supporting details, were set up and paid. Four cases were of the "fund transfers through the accounts" type, all in financial institutions where the perpetrator's and his accomplices' accounts appeared as liabilities; the others were of different types. Thus, in terms of scheme type, the biggest computer frauds are all old wine in new bottles. The technology may be random access and hexadecimal, but the scheme itself should be as familiar to the auditor as debits and credits.

A surprise is the variety of the job positions of the perpetrators; it appears that big frauds can be conducted from almost any job position but the higher the position of responsibility, the greater the prospects for fraud. The one job position conspicuously absent from the big cases was that of computer programer. Perhaps these people are not as dangerous as had been feared; but it's also possible that the reverse is true. This is a good illustration of the problem of working from detected cases—we have no way of correcting for sample bias. In this situation, we know nothing about currently successful embezzlers. One thing that the perpetrators throughout the biggest cases have in common is that each had a thorough understanding of the functional operation of the computer system. Of the 15 cases, 1 involved a man who had designed and installed the computer system, 4 were conducted by managers of computer departments and all others were frequent users of the system.

One big surprise in this tabulation was that all but one of the cases were effected by manipulation of transactions, mostly by unauthorized transactions being added to the input stream. Another was the paucity of cases detected by ordinary audit—1 case out of 15. Most were uncovered by suspicious associates and employees of related parties, such as banks. Again, this is probably misleading. No doubt many schemes were detected by internal audit or external review or were thwarted by internal controls and were never publicized. Thus, long running schemes must necessarily have escaped ordinary audit.

FIGURE 6.—JOB POSITION OF PERPETRATOR, TYPE OF VICTIM

Job position	Corporation	Bank/savings and loan	State and local government	Federal Government	Total
1. Data entry/terminal operator	6	2	6	1	15
2. Clerk/teller	6	4	3	3	16
3. Programer	7	7	1		15
4. Officer/manager	7	12	2		21
5. Computer operator	3	5	1		9
6. Other staff	4		1		5
7. Outsider (nonemployee)	2	3			5
8. Unknown	2	1			3

Note: All but 4 of the Federal Government cases were excluded because of missing information in those case descriptions.

