THE CPA'S RESPONSIBILITY FOR THE PREVENTION AND DETECTION OF COMPUTER FRAUD

by

Charles R. Wagner

A DISSERTATION

Presented to the Faculty of

The Graduate College in the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Doctor of Philosophy

Interdepartmental Area of Business

Under the Supervision of Professor George C. Holdren

Lincoln, Nebraska

May, 1976

TITLE

THE CPA'S RESPONSIBILITY FOR THE PREVENTION

AND DETECTION OF COMPUTER FRAUD

BY

Charles R. Wagner

APPROVED	DATE
George C. Holdren	April 27, 1976
O. J. Anderson	April 27, 1976
Keith Broman	April 27, 1976
William G. Dick	April 27, 1976
Robert H. Raymond	April 27, 1976

SUPERVISORY COMMITTEE

GRADUATE COLLEGE **UNIVERSITY OF NEBRASKA**

ACKNOWLEDGEMENT

Most research utilizes material drawn from numerous sources and this effort was no exception. Though many sources are referenced in this study, it would be virtually impossible to cite all who have contributed in some measure to the completion of this project.

I would like to express my appreciation, in particular, to the following individuals (listed in alphabetical order): Professor Joseph Anderson, Reading Committee Member, University of Nebraska at Lincoln; Dr. Keith Broman, Reading Committee Member, University of Nebraska at Lincoln; Professor James A. Herbert, Creighton University; Dr. George C. Holdren, Chairman of my Doctoral Committee, University of Nebraska at Lincoln; Michael S. Keplinger, National Bureau of Standards; Donn R. Parker, Stanford Research Institute; Rex Roth, Director of Security Control, Aetna Life and Casualty Co.; Mary Jane Ruhl, U. S. Department of Commerce, and, Dr. Marvin W. Wofsey, George Washington University.

I am immensely grateful to my wife, Rutheda, for typing first (through nth) drafts, and to Mrs. Suzie Sybouts for handling and organizing the typing and other machinations necessary to produce the final dissertation copies.

Charles R. Wagner

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

COMPUTER FRAUD: IS IT A PROBLEM?

Computer fraud: Is it a problem? Yes! Some experts believe that the illegal use of computers is the fastest-growing type of white-collar crime, which in total is estimated to now exceed $40 billion annually, and that as much as 85 percent of the computer crime, which is estimated to now exceed $100 million annually, is not reported.[1]

In our free enterprise system, the burden of the economic losses resulting from such business crimes are, for the most part, shifted to the consumer via an increase in the price paid for goods and services. Naturally, computer fraud is punishable under our legal system--but often the victim chooses for one reason or another not to press charges. Obviously, the commission of computer fraud is an expression of behavioral phenomena that may not conform to normative sociological precepts.

For society at large, computer fraud causes economic, legal and/or sociological problems just as does any other identifiable kind of fraud. The more commonly recognized terms to identify other kinds of fraud would probably include: Art fraud, bank fraud, bankruptcy fraud, business fraud, check fraud, consumer fraud, contract fraud, credit card fraud, employee fraud, government fraud, insurance fraud, management fraud, pension fraud, securities fraud, tax fraud, and writer's

---

[1] Based on facts and figures referenced later in this chapter.

fraud. Some of these may also be of the computer fraud variety.

The term itself--computer fraud--may cause a problem as to its meaning as understood by either a "sender" or "receiver" in the typical communication process. As in any of the other kinds of fraud mentioned in the preceding paragraph, the descriptive term is merely a label that attempts to define the fraud by its most readily identifiable and distinguishing characteristic. In most cases, this characteristic entails a unique environment or a class of individuals or the instrument utilized. There is no one definition or even one term that is used universally to cover all incidents of computer fraud.

Computer fraud: Is it a problem for the CPA? Yes! His professional image may be diminished in prestige and stature since it appears that the news media and some "key publics" believe that there is a lack of auditor involvement in the detection of computer fraud.[2] Recently a court decision for the Equity Funding case resulted in the conviction of three CPAs primarily on the basis of "sheer negligence" and "'lack of involvement' in the basic auditing of Equity Funding accounts." Important aspects of this fraud case included mis-use of computer files and reporting of fictitious data on computer output.[3]

---

[2]Based on facts and figures referenced later in this chapter and in Chapter 6.

[3]The Equity Funding case is briefly described in Chapter 2. See Wall Street Journal, May 22, 1975, p. 9, for more complete results of court action noted above.

The auditing profession has established standards that are supposed to define the degree of responsibility that a CPA has for the prevention and detection of fraud. Since the use of a computer by a client may, and often does, constitute a new "encounter" for a CPA on an audit engagement, the CPA must have the ability to "cope with" the changed environment and controls. Inherent in this ability, in the opinion of this author, is the obligation of the CPA to prevent and detect "material" amounts of computer fraud if the client firm's resources have been unable or unwilling to do so.

The initial objectives of this research project were to determine the extent of computer fraud; to ascertain the reasons for its occurrence and how it was discovered in each case; to study each case, if possible, in an effort to uncover weaknesses in auditing procedures; to examine the characteristics of a computer environment and computer fraud in relation to auditing procedures and generally accepted auditing standards; and to re-assess the question of the auditor's degree of responsibility for the prevention and detection of fraud in a computer environment.

In the pursuit of the above objectives, library and periodical research and a survey of potential information sources were conducted. The survey revealed that the Advanced Research Projects Agency (ARPA) of the Department of Defense and the National Science Foundation (NSF) had funded projects which issued in March and November 1973 final reports entitled Threats to Computer Systems and Computer Abuse, respectively. With the results from the survey and from the examination of these reports

the decision was made to modify the objectives of this research.

The reports of the funded computer abuse-threat projects included all known cases of computer fraud up to the publication dates. The questionnaires used to collect data for the ARPA and NSF projects, however, were not designed to capture information items that had been contemplated as necessary in fulfilling the objectives of this author's research. Accordingly, the ARPA and NSF reports did not contain information on the amount of recovery through fidelity bond, liability insurance and/or court-awarded claims; on the CPA's role (if any) in the particular situations; on the weaknesses in internal control; or on the weaknesses in auditing procedures.

Since it was not considered possible to duplicate survey coverage of the participants in the funded projects,[4] this author's research objectives were altered slightly. Emphasis was placed on trying to determine the risk of computer fraud exposure for the CPA and on evaluating the auditing profession's acknowledgement of the computer in terms of auditing standards and accepted responsibility. However, the original, and still the chief, hypothesis of this study is that the CPA has a greater degree of responsibility for the prevention and detection of computer fraud than the auditing profession currently accepts in its expression of auditing standards relating to the subject of fraud.

---

[4]Although personal funds in the amount of (approximately) $2,000 have been expended by this author in the furtherance of this research project, considerably more would have been necessary to reach the levels of funding available to Stanford Research Institute under the ARPA contract and the NSF grant.

In Chapter 1 the developments in accounting, auditing, data processing, computers and communications are briefly traced and related as components of the business and auditing environments. Then the methods of computer fraud as seen by several authorities are enumerated. The losses from employee dishonesty in dollar amounts are considered as a prelude to computer fraud impact in dollars and on the auditing profession.

The primary thrust of Chapter 2 is toward developing an awareness of the extent and diversity of computer fraud cases, which are summarized in Appendix A, and of the problem of collecting information about computer fraud cases. The results of the survey of information resources are summarized here with details in Appendix B. Some excellent suggestions and noteworthy comments from survey respondents are included. Some existing "fraud" reporting systems are noted.

Chapter 3 details the important findings of the literature search. The significant early literature on auditing and EDP is identified as well as references pertinent to a study on computer fraud as contained in the Accountants' Index and Subject Guide to Books in Print 1974.

The material in Chapter 4 is presented in such fashion that definitions and interpretations from the pre-computer era and non-computer sectors form a foundation for development of an understanding of "computer fraud" as it is interpreted today. Legal, layman, and auditor definitions and interpretations of fraud, embezzlement and white-collar crime are developed as a prelude to consideration of computer

fraud terminology in the literature.

The primary purpose of Chapter 5 is to attempt to determine an index of a CPA's exposure to computer fraud. Several parameters--namely, numbers of computers, of terminals, of employees in direct computer occupations, of business firms, of CPA firms, and of computer fraud (abuse) cases in the several industry divisions--are used to illustrate some relationships for the development of a model.

Against a "backdrop" of eras in the auditing evolution, Chapter 6 traces the development of auditing standards and audit objectives. Computer auditing skill levels are examined in the light of knowledge and proficiency considered necessary by some early-on EDP authors as well as by several AICPA task groups. The AICPA position on acceptance of responsibility for the detection of fraud is traced and the public's doubts about that position are noted.