FIGURE 7.—LONG RUNNING COMPUTER FRAUDS

Case and summary	Amount (thousands)	Time frame (years)	Type of scheme	Computer manipulator	Fraudulent debit	Job position of primary perpetrator	Number of perpetrators inside/outside	Means of detection
1. Accountant at west coast department store set up phony vendors, purchase and vouchers.	$100	1.3	Disbursements	Unauthorized transactions added.	Inventory	Accountant	1/-	Suspicious bank employee.
2. Claims reviewer at insurance company prepared false claims payable to friends in a manner that would be paid automatically by the computer.	128	4	Fraudulent claims paid.	do	Expense	Claims clerk	1/22	Error made by greedy associate.
3. Clerk at storage facility entered false information to computerized inventory system to mask theft of inventory. Shipments then made without billing.	4,000	6	Inventory/billing	Input transactions altered.	Inventory	Computer terminal operator.	1/13	Physical inventory shortage detected in audit.
4. Warehouse employees manipulated computerized inventory system through unauthorized terminal entries to mask inventory thefts.	200	[illegible]	Inventory	Unauthorized terminal entries.	None (inventory records changed as to location).	Warehouse employee(s).	(1)	Suspicious wife of store manager.
5. Accountant at metal fabricating company padded payroll, thereby extracting funds for own use.	100	[illegible]	Payroll	Unknown	Expense	Accountant	1/-	IRS investigation.
6. Officer of London bank stole funds from inactive customer accounts.	29?	[illegible]	Account transfers	Unauthorized addition and alteration of transactions.	Customer accounts (liability).	Computer liaison officer.	1/-	Unknown.
7. Bank employee misused on line banking system to perpetrate large lapping fraud including unrecorded transactions, altered transactions and unauthorized account transfers.	1,400	[illegible]	Lapping	Transactions altered, added and withheld.	do	Teller supervisor	1/-	Gambling activities uncovered by police raid.
8. Manufacturing company manager who had designed and installed automated accounting system used it to steal.	[illegible]	[illegible]	Disbursements (also lapping fraud).	Transactions altered (also unauthorized transactions).	Inventory (also expense).	Operations manager.	1/1	Suspicious associate.
9. Customer representatives of large public utility, together with outside associate, erased customer receivables using computer error correction codes; received kickback from customer.	[illegible]	[illegible]	Accounts receivable—collections.	Unauthorized transactions.	Expense (adjusting entry).	Customer service representative.	2/1	Suspicious bank employee together with expanded type of scheme.
10. Clerk in department store established phony purchases and vouchers paid to friend's company.	120	[illegible]	Disbursements	do	Inventory	Accounts clerk	1/1	Suspicious associate.
11. Organized crime ring operated check-kiting fraud between two banks using computer room employees who altered deposit memos to record check deposits as available for immediate withdrawal.	900	4	Kiting (float fraud)	Transactions altered.	Timing	VP-computer systems (also assistant branch manager).	2/3	Bank messenger failed to deliver checks on time.
12. Accountant at large wholesaler established phony vendors through computerized accounting system that he operated.	1,000	4	Disbursements	Unauthorized transactions.	Inventory	Controller	1/-	Gave up.
13. Officer of brokerage house misappropriated company funds through computer system that he controlled.	277	3	Account transfers	do	Revenue account (interest earned).	VP-computer system.	1/-	Unknown.
14. Partner at brokerage house transferred funds from firm's accounts to his own.	81	3	do	do	Expense (via adjusting entry).	Partner-head of computer system.	1/-	Do.
15. Director of publishing subsidiary manipulated computer system to add false sales and block recording of accounts payable—all to improve operating results, thereby securing a position on board of directors.	11,500	(2)	Padded sales (also unrecorded expense).	Program alterations (also file changes).	Receivables	Director of subsidiary.	5/-	Do.

[1] Several.
[2] Probable losses much greater.
[3] Several years.

Auditors should be particularly interested in the conclusions about the biggest computer frauds drawn from the column labeled "fraudulent debit." In every accounting-based fraud, a trace or "footprint" of the fraudulent transaction is left in the accounts. In almost every case, it is the debit that should be the focus of internal control or the base of fraud detection. For example, disbursement frauds result in bogus debits to inventory or, in some cases, expense accounts; payroll debits are to expense accounts; and theft from dormant or inactive accounts in banks include fraudulent debits to customer accounts. The key to long running frauds is in the identification of unauthorized debit entries. In the 15 biggest cases, these entries form a definite pattern: 6 were to inventory or receivables, 3 were to expense, 2 were adjusting entries to revenue and 2 were to customer accounts (liabilities). Two involved schemes other than manipulation of accounting entries. These cases became big because these debits were such that detection by management was seriously impaired: inventory shortages were probably considered part of normal shrink, expenses were to those accounts where additional charges wouldn't be easily spotted (payroll, claims expense in an insurance company, interest expense at brokerage houses or revenue adjustments that appeared to be correcting entries). In reviewing automated accounting systems, the auditor would do well to establish a clear idea of the debit entries most likely to be fraudulently used.

CONCLUSION

The first time I assembled a set of computer fraud cases, I was struck by the incompetency of most of the embezzlers who had been discovered.[1] Since the computer provided such a high degree of fraud potential, I wrote at that time, "I can't help wondering what the really clever people are doing" with the computer. I still wonder; I think the biggest computer frauds are still to be revealed.

APPENDIX

Five sources were used to collect cases for this article:

1. Annual reports, magazine articles and newspaper clippings.

[1] Brandt Allen, "Computer Fraud," *Financial Executive*, May 1971, p. 38.

2. Case files of the Stanford Research Institute. Donn B. Parker of the SRI allowed me to examine his case files, which have been established, in part, through research sponsored by the National Science Foundation.

3. Case files of the U.S. General Accounting Office. These cases are described in *Computer-Related Crimes in Federal Programs*, GAO Report FGMSD-76-27, April 27, 1976. Walter Anderson of the GAO's Financial and General Management Studies Division provided further details of these cases short of identifying the agencies and individuals involved.

4. Case files of the Federal Bureau of Investigation. Summaries of closed cases with individual and institutional identification removed were obtained from the FBI.

5. My own files from previous research and consulting projects.

While I am indebted to these organizations and individuals for their cases and assistance, I alone am responsible for the summaries, analyses and speculations contained in this article.

INITIATIVE CONSTITUTIONAL AMENDMENT

Mr. ABOUREZK. Mr. President, on July 11 of this year, Senator HATFIELD and I introduced Senate Joint Resolution 67, a joint resolution proposing a constitutional amendment to allow the use of the initiative process at the national level.

Though 23 States have successfully used the initiative for many years, the idea of a national initiative is fresh and warrants explanation. To make information on the initiative process available across the country, I am working with Initiative America, an organization with representatives in more than half the States. Initiative America has prepared a series of questions and answers which clarify some of the issues involved.

I ask unanimous consent that the question and answer document prepared by Initiative America be printed in the RECORD.

There being no objection, the document was ordered to be printed in the RECORD, as follows:

QUESTIONS AND ANSWERS ON THE NATIONAL INITIATIVE CONSTITUTIONAL AMENDMENT

Q. What is the Initiative Process?

A. The Initiative is the process by which citizens can propose and enact laws independently of the legislative body. Laws are placed on the ballot after citizens collect a required number of signatures. A majority affirmative vote enacts the measure into law, a majority negative vote rejects the measure.

Q. What is a National Initiative?

A. A National Initiative process enables citizens to petition to place federal laws on the national Congressional election ballot every two years. Though not now available federally, a proposed constitutional amendment to provide for a National Initiative was just introduced into the U.S. Senate.

Q. Where is the Initiative now available? When was it established?

A. The right of Initiative is authorized by the constitutions of 23 states: Alaska, Arizona, Arkansas, California, Colorado, Florida, Illinois, Idaho, Maine, Massachusetts, Missouri, Montana, Michigan, Nebraska, Nevada, Ohio, Oklahoma, Oregon, North Dakota, South Dakota, Utah, Washington, and Wyoming.

In addition, the Initiative is presently available in hundreds of municipalities around the country.

Use of the Initiative began in the United States around the turn of the Century, after South Dakota became the first state to adopt the process in 1898. Other states followed South Dakota's lead, with 18 additional states authorizing Initiative in the following 20 years. The origins of Initiative procedures date back to the "plebiscitums" of the ancient Roman Republic, whereby the question of repealing or enacting laws over the opposition of the Senate could be put to a vote of the "plebes"—the enfranchised commoners. Initiative procedures were really pioneered in Switzerland in the years 1631-1891, however, when various forms of the Initiative came into use. Their use is continued on a national basis in the present Swiss Constitution.

Q. Does a National Initiative really require amending the U.S. Constitution?

A. Portions of the existing Constitution lay the foundation for a National Initiative process, but a separate amendment is necessary to provide a specific procedure by which citizens can use this right. The first amendment states that the people have the right to petition the government for redress of grievances, for instance, but the first amendment does not provide a procedure to practically implement this right.

Q. Exactly how will a National Initiative work?

A. Citizens would be allowed a maximum of 18 months to collect signatures of registered voters equal in number to 3 percent of those voting for the office of President at the last Presidential election. Of this total figure, a distribution requirement of at least 3 percent in each of 10 states would apply. The total signature requirement, based on the 1976 Presidential election (81.5 million voting) would equal 2.45 million valid legal signatures. Signatures would be certified within 90 days for their sufficiency by the U.S. Attorney General, and then placed on the next national Congressional election occurring at least 120 days after certification is completed. Initiative proposals could appear every two years at Congressional or Presidential elections.