Chapter 7 summarizes the findings of the research effort in terms of the study objectives and hypothesis. The AICPA position in regard to audit standards and EDP expertise is noted. The search for a solution also includes identification of generalized computer audit programs and the details of such a survey in Appendix C and Appendix D, respectively. Conclusions and recommendations based on research results are offered. Essentially, it is deemed necessary for the CPA to enlarge his responsibility for fraud detection with beginning steps involving a computerized information retrieval system and the offering of a separate service for computer fraud detection.

As indicated earlier it will be necessary first to briefly

picture the development of accounting systems, data processing, computer and communications technology, and adaptation of auditing to these changes in the business environment. Current accounting systems stem from developments that have spanned more than five centuries. Historical documents reveal, however, that accountability records were maintained in some fashion--clay tablets, stone, or wood--as early as 2,000 B.C. The coordinate function of auditing also appears to be ancient in origin. There is evidence that audits of records were accomplished as early as nine centuries ago. As one might suspect, accountants and auditors in early times held a common set of skills and knowledge; nearly all auditors served apprenticeships as accountants.

Although it is recognized that great contributions to the development of early accounting systems were made by individuals of diverse background and geographical origin, the single most important accomplishment may well have been the documentation of double-entry bookkeeping by Pacioli in 1494. Throughout these nearly five centuries of use, the basic accounting systems have retained some of the rather simplistic characteristics described by Pacioli. Individual journal or account entries are still defined as either debits or credits. Today, as in yesteryear, the basic accounting equation requires that debits equal credits.

Accounting encompasses every aspect of an entity that can be expressed in terms of money.[5] Thus, all economic events relating to

---

[5]Committee on Terminology, Accounting Terminology Bulletins, Number 1, Review and Resume (New York, N.Y.: American Institute of

assets, liabilities, ownership, revenue and expenses must be recognized and recorded. Accounting data include the debit and credit descriptions of all transactions stemming from the entity's set of economic events. In some cases, accounting data may include quantitative descriptions in terms of physical units of certain entity resources which must be controlled. Maintenance of an accounting system has traditionally entailed recording the accounting data details of the pertinent transactions on business documents or vouchers; journalizing and posting the debit and credit entries to appropriate books of account in accordance with an established account structure and generally accepted accounting principles; and preparing reports which summarize account balances or activity in the format of financial statements (to be furnished) to users.

The auditing function has kept pace with the accounting function. There is still a common ground for accountants and auditors for a set of appropriate skills and knowledge, but each may require some additional set. Today, auditors may enter directly into that field of endeavor. Some auditors use such training as a springboard to higher-level accounting positions. Each of the two functions may provide its own career pathing. Each may be classified as having two major areas of interest.

Accountants, 1953), p. 9. This bulletin notes that "after extensive consultation and careful consideration, the committee in 1941 formulated the following definition: Accounting is the art of recording, classifying, and summarizing in a significant manner and in terms of money, transactions and events which are, in part at least, of a financial character, and interpreting the results thereof," and further notes that "after the passage of more than ten years, this choice of broad but significant language continues to seem wise, and the definition to appear comprehensive as well as succinct."

Accountants may be either the financial or management variety. Auditors may work in either internal or external audit capacities.

Over the years, accountants have added refinements to both the physical and conceptual structures of the basic accounting system, as the volume[6] and variety of transactions increased and as the need for a change in accounting objectives was perceived. Since the turn of the century, developments within the accounting and auditing disciplines have had considerable impact on the thrust of the respective segments. The beginning of "big business" led to the development of the public accounting[7] (auditing) profession. Expansion of business resulted in increased "economic event" activity. Manual methods of handling accounting data were recognized as being inadequate. Ingenuity and technology teamed to provide mechanized and automated equipment suitable for accounting work.

Although it is impossible to include here all critical events in the advance of data handling and processing techniques, some of the

---

[6]For example, for the years indicated transactions for selected items were:

	1940	1955	1970
Checks written	1.2 billon	2.1 billion	7.2 billion
Telephones in use	19.3 million	56.2 million	120.2 million
Airline passengers	3 million	42 million	171 million
NYSE transactions	282.7 million	820.5 million	3.2 billion

Source: Table 3-1, Databanks in a Free Society by Alan F. Westin and Michael A. Baker (New York, N.Y.: Quadrangle/The New York Times Book Co., 1972).

[7]Committee on Terminology, loc. cit. "Public accounting is the practice of this art by one whose services are available to the public for compensation." In this reference, "art" refers to the previously defined "accounting" as set forth in footnote 5.

key inventions and their applications will serve to highlight and illustrate the transition from manual to automated accounting operations In 1914, the Sundstrand 10-key adding machine was produced and the Monroe calculator was invented. In 1936, the U. S. Social Security Administration installed IBM punched card equipment. By 1950, mechanical equipment was being used in all phases of the processing of accounting data. Much of the equipment was keydriven and electric energy was being used to power the larger desk-top equipment items and bookkeeping machines. After 1950, there was a rapid expansion in the use of punched card equipment. In mid-1951, Univac I was installed as the first commercial computer at the U. S. Bureau of Census. In late 1954, the first IBM 650 electronic data processing machine was delivered to a customer.[8]

For the purposes of this study, the time spans and the processing techniques involved are of considerable importance. In combination, these factors highlight the momentum of technological advances. Let us now consider what has happened as a result of the coming of the "machine age" in relation to the handling and recording of accounting data. Today relatively few accounting systems are maintained on a strictly manual ("written-by-hand") basis, whereas in earlier systems manual techniques were utilized exclusively. Accordingly, it is reasonable to say that the change in the techniques of processing accounting data involve the degree to which some form of mechanization or automation equipment

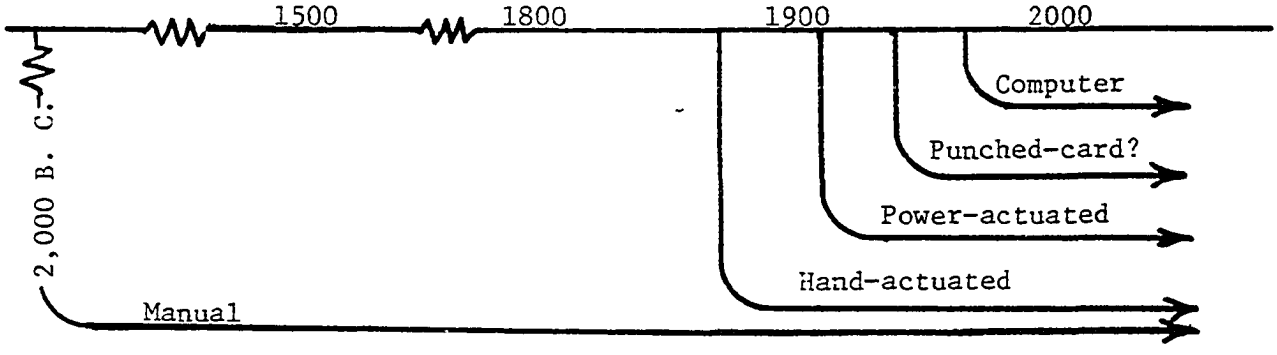
---

[8]"EDP Almanac 1642-1971," Data Management, January, 1972, pp. 26-28.

has been employed. Essentially, the combination of these techniques with the evolving equipment capability can be identified as stages of a continuum. These stages may be appropriately labeled by terms that highlight a distinctive characteristic or feature: manual, hand-actuated, power-actuated, unit record or punched card, and computer. All are still in use today; however, it is anticipated that the punched-card approach will eventually be eliminated.

Since all of these stages and the concomitant procedures should be included in any general description of data processing, it seems advisable here to illustrate (schematically) the momentum of the technological advances affecting accounting data processing.

CONTINUUM OF TECHNIQUES AND EQUIPMENT USED TO PROCESS ACCOUNTING DATA



Today, data processing books seem to proliferate as new (and even some repeat) authors profess to have found a new approach to explaining the subject. Most have in common, however, a statement to the effect that data processing is an activity that is ancient in origin--only the term may be new. A few acknowledge accounting as the antecedent.

Similarity is also found in how the various authors describe the steps involved in data processing. Although even the most casual reader would surely note wide disparity among the authors in respect to the number of steps delineated in describing data processing in detail, the concept and terms are essentially the same throughout all the works. Some authors define data processing as consisting of nine steps; others use as few as three steps.[9] This author believes that all may be generalized into the following: Capturing, conversion, classifying, processing, storing, retrieving, and communicating.

The computer, as a data processing device, is one of the most important technological developments of the twentieth century. In less than three decades, we have seen the field grow from a handful of experimental machines to a point where the manufacture of electronic data processing (EDP) equipment is considered a major industry. In that short time span we have seen at least three generations of computer hardware and computer software as a result of technological breakthroughs.

Though the various data processing authors are not in exact agreement as to the beginning dates and life spans of each generation, there is at least a general concurrence. For the purposes of this study it is important to recognize the major changes in the technological features of each computer generation. Each such technological advance caused a change within one or more of the data processing steps and was

---

[9] Recall that accountants have defined accounting as the "art of recording, classifying, and summarizing . . ." (see footnote 5). Some data processing authors use those same three terms.

thus potentially of significance in applying auditing procedures to those steps. Table 1-1 summarizes the most important features marking the evolutionary process in the development of computers.

TABLE 1-1

EVOLUTION OF COMPUTER TECHNOLOGY

First Generation	Second Generation	Third Generation
	HARDWARE	
Year Introduced: 1951	1959	1964
Type: Special Purpose	General Purpose	Multiprocessor
Electronics: Vacuum Tubes	Transistors	Integrated Circuits
Memory Capacity: 2-4K words	10-20 Million Characters	100+ Billion Characters
Speed: Milliseconds (1/1,000 sec.)	Microseconds (1/1,000,000 sec.)	Nanoseconds (1/1,000,000,000 sec.)
	SOFTWARE	
Year Introduced: 1951	1954	1964
Operations: Instructions	Executives	Systems
Languages: Machine & Assembly	Compiler	Interactive
Files: Sequential	Sequential	Random

TABLE 1-1 (continued)

NOTES: (A) Hardware and software generations do not necessarily coincide. For example, second generation software was not restricted to second generation hardware. This author completed an Assembly Language course in 1958 for the first generation IBM 650, and an Assembly Language course and a Compiler Language course in 1962 for the second generation IBM 7090. Generally, software capability has tended to lag hardware capability.

(B) Some data processing authors claim a third and a half or fourth generation was introduced in 1970, when further circuit miniaturization was achieved and a tie-in between computer and data communications systems became economical. Others believe the fourth generation will be introduced in the 1978-80 time frame, when distributive network systems will become popular.

(C) A few computers were in existence prior to 1950. The first effort to build a computer actually began in 1937.

(D) In EDP parlance "K" equates to 1,000. Since different computers have different word sizes in terms of number of characters, storage capacity is often referred to today in terms of the basic data unit, the character.

Each generation (or stage) of development furthers the proliferation of computers as the increase in "power," the decrease in cost, or a combination of these factors attract more users.

During the decade of the Sixties the growth pattern was fairly consistent within the computer-size classifications of small, medium, and large. These segments consistently accounted for about 14 percent, 83 percent, and three percent of the computer installations. In general, the ranges for these classifications were based on monthly rental costs. Although a variety of scales was used by different

writers, a common one had breakpoints at $5,000, $25,000, and $100,000 per month rentals, respectively.

By the early 1970s, however, computer technology was having an impact on that pattern. Minicomputers had been proved feasible, adaptable and economical--especially when used as a control and/or communications computer. The "minis" earned the name in part from their physical size and in part from the cost aspect--a common definition used a $25,000 purchase price for the basic machine as the upper limit of the mini-size classification.

The growth rate of data communications has been nothing short of phenomenal. The Bell System network has experienced an increase in such traffic of an average of 50 percent each year. It is projecting a tenfold increase in data transmission revenues within the next decade. The Bureau of Labor Statistics Bulletin, 1826, Computer Manpower Outlook (1974 edition) notes, ". . . growth trend in data communications . . . estimated to be 50 percent annually."

Competition seems to be "spurring" the data communications field as the industry widens. Western Union is expanding its offering of data communication services. The Federal Communications Commission has recently given approval for additional common carriers and several companies are already either in operation or under development. Some computer service companies offering time-sharing (T/S) have elected to create their own data networks in a bid to expand clientele in numbers and in geographic distribution. Thus, T/S client users in widely spread cities may use the common, central

computer simply by dialing a "local" telephone number.

Data networks may provide only transmission services or they may be the link to computer data processing. Prior to the 1960s, data communication had been available for many years in the form of teletype. This capability was used primarily for transmitting telegrams and operated chiefly point-to-point via stations connecting intervening line segments between the sending unit and the desination unit. Newer applications involve many different kinds of terminals and usually route transmissions through a "store-and-forward" message switching system. These new systems often use minicomputers to control communications with a large central computer which is used for data processing.

Familiar examples of applications which use large numbers of data terminals and widespread data communications systems are found in airline reservation systems, credit checking systems, and hotel/motel reservation systems. Within these systems, the cathode ray tube (CRT) display and keyboard terminal is probably most common and should be readily identified by the auditor--as a traveler if not as an auditor. However, there is a variety of terminals. Jancura distinguishes three main types of commonly used devices: Document transmission terminals, human-input terminals, and answer-back devices and display. Examples of some common terminals that fall within one or more of these categories are: Paper-tape reader, badge reader, display screen, graph plotter, keyboard, teleprinter, light pen, and Touch-Tone phone.[10]

---

[10]Elise G. Jancura, Audit and Control of Computer Systems (New York, N.Y.: Mason/Charter Publishers, Inc., 1974), p. 243.

Although the field of data communications can be segmented into a number of categories, for the purposes of this study, terminal population is most important. Each terminal provides opportunity for access to magnetically stored data and/or information. Each terminal is a potential entry/exit point for the fraudulent manipulation of data and/or information. Thus, each terminal is a risk unit--just as the input or output device at the central computer is a risk unit.

The typical CPA--a member, partner, or practitioner in either a regional or local firm--since the mid-50s, examined clients' records utilizing traditional auditing functions by following the traditional audit trail so familiar in a manual system. During the 60s, computers, more and more frequently, were being integrated into clients' facilities to become a part of the accounting systems. Still, it was possible to generally audit "around" and thus ignore the computers' effects and to carry on the traditional auditing role in most instances. On some occasions it became necessary to ask a client to modify his computer system in order to provide a "hard-copy" audit trail.

During these years some CPAs at conferences, seminars and even meetings of the local chapter of the state Society had heatedly discussed the merits of auditing "through" or "with" the computer. "Around-the-computer" assumes that if the input data are correct and the output is correct, then the internal program processing must have been accomplished correctly. Sometimes this is interpreted as having the auditor "ignore" the computer. "Through-the-computer" also encompasses the "with-the-computer" approach. These require that the auditor verify

input data as correct and internal program processing as correct. Then the assumption is that output is correct. Obviously, the output may also be verified external to the computer. "Through" requires a test deck that is run through the computer to test desired aspects of the installation's programs. "With" allows the auditor to utilize his own programs or standardized packaged audit programs. The latter is commonly referred to generalized computer audit programs.

Many CPAs--especially those in local and some regional firms--were satisfied to continue working "around" the computer. In the latter, source document input data were visible and could be traced to the printed output data with only some minor manipulations and second-guessing to duplicate what went on inside the computer. Flowcharts are presented on the next page to show in summary form the nature of the "audit around," "audit through," and "audit with" approaches.

A 1965 survey indicated that 39 percent of the staff auditors did not comprehend computer functions and could not read or interpret flowcharts and block diagrams.[11] Even as late as 1968 when there were 63,170 colleagues in the AICPA[12] and over 300 public accounting firms which had installed computers[13] on their premises, a number of CPA

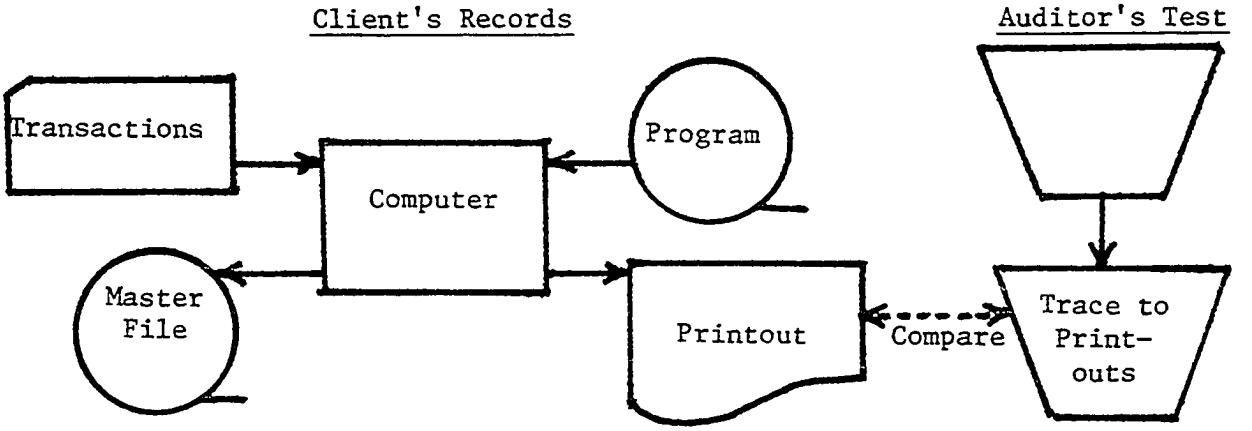
---

[11]Wayne S. Boutell, Auditing with the Computer (Los Angeles, CA.: University of California Press, 1965), pp. 164-169.

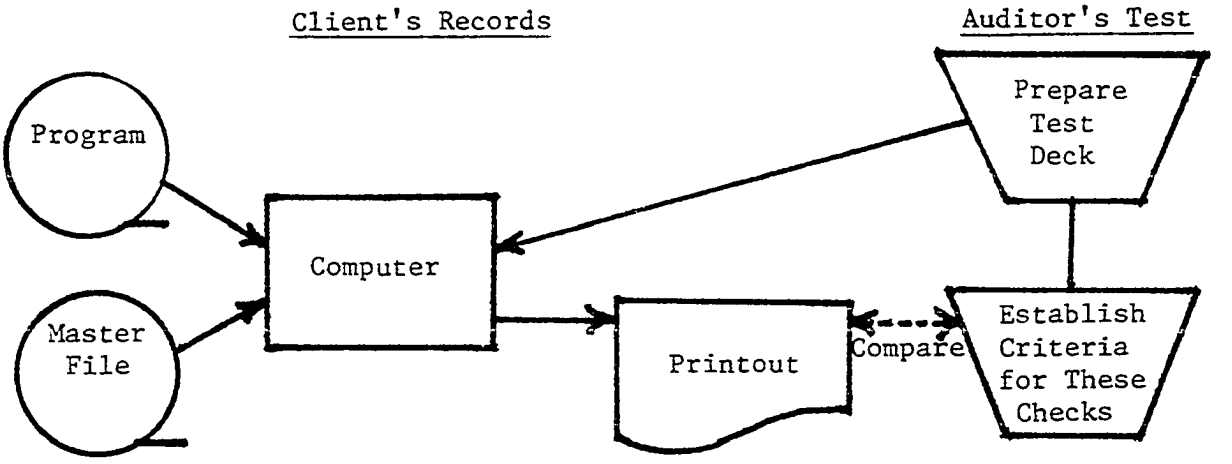
[12]Letter (of welcome) from Marvin L. Stone, President, American Institute of Certified Public Accountants, New York, NY, April 1, 1968.

[13]Jerome Farmer, "Auditing and the Computer--A Suggested Program," Journal of Accountancy, July 1970, p. 54.

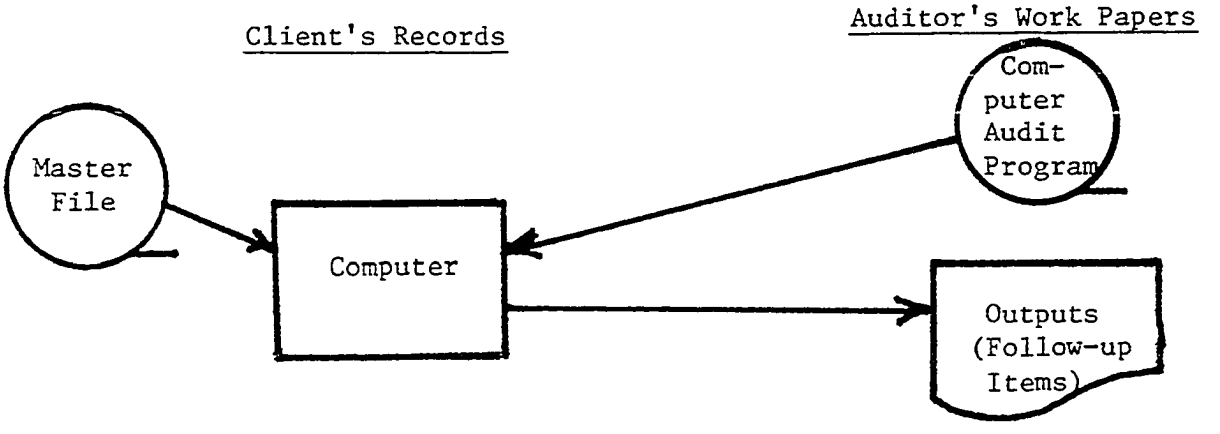
Test of Transactions Around the Computer



Test of Transactions Through the Computer



Analysis of Accounts with the Computer



compatriots avoided, or even resisted, any association with the computer.

From the experiences of the handful of accountants who had worked with the computer and the audit procedure problems it created, some fairly clear patterns of practice emerged. The first problem the auditor encounters is obtaining specially prepared audit programs to deal with the variety of computer audit environments. The chief problem seems to be one of not being able to catch up to the computer. In recent years, especially since late 1967, auditing for the computer environment had advanced quickly in response to those who feel auditing around the computer is inefficient and incomplete, and those who do not know enough about the computer to audit through it. Thus, audit procedures have been developed to alleviate the problem.

Basically most authors have agreed on the approaches that are available for obtaining computer programs for use in the auditing function. Both Horwitz and Webb, writing in 1970 in different articles, delineated essentially similar steps. Horwitz stated that either the client or audit staff may write programs, or purchase may be made of either specialized audit programs, generalized audit programs, or time-sharing services.[14] Webb cited four approaches that have been used in obtaining suitable computer programs for use in the evaluation and testing of records: (1) programs written by the client, (2) programs

---

[14]Geoffrey B. Horwitz, "EDP Auditing--The Coming of Age," Journal of Accountancy, August 1970, pp. 48-56.

written by or under supervision of the auditor, (3) specialized audit programs, and (4) generalized audit programs.[15]

The writing of programs seems to require that the auditor have, or develop, considerable EDP expertise to include evaluation of software, hardware and personnel capabilities. Specialized audit programs do not fit a philosophy for standardization, whereby techniques, procedures and methods may be used repeatedly, and thus provide lower unit costs, and also become well understood. Generalized audit programs are discussed in more detail below.

Time-sharing has become very popular with what might be called general users. In 1971, there were about 100 time-sharing companies in the United States. Time-sharing revenue increased from $10 million in 1965 to $55 million in 1968 and $350 million in 1971. The more than 3,000 public accounting firms buying (in 1968) computer time in some form from computer service facilities were making extensive use of time-sharing.[16] Such utilization was primarily in support of "write-up" work and special assignments for the management services functions. Time-sharing involves the use of a terminal at a monthly rental of about $115 plus other computer use and storage charges.[17] It is often difficult to apply this medium at the client's facility.

---

[15]Richard Webb, "Audassist," Journal of Accountancy, November 1970, pp. 55-56.

[16]Farmer, loc. cit.

[17]Morris B. Kadin and Robert Green, "Computerization in the Medium-Size CPA Firm," Journal of Accountancy, February 1971, p. 47.

The generalized computer audit program subject began to appear about the same time the third generation computer was born--or at least introduced to the EDP buying public. As defined by Horwitz, "a generalized computer audit program is a prewritten program designed to automate part of the audit by providing a selection of optional routines of a given audit situation."[18] If standardized guides, which suggest outlines of procedures to be utilized in audit examinations may be used for preparation of audit programs in a given audit situation, then a generalized computer audit program ought to be useful in performing standard audit procedures.

There seems to be a reasonable consensus--at least as to the number--for the classification of chief kinds of computer fraud machinations. Most authors list four while some list three. Actually, the descriptions by the respective authors are very similar in most instances. Some distinctions may be drawn depending upon whether the author thinks in terms of the accounting environment or in terms of the computer environment.

Although articles by Dr. Brandt Allen, Roy N. Freed, Dennie Van Tassel, and Joseph J. Wasserman are often referenced as pioneer efforts in this field, the first definitive work by an accountant appears to be that of Dr. D. R. Carmichael. He notes that "access to records alone is sufficient for a type of fraud which has been

---

[18] Horwitz, loc. cit.

referred to as manipulation."[19] This is a direct reference to Harvey Cardwell's 1960 monumental effort in regard to audit surveillance principles.

Dr. Carmichael, in the referenced article, is writing for internal auditors but the lessons are equally important for the CPA. His classifications of manipulative computer fraud through access to records include:

> (1) Accounts with employee-defrauders. This category is usually found in brokerage firms and financial institutions. The brokerage firm employee often has a trading account with his employer. Some banks require their employees to bank with them. In a retail firm an employee might have a charge account with the firm.
>
> (2) Accounts with fictitious entities. Either an Account Receivable or Account Payable with a fictitious party could be placed on the records by an employee-defrauder through a legitimate or a fictional transaction.
>
> (3) Accounts with accomplices of employees. An account with a person or business in collusion with an employee-defrauder would be included in this category.
>
> (4) Accounts with third-parties employing accomplices. An account with a legitimate supplier or customer could be used for fradulent purposes if such a business employed an accomplice of an employee-defrauder in a strategic position.

Dr. Carmichael also lists "the following basic methods of fraud in an EDP system":

(1) Console intervention (i.e., control and operation altered)

(2) Irregular program and master file maintenance

---

[19] D. R. Carmichael, "Fraud in EDP Systems," Internal Auditor, May/June 1969, pp. 28-38). (Adapted from a co-authored article published in 1967 in Germany.)

(3) Manipulation of input data.[20]

In a very recent article, another author also notes that "in general there are three methods of committing computer fraud: (1) altering programs, (2) changing master files, and (3) introducing new input."[21] These are virtually the same suggested by Dr. Carmichael, except that technological advances in software for job control and accountability have served to essentially eliminate the problem of console intervention--at least in third generation computer equipment.

In 1972, Belden Menkus, a management consultant noted weaknesses in computer systems and a classification structure for computer fraud.

> Certain features inherent in computer systems operations make it easier to compromise the data being processed. These include: (a) handling data in a form suitable for machine processing but that cannot be read by people; (b) limiting the number of people handling data but expanding their access to it and their ability to influence processing of particular transactions; and (c) eliminating intermediate records and processing summaries, which makes it difficult--if not impractical--to independently examine or verify data processing activities.
>
> Frauds in computerized information systems may be perpetrated in four different ways:
>
> 1. Transactions direct with employees
>
> 2. Transactions falsely entered with non-existent persons or companies
>
> 3. Transactions with employee accomplices in other companies

---

[20] Ibid.

[21] J. Walker Voris, "The Computer and You, How the Computer Can be Used to Commit Fraud," Practical Accountant, March/April 1975, pp. 63-64.

4. Transactions instigated by third parties.[22]

It is interesting to note the similarity to Carmichael's categorization and the recognition of the manipulative character of transactions.

In late 1973, the EDP Analyzer, a well-known trade paper, carried a quite comprehensive article that discussed the problem of computer fraud and embezzlement. It was particularly noteworthy in that the discussion carried the views of a number of individuals all of whom qualify as authorities on the subject. Among these was Professor John Carroll of the University of Western Ontario (Canada). He described four types of conventional frauds that take advantage of the "erasable-storage-media characteristics of the computer." These were:

Valid balance embezzlement (Borrow an asset to produce income)

Improper write-off embezzlement (Eliminate a valid account)

Improper shifting of expenses (Reduce tax or liabilities)

Fraud on the customer (Overbill or overcharge)

The article noted that "auditors that we have talked to have been very reluctant to discuss how frauds and embezzlements took place, on the basis that they did not want to 'train potential embezzlers.'" The other "side of that coin" is that some (a few, many, a majority, most, nearly all?) auditors need to train themselves in the techniques

---

[22]Belden Menkus, "Computerized Information Systems Are Vulnerable to Fraud and Embezzlement," Menkus on Management (Bergenfield, NJ.: Belden Menkus, 1972), pp. 1-4. (Appeared also in January 1973 Retail Control; reprinted in July 1973 CPA Journal; and, reviewed in November 1973 EDPACS.)

of stealing via computer so that they may recognize the characteristics of such actions. The article notes that "in general, cash or mechandise has been stolen through the use of the computer by adding, deleting, altering, substituting, or duplicating records." The conclusion is drawn "that there are many, many techniques for fraud and embezzlement." The most prevalent ones seem to be:

> Manipulation of input data
>
> Manipulation of computer programs
>
> Manipulation of data files
>
> Manipulation of output[23]

Computers may be utilized in both indirect and direct fraud. However, big losses and big problems can occur when direct manipulation of the computer system is made an integral part of the fraud scheme. The manipulation methods noted above in skeleton form have been delineated more fully. In an earlier article, Brandt R. Allen pointed out "four basic approaches may be used, either singly or in combination:

> 1. Manipulation of input data such as basic transaction data, adjustments, etc.
>
> 2. Development of improper computer programs or routines or unauthorized changes to previously audited and approved programs
>
> 3. Alteration of data files or creation of fictitious data files usually maintained on magnetic tape or disk; i.e., master files

---

[23]"Computer Fraud and Embezzlement," EDP Analyzer, September 1973, pp. 1-14.

4. Illegal transmission, interception, or diversion of teleprocessed information[24]

This delineation by Allen may well be a classical one since many researchers writing on the subject use this particular listing as a reference.

It is important to recall that many computer users have access to a combination computer-communications system. Such systems may be of the commercial time-sharing variety or "in-house" installations that provide time-share or real-time processing capabilities. Computer fraud penetration of these types of systems may also be accomplished through one or more of the basic approaches enumerated above. These approaches have been refined and further delineated according to threats of unauthorized entry. Typically these are as described in a following referenced article.

Although the main thrust of the article described ADEPT-50 security, the enumeration of system threats is equally applicable to other time-sharing systems. ADEPT-50 was a medium-scale, general-purpose, resource-sharing system for data management and program production tasks for government and military applications. However, its environment characteristics were much the same as any commercial time-sharing system--remote, multi-user, multi-programmed, multi-filed. Accordingly, the threat types (see Table 1-2) for ADEPT-50

---

[24]Brandt R. Allen, "Computer Fraud," Financial Executive, May 1971, p. 39.

TABLE 1-2

THREAT TYPES OF UNAUTHORIZED ENTRY TO TIME-SHARE SYSTEMS

Accidental Threats

1. Open system trapdoor (loophole) discovered
2. Component failure invalidates a protection safeguard
3. Communication error leaks information improperly
4. Component failure reveals and/or leaves vulnerable critical protection mechanisms

Passive Threats

5. Electromagnetic pickup of system radiations
6. Wire-tapping communication subsystem
7. Exposure of critical system data to unauthorized persons

Active Threat

8. "Browsing" through system files for sensitive data
9. Impersonating authorized user
10. "Between lines" entry (system used when user on but inactive)
11. "Piggy-backing" (intercepting and substituting for original user/system dialog)
12. Corrupt knowledgeable system people
13. Trapdoor entry (probe for unprotected or weak points)
14. Data acquired from residual memory
15. System employed to subvert itself (ferret out own weaknesses)

SOURCE: Table 3 from Clark Weissman article (see footnote 25). Weissman acknowledges use of foundation material from the Proceedings of the 1967 Spring Joint Computer Conference.

are pertinent to other time-share computer systems and do offer access or entry that could be utilized to accomplish some type of computer fraud.[25]

The validity and enduring applicability of the threats in the above table are evident in the repetition by the Chamber of Commerce in a 1974 Handbook on White Collar Crime. Wiretapping, electromagnetic pickup, browsing, between-the-lines entry, piggyback entry and trap door entry are briefly explained as methods "to gain unauthorized outside entry to a computer system that utilizes communication links."

Estimates related to employee dishonesty may be used to gauge the incidence and trend of computer fraud. One source estimated the loss from employee dishonesty in 1937 as being $200 million annually.[26] A 1962 estimate placed the annual financial loss from employee dishonesty as ranging between $500 million and $3 billion.[27] In a 1967 auditing text, Stettler estimated employee theft and embezzlement accounted for about $500 million of business losses per year.[28] In a 1971 edition,

---

[25]Clark Weissman, "Trade-off Considerations in Security System Design," Computers and Management, 2d ed. by Donald H. Sanders (New York, NY: McGraw-Hill Book Company, 1974), pp. 470-481. Reprinted from Data Management, April 1972, pp. 14-19.

[26]Harvey Cardwell, The Principles of Audit Surveillance (Princeton, NJ: D. Van Nostrand Co., Inc., 1960), pp. 25-26.

[27]Mary E. Murphy, Advanced Public Accounting Practice (Homewood, IL: Richard D. Irwin, Inc., 1966), pp. 85-86.

[28]Howard F. Stettler, Systems Based Independent Audits (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1967), p. 389.

Holmes and Overmyer note that estimates of employee frauds approach $6 billion per year.[29]

Brandt R. Allen quotes some interesting facts about fraud from Dun and Bradstreet's "The Failure Record through 1969."

> Conservative estimates place the total corporate loss at one billion dollars per year. Many estimates exceed that figure by a factor of two or three.
>
> Loss through fraud and embezzlement exceeds total corporate losses through robbery, burglary, and shoplifting by a wide margin. And the former is increasing more rapidly than the latter.
>
> Since 1950, over 100 banks failed or were forced to close where fraud was determined to be the primary factor. The number of instances of bank fraud that did not result in failure has not been published, but it is no doubt much greater.
>
> In 1969, over 100 business organizations failed (1.2 percent of total failures) because of fraud on the part of the principals.[30]

About two dozen different current (1971-1975) author's works were reviewed for estimates of employee dishonesty and computer fraud losses. Only two of those sources gave specific estimates for computer fraud--these will be discussed later. Although the range for estimated losses due to employee dishonesty (sometimes referred to as internal theft, or employee theft and embezzlement) extended from as low as $1 billion per year to a high of $16 billion per year, the consensus

---

[29]Arthur W. Holmes and Wayne S. Overmyer, Auditing Principles and Procedure, 7th ed. (Homewood, IL: Richard D. Irwin, Inc., 1971), p. 93.

[30]Brandt R. Allen, "Computer Security," Data Management, January 1972, pp. 18-24.

or modal view placed the amount at approximately $4 billion per year.

Some observations and comments by these various authors elaborated upon the nature and characteristics of such losses and employees involved. It was noted that bonding companies, after a multitude of samplings, had concluded that of bonded employees 25% were honest because they wanted to be, 25% were dishonest in varying degrees, and 50% were only as honest as the system required. One author referred to a Wall Street Journal article in which an expert had estimated that 95% of the dishonesty in any given firm was effectuated by employees who thought of themselves as honest when hired. Another consultant believed there was a 50% chance of substantial dishonesty in any firm. One expert on industrial theft thought that about 5-8% of all workers steal in volume.

Several of these authors noted that about 30% of business failures were the result of employee dishonesty. Two sources made the observation that about 15% of the price paid for goods and services goes to cover the cost of dishonesty. Another noted that less than 1/30 of the known losses due to employee dishonesty are actually recovered.[31]

Such drastic amounts of losses are not unknown. It may be well to recall some recent notable cases of famous-or infamous-fraud.

---

[31]Some of the observations noted in the preceding two paragraphs and in the Allen quotation may also be found in the Chamber of Commerce's Handbook on White Collar Crime, 1974, pp. 4-5.

Billie Sol Estes is believed to have obtained about $22 million through mortgage transactions on non-existent ammonia storage tanks. Tino De Angelis reportedly obtained over $100 million as a result of the salad oil swindles--some authors writing prior to 1973 used that figure as a measure for the potential "big" computer fraud.[32] In an earlier case, Krueger took more than $500 milliion from the company that carried his name.[33]

Of most critical concern perhaps are the trends and projections. While one noted that employee dishonesty had increased threefold in the 1960s, another observed that known employee crime among companies of all sizes was increasing at the rate of 15% per year. Another author was also pessimistic about any improvement and was projecting an increase of 200-300% for employee dishonesty losses during the 1970s.

Employee dishonesty is now ranked by an IBM computer security expert in second place among six categories of computer-related losses. This was an advance from fourth position held in 1972. The Fortune article also noted that computer crime financial losses, with a few notable exceptions, have not been large but do seem to be growing. Of

---

[32]Among these were Haig Neville, "Computer 'Capers' Herald New Crime Wave of Embezzlement," The National Underwriter (Property & Casualty Insurance Edition), August 20, 1971, pp. 1-2, 13. Neville notes that "it has been predicted that within a few years a computer based fraud will be uncovered that may make the 150 million dollar salad oil swindle look small." (He was prophetic; see later citation of the now well-publicized and well-known Equity Funding case.)

[33]Murphy, p. 84.

critical concern are the observations that nearly all cases have been discovered by accident, that one expert feels "only one in one hundred is detected." and that most computer fraud remains undetected.[34]

A common thread seems to permeate most writing about computer fraud. One point in this commonality relates to detection. The following quotations are typical.

> The advantage of fraud by computer is the extreme difficulty of detection. Indeed the recorded instances of computer fraud have almost all come to light only when, for some reason, the system has temporarily reverted to manual processing. What percentage of the total these represent is anyone's guess, but an acknowledged expert in the field put it at less than 20%.[35]

> . . . . Computerized larceny has several advantages over regular old style larceny. Actually, the plain and obvious fact is that computerized larceny is seldom discovered and usually difficult to prosecute even if it is discovered.[36]

> In fact, experts believe that the illegal use of computers now is the fastest-growing type of white-collar crime . . . . Computer-related crime is difficult to detect . . . [and] as much as 85 per cent of such crimes goes unreported. Almost every one of the cases . . . was discovered by accident . . . and because we haven't developed ways to detect unauthorized acts on computers, there are undoubtedly many we just don't know about.[37]

---

[34]Tom Alexander, "Waiting for the Great Computer Rip-off," Fortune, July 1974, pp. 143-150.

[35]Susan Wooldridge, Colin R. Corder, and Claude Rl Johnson, Security Standards for Data Processing (New York, NY: John Wiley & Sons, 1973), p. 6.

[36]Dennis Van Tassel, Computer Security Management (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1972), p. 1.

[37]"Using Computers to Steal--Latest Twist in Crime," U.S. News & World Report, June 18, 1973, pp. 39-40, 42.

> . . . . It is a fact that the use of the computer has enhanced the opportunities to commit fraud and made it far more difficult to detect. Traditional measures for internal control have become ineffective or difficult to accomplish in the computer age.[38]

Another point in the commonality thread prevalent within computer fraud writings concerns the lack of auditor involvement in the detection. The following quotations are typical and, just by their presence, imply that there is a recognized need for some activity to accept a role for the prevention, detection, and investigation of computer fraud.

> If the auditor is not able to use the computer to do the auditing, then he is at quite a disadvantage with an embezzler who will surely use the computer. Increased sophistication and speeds of the computer will tend to favor the embezzler rather than the auditor unless the auditor understands the computer.[39]

> None of the cases . . . was discovered by police or other investigating bodies . . . . One of the most serious problems is that the fields of accounting and law enforcement are not capable of auditing most computer systems.[40]

> In one recent case--unreported in the newspapers--the team consisted of a company accountant, a programmer and an operator. . . . The fraud was a very complicated one based on the subtleties of a change in accounting procedures. Even the company auditors missed it in the annual audit.[41]

---

[38]Milo Gilson, "Computer Assisted Fraud--Who Gets the Axe?" Data Management, April 1975, pp. 22-23.

[39]Van Tassel, p. 51.

[40]"Using Computers to Steal--Latest Twist in Crime," pp. 40,42.

[41]Wooldridge, Corder, and Johnson, p. 83.

> The [security, accuracy and privacy] techniques need to be clearly understood by auditors (but frequently are not) . . . .[42]

In a recent interview with Dr. Carl Hammer, 1973 Computer Sciences Man of the Year and Director of Computer Sciences for Univac, the need for computerization and the fraudulent use of computers--among other subjects--were discussed with Helen M. Milecki, Editor of Data Management. Dr. Hammer said that the reason we need to use so many computers is "the corruption in our society . . . [where] ninety percent of the computers are used to combat a dishonest society--law enforcement, payroll, and mundane areas like inventory because people are always stealing." Dr. Hammer also said that "we need . . . bigger and better models, and tools, to penetrate the systems to find the computer 'crooks.'" He went on to fault the auditing profession by stating that "the majority of CPAs who audit computers are not truly computer professionals . . . [and do not make] an audit of the computer." He also noted that of the AICPA's 85,000 members, "ninety percent know nothing about computers" and that has caused "great problems for the computer community in the business environment.[43]

Two "computerniks"--their own label--have claimed "computer fraud is big business in the United States" and that the take is enormous--"known to be more than $15 million per year." In keeping

---

[42]James Martin, Security, Accuracy, and Privacy in Computer Systems (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1973), pp. 4-5.

[43]Helen M. Milecke, "DPMA's 1973 Computer Sciences Man of the Year," Data Management, June 1973, pp. 14-20.

with the observations noted above these "computerniks" also claim that computer fraud has rarely been detected by auditing or conventional means. "Sheer accident" is the main method of discovery and "since it is impossible to say how many accidents have not yet happened, no one knows how high the annual take really is." The "computerniks" also observe that the "black box" concept has been applied by, and has mesmerized, "business executives, accountants and attorneys into the false sense of security which invites fraud and embezzlement."[44]

The Chamber of Commerce included a classification of "computer-related crime" in the amount of $100,000,000 as part of an estimate of "not less than $40-billion" as the annual cost of "short-term and direct dollar loss" of white collar crime. "Dollar loss per incident" of computer-related crime was noted to have been "as high as $5-million." Separate estimates for embezzlement and pilferage placed these losses at $3 billion and $4 billion per year, respectively. As the references to other authors' writings indicate, the Chamber also presented a critical note on the auditor's role in computer fraud.

> Auditors have little, if any, expertise or background in computer operations. (As a result, they may audit 'around the computer', not 'through' it, and, in effect, miss weak spots that are being exploited.)
>
> Despite repeated warnings to the contrary, too many businessmen still assume that a major purpose of ordinary examinations of financial statements by independent auditors is the detection of fraud . . . . Thus misunderstanding of

---

[44]Stephen W. Leibholz and Louis D. Wilson, User's Guide to Computer Crime, Its Commission, Detection & Prevention (Radnor, PA: Chilton Book Company, 1974), pp. 3, 123.

> the outside auditor's role and/or his under-utilization can leave firms seriously exposed to undetected fraud.[45]

As indicated earlier auditing activity may be performed by two types of auditors. On the one hand the internal auditor is an employee of the firm in which the auditing activity takes place. On the other hand, the CPA is engaged by a firm to accomplish an independent audit. This author believes it would be fair to state that the "traditional school of thought" has held that the internal auditor has primary responsibility for the prevention and detection of fraud.

Reference to substantive authoritative literature on internal auditing indicates that the beliefs of the "traditional school" may not be in accord with the facts. Two works on operational auditing did not even mention fraud.[46] While the above approach may have been true in the past, internal audit objectives and standards in regard to fraud seem to have changed considerably over the last two decades. Brink and Cashin, commonly accorded authoritative status in their writings on internal auditing, have noted these changes. In 1958, they commented as follows:

> An important phase of the conservation of resources has to do with the detection of fraud and dishonesty of all kinds. This is the phase of auditing activity which has

---

[45]Chamber of Commerce, A Handbook on White Collar Crime (Washington, D.C.: Chamber of Commerce of the United States, 1974), pp. 5-6, 20, 24, 61.

[46]See Operational Auditing Handbook by Bradford Cadmus, published by The Institute of Internal Auditors, 1964; and, Operations Auditing by Roy A. Lindberg and Theodore Cohn, published by American Management Association, Inc., 1972.

> ordinarily been given the widest recognition. It is without question an important objective and responsibility of all auditors and, therefore, also of the internal auditor . . . . Nevertheless, the services in connection with fraud are important, and because of the greater time at the disposal of the internal auditor and his greater familiarity with company operations, the responsibilities of internal auditing activity for fraud prevention and detection are in many respects greater than those of the outside auditor.
>
> The emphasis of internal auditing, in any event, should be on prevention rather than on detection of fraud . . . . The internal auditor's efforts are thus not directed primarily at fraud detection but, instead, at seeing to it that proper routines and procedures exist and are functioning to prevent the development of fraudulent actions . . . .[47]

In 1973, they commented on the observed changes in the accepted role of the internal auditor.

> In the earlier days of internal auditing one of the primary roles of the internal auditor was to accomplish the detection of fraud to the maximum extent practicable . . . . The more general view today is that the internal auditor's interest is in fraud prevention rather than fraud detection . . . . And the current view goes still further in the position that fraud prevention itself is only one of a number of operational objectives to be achieved, and not necessarily the most important of these objectives. Thus fraud prevention will be balanced against the cost of controls that are necessary to prevent fraud completely . . . . Fortunately, in most situations the measures that are taken for normal operational control purposes at the same time cover the possibility of fraud . . . . Having put the internal auditor's concern with fraud prevention in proper perspective, it is still true that the internal auditor is interested in fraud, and particularly in actual fraud developments . . . . This broader approach, however, does not deny the fact that the internal auditor has certain basic responsibilities

---

[47] Victor Z. Brink and James A. Cashin, Internal Auditing, 2d ed. (New York, NY: The Ronald Press Company, 1958), pp. 14-15.

> in this area . . . [but] the point has previously been made that the detection of defalcations is not a primary objective of the internal auditor.[48]

In a recent book, Lawrence B. Sawyer, sometimes acclaimed as the "father" of internal auditing, stresses the practice of modern internal auditing in contrast to classical compliance auditing. His remarks on fraud are somewhat of a study in contrast. In one sentence he clearly and unequivocally states, "The auditor has no responsibility for detecting fraudulent acts." Two sentences later he modifies his view by stating that "while the auditor cannot reasonably be considered to be an insurer against fraud, his examinations should be made with due professional skill and care." In devoting about two and a half more pages to fraud, he provides two exhibits--one is "a list of signals that point toward the possibility of embezzlement" while the other is "a list of common forms of fraud." Sawyer also has a chapter on computer auditing but in it discusses fraud briefly and only in respect to prevention via established controls.[49]

So long as our society subscribes to the precepts encompassing property ownership rights, internal auditors have a moral obligation to both prevent and detect (computer) fraud in fulfilling their responsibilities under the employee-employer relationship. In large

---

[48]Victor Z. Brink, James A. Cashin, and Herbert Witt, Modern Internal Auditing, 3rd ed. (New York, NY: The Ronald Press Company, 1973), pp. 19, 356-357, 703.

[49]Lawrence B. Sawyer, The Practice of Modern Internal Auditing (Orlando, FL: The Institute of Internal Auditors, Inc., 1973), pp. 120-123, 216-273.

part, however, society cannot rely upon internal auditors to "keep everyone honest." Although many companies with over 1,000 employees, most stock-exchange-listed publicly held companies (presumed to number between 8,000 and 10,000 firms), and most urban banks have internal auditors, the total in this segment of the auditing profession is just over 100,000. Membership in the Institute of Internal Auditors is now approximately 12,000.[50] Perhaps even more important is the lack of EDP expertise among internal auditors. An informal survey was conducted at the Fourth Conference on Computer Audit, Control and Security in an effort "to determine the ratio of EDP auditors to EDP personnel in those firms represented at the meeting." After eliminating extreme or unusual cases, the final statistics covered 85 companies in nine broad industry groupings. These firms reported a total of 218 EDP auditors. For each EDP auditor, there was, on average, a total of 100 EDP personnel of which 49 were engaged in systems analysis and/or programming assignments.[51]

As indicated above, internal auditors are employees of the firm in which the auditing activity takes place. Thus, there is not direct third party reliance upon their work. However, professional standards and ethics, the work ethic itself, and other mores of society do establish parameters that form boundaries for the scope of their

---

[50]Brochure from The Institute of Internal Auditors, Inc., 5500 Diplomat Circle, Orland, FL, 32810.

[51]Donald L. Adams, "EDP Auditors vs EDP Personnel Survey," EDPACS, January 1974, pp. 13-14.

auditing responsibility and for the measurement of their performance therein.

Since the internal auditor does not serve in an attest function but rather as staff personnel or as an extension of management, no further discussion is warranted for the purpose of this study. Of course, it may be necessary to at least note that there is often a special working relationship between internal auditors of the client and the external auditors. In any case, when it comes to expressing an opinion, the ultimate responsibility belongs solely to the CPA.

Interest in computers by AICPA members does not seem to be widespread among the constitutency, if attendance at the annual conferences on computers and information systems is an indicator. Over the last decade, attendance at the said annual conferences has rarely exceeded 300 participants.

Over the last five years the subject matter and format have not varied much. The conferences do seem oriented toward the smaller practice unit and even in that respect to emphasize usage of the computer for management services, tax returns, and "write-up" work rather than in the audit (attest) function.

To the casual observer this could easily lead to several conclusions. Among these would be the opinion that nearly all CPAs are so expert in computers that such conferences are "beneath" their knowledge level (or egos), or the opinion that only a very, very few of the CPAs encounter computers in their work.

As pointed out earlier, computer fraud seems to be growing in

number and size of incidents. The computer mystique seems to be losing ground for at least one group of people within our society. According to the experts, the individuals who engage in computer fraud never had it so good. And, the CPAs have a problem as a result.

CHAPTER 2

COMPUTER FRAUD: SEARCH FOR CASES

In this chapter the primary thrust is toward developing an awareness of the extent and the diversity of interest in computer fraud cases. Although the cases as described in the accompanying Appendix A may appear to be simplistic in nature, oftentimes perpetration of such actions requires extensive and comprehensive knowledge of computer systems and/or procedures. It should also be noted that there are only a very small number of activities or agencies devoted to the documentation and the subsequent dissemination of information about such cases.

The term "cases" does not necessarily refer to litigation in the courts. In fact, for the time being the reader is cautioned to not be too strict in the definition and application of the term "computer fraud cases." Cases should be construed as "occurrences." The fraud cases cited may include fraud or embezzlement, stealing or theft, misappropriation or mis-application, or just plain misuse or abuse of some kind of computer-related property, information or media. Any popular notion of a "computer" is sufficient for now. All of these terms will be defined or described in context more fully later in this paper so that they will be more useful as parameters or boundaries in the discussion of the major topics.

Shortly before formal approval of this author's dissertation proposal for research on "computer crooks," the Equity Funding scandal

was exposed. It was labeled "massive fraud" and the "first great computer fraud in history."[1] Various news media were quick to report the details. The fraud was reported to have involved the creation of approximately $120 million in non-existent assets and of perhaps as much as $2 billion in life insurance policies on non-existent persons.[2] More than 7,000 stockholders would lose at least $114 million, based on the last quoted share price before trading was suspended on the New York Stock Exchange.[3] Investors in other companies, which had specific relationships with Equity Funding, also suffered losses as the stock market "knocked the whole group down 10% to 25%."[4]

Although the Equity Funding story is told elsewhere[5] in even greater detail, the news media did serve to highlight the possibilities of computer fraud quickly and effectively. There was a flurry of articles as the press found leads to computer fraud cases, past and present. Some characteristics of the news media effort are noteworthy

---

[1] Wall Street Journal, April 9, 1973, p. 3; and Computerworld, April 25, 1973, pp. 1, 4.

[2] Wall Street Journal, April 24, 1973, pp. 1, 37, and May 4, 1973, pp. 1, 8.

[3] "Fraud: Conning by Computer," Newsweek, April 23, 1973, pp. 90, 93.

[4] "Weighing the Scandal Factor," Business Week, April 14, 1973, p. 71.

[5] See Raymond L. Dirks and Leonard Gross, The Great Wall Street Scandal (New York, NY: McGraw-Hill Book Company, 1974); Ronald L. Soble and Robert E. Dallos, The Impossible Dream, The Equity Funding Story: The Fraud of the Century (New York, NY: G. P. Putnam's Sons, 1975); and, articles in numerous periodicals.

for the purposes of this study. Often computer fraud cases were--and still are--reported in two or more newspapers and/or magazines. Where this is true for a given case, sometimes the facts, as described in the respective sources, do not coincide. The difference may be great enough that the casual reader might have difficulty in determining that the two sources are describing the same case. Many times no reference is made to an auditor. Thus, one generally cannot ascertain on the basis of the facts presented whether a CPA uncovered the fraud, included coverage and analysis of the fraud in audit working papers, or was even aware of the existence of fraud.

Since preliminary library research shortly before and after the Equity Funding scandal did not reveal any "rich" reference resource--bibliography, reference book, textbook, documentary, or trade or professional publication--for the citation of computer fraud cases, a survey[6] was designed with the objective of attempting to develop the widest possible network of information resources for such material. At the time it was presumed that there was no organized effort or channels of communication for the collection and dissemination of information about computer fraud cases. The following resources were thought to offer the greatest potential for computer fraud case information:

Selected accounting firms
Selected consultants, educators, and researchers

---

[6]See Appendix B for additional details concerning recipients and responses for the survey.

Selected boards of public accountancy
State societies of certified public accountants
Selected business and electronic data processing periodicals
Selected information centers and regulatory agencies
Selected business, commerical, industry, professional, and trade organizations/associations
Selected computer vendors
Selected insurance companies
State officials having supervision of insurance activities

Even though the 35% overall response rate indicated considerable interest in the subject matter, the findings of the survey were, in general, disappointing. It was particularly disheartening to learn that none of the respondent CPA state boards and state societies maintained files of any kind on computer fraud cases. Seventy percent of the respondents overall had no such files. Only seven of 132 respondents--perhaps, this is really good news--had files which included "first-hand (raw) data." One of these was a CPA assigned to help unravel, after the fact, the Equity Funding "fraud" maze. Two were consultants who headed up computer software firms. Another was Donn B. Parker of Stanford Research Institute whose work is used later in this paper. An EDP security consultant, who had actually been a former fraud perpetrator, indicated he would release such information only for a fee.

Among the first-hand (raw) data held by respondents were two apparently new computer fraud cases. Upon receiving notification of these, this author advised the respondents to contact Donn B. Parker.[7]

---

[7]Donn B. Parker was director and primary researcher for the ARPA and NSF computer abuse/threat projects, which were briefly mentioned in Chapter 1. The NSF project was still in progress at the completion of this author's survey, which apparently uncovered new "case" material.

Several respondents were reluctant to release information, which they had available. Only 13 respondents would grant free and open access to computer fraud case files. Although three insurance companies offering surety, fidelity and professional liability coverage responded, none offered free access to relevant records. In fact, one flatly stated without giving any reason that "we cannot assist you in your effort," however, the company suggested "contact with banking institutions."[8]

Several suggestions and other comments were offered by survey respondents. Harold Weiss, Director of Automation Training Center, wrote:

> My own informal polls of hundreds of auditors during the last decade or more of training auditors in computer subjects indicates relatively few true cases of computer-based fraud. Many of the stories which circulated in the field have been apocryphal and cannot be trusted. Most of the actual incidents have been petty rather than large scale although a few of the latter do exist. In most cases there was extremely poor division of duties and no auditing or very poor auditing of the computer function. I do not believe

---

[8]It should be noted here that computer fraud of interest to CPAs does not exist solely within the banking industry. True, there is great concern about the increases in cases and in losses for fraud and embezzlement in all financial institutions. The record shows 2,835 cases and losses of $20.4 million in FY 1964-65; 10,181 cases and losses of $188.7 million in FY 1974-75. Thus, with an increase in cases of about 400%, losses increased about 900%. An official of American Bankers Association "does not believe the increase results from changes within the banking industry and specifically rejects the notion that computerized accounting methods have made embezzlement and other frauds easier to perpetrate. 'A fraud would be committed with or without the computer,' he says." See Business Week, September 8, 1975, p. 30.

> that the existence of computer-based fraud is widespread as yet; however, it will undoubtedly increase. Were computer fraud prevalent, more incidents would have surfaced in almost two decades of extensive computer use by American business. I must admit that some of the public accounting people always intimate that there is a lot that doesn't surface.[9]

Jerome Priest of Computer Resources Corporation wrote of their effort:

> We have been working in the area for seven years now. While we can accept no direct credit for the fact that none of our customers have experienced a fraud based on a computer, we do feel there is a correlation . . . . We are part of an overall audit philosophy representing more effective audit techniques . . . . The knowledge that an auditor is auditing through the computer and the management philosophy demonstrated thereby creates a deterrent.[10]

Brandt R. Allen, Associate Professor of Business Administation, University of Virginia, offered a referral drawing "attention to Donn

---

[9]Letter from Harold Weiss, Director, Automation Training Center, Reston, VA., August 14, 1973. It should be noted that Mr. Weiss was also prophetic in regard to the now well-publicized and well-known Equity Funding case. In a June 1969 article ("The Danger of Total Corporate Amnesia," pp. 63-64, 67-68) in Financial Executive, he foresaw the problems of internal control and of top management collusion:

> Another hazard which has received recent publicity is computer related fraud . . . . We are more vulnerable to computer fraud only when we abandon a prudent approach to internal control . . . .
>
> . . . . Probably the greatest threat of a major disaster from computer fraud ironically stems from top management itself. Elements of high level management can acquire the ingredients necessary to perpetrate a large-scale fraud of this type as well as the means to profit from it personally on a significant scale.

[10]Letter from Jerome Priest, Computer Resources Corporation, Darien, Conn., July 30, 1973.

Parker's work at Stanford Research Institute . . . rather thorough study of some 140 cases."[11]

J. J. Wasserman, President, Computer Audit Systems, added a fairly lengthy note to the questionnaire.

> I believe you will find it very difficult to develop meaningful and accurate data on CAF [computer-assisted fraud]. News media reports are generally very inaccurate, and many cases they do report have nothing to do with using the computer to commit fraud. Donn Parker (Stanford Research Institute) has compiled a list of 40 CAF which he is reviewing to determine their accuracy.[12]

Donn B. Parker, Senior Information Processing Specialist, Stanford Research Institute, noted:

> Currently completing a study on Computer Abuse funded by NSF [National Science Foundation]. Final report to be completed in September 1973. This study is based on two years of research and a data base of 150 reported cases of computer abuse. . . . I suggest that we could benefit greatly from an exchange of information and discussions. I am currently investigating the Equity Funding Insurance Case.[13]

Alan R. Kaplan, Editor of Modern Data, added the following note to his questionnaire:

---

[11]Letter from Brandt R. Allen, Associate Professor of Business Administration, Graduate School of Business Administration, University of Virginia, Charlottsville, VA., July 30, 1973. It should be noted that Dr. Allen has published several articles on the subject of computer security, which included discussion of computer fraud. Some of these articles are referenced elsewhere in this paper.

[12]Questionnaire returned from J. J. Wasserman, President, Computer Audit Systems, East Orange, NJ., July 23, 1973.

[13]Questionnaire returned from Donn B. Parker, Senior Information Processing Specialist, Stanford Research Institute, Menlo Park, CA., July 23, 1973.

> A related area that particularly concerns me is the growth in numbers of companies and consultants that prey on firms anxious to protect themselves against computer fraud. We have observed several cases of opportunistic organizations using "horror stories" with no basis in fact to sell their services and products.[14]

M. B. Woodbury, Deputy Comptroller for Audit Policy, office of the Assistant Secretary of Defense, in a letter wrote in part:

> I made inquiries in the offices of several of the Department of Defense (DoD) audit organizations to ascertain the specific kinds of computer-assisted fraud (CAF) case files they maintain. I was informed that their files are limited primarily to the most publicized cases of computer-assisted fraud.
>
> Normally, if an internal audit in the Department of Defense discloses operations involving suspected fraud or other irregularities, the matter is transferred from the audit organization to an investigative body for thorough investigation and prosecution and other appropriate action. As a result, firsthand data on fraud cases are usually not retained in the audit files. Further, the results of these investigations are not publicized extensively. The circumstances surrounding the Chase Manhattan Bank