Q. How does this process work in conjunction with our representative system of government?

A. The Initiative is an integral part of our representative system of government. It is a complement to the present system, because it helps it to operate more accountably and openly. Initiative is simply another check and balance in our political system, except, instead of one branch of government being a check against another, the Initiative is a final check against the institutions to which the people have delegated authority.

Initiative is accepted as another democratic means by which citizens can express themselves. The Initiative has survived the test of nearly 80 years of use in 20 states across the United States. Initiative drives provide feedback to legislators about how the people feel on different issues. Additionally, many Initiatives prompt a public discussion about pertient issues which would otherwise go unaddressed. By providing another communication link with our elected officials, Initiatives bring more citizens into the mainstream of public affairs and bring greater responsiveness on the part of the legislative body.

Any tool such as the Initiative which improves consultation between government and the people is a tool which enhances the effectiveness and openess of our democracy.

Q. Won't the ballot eventually become very complicated by dozens and dozens of issues?

A. The history of state-level use does not indicate that such frequent use of the Initiative has ever occurred. There are built-in safeguards to insure that the Initiative is used for issues with substantial public interest and support. The signature requirement is still enough to prohibit most drives from gaining the legal number of signatures to qualify for the ballot in the first place.

Q. What will prevent the process from being controlled by special interests? Is the Initiative really a citizens tool?

A. Special interests already enjoy an unequal voice in the legislative process through full-time lobbying of the legislature. The Initiative is proposed as a people's check for those times that the legislature is unresponsive to public needs.

The Initiative process has several unique features which make it an effective citizens tool, enabling the people to be heard even when normal legislative channels fail. Initiative gives people the power to get a fair hearing on an issue which concerns them. If there are enough citizens willing to sign petitions to put a question to a public vote, then that issue, at the very least, will be fully debated and addressed in a public way. Even if the issue is lost at the polls, the increased public awareness and education may go a long way toward resolving a question left unaddressed by the legislature.

The Initiative is also a very open process which invites scrutiny by the public, the media, and by community leaders. If special interests use or attempt to unduly influence the Initiative process, the community is aware of it. It is not easy to work behind closed doors when an issue is on the ballot. Of course, appropriate disclosure and other campaign requirements are useful complements to the Initiative process.

State level Initiative use has demonstrated that a measure qualified and campaign for by a private, special interest group cannot succeed at the polls without the active support of community and political leaders.

Q. The Initiative has worked for decades at a state and local level. Will it work equally well at a national level?

A. Initiative will work every bit as effectively at a national level. Early opponents of this process argued that it could not work effectively at a state level, because of the complexity of the issues it could be used to address, the lack of understanding citizens were said to have of complicated state budgets, and the like. However, the best test of the Initiative has come in the state of California, a state with 10 percent of our nation's population and a $14 billion budget. Even with California's traditionally complex social problems, the Initiative has performed well. There is no reason to believe that Initiative will not work equally effectively when applied to national issues.

Q. Why a 3 percent requirement for signature gathering?

A. The signature gathering requirement must be substantial enough so as to discourage frivolous, unsupported drives, yet not so difficult as to preclude use of the process by volunteer, grass-roots efforts. Any percentage over 3 percent would require an effort so large that only well-financed or already formally-organized interest groups could use the Initiative.

The total signature gathering requirement of 3 percent of those voting for the office of President at the last Presidential election equals 2.45 million legal, valid signatures of registered voters, based on voter turnout of 81.5 million in 1976.

Any signature gathering drive must take into consideration an invalidation rate (for non-legal signatures) of anywhere from 33 to 50 percent. The practical goal for a National Initiative signature drive would likely be between four and five million. Anyone who has gathered legal signatures surely realizes the magnitude of such an effort.

Q. Are there safeguards preventing one region of the country from dominating the use of the Initiative?

A. Yes. The proposed amendment requires that, of the total signatures collected, there

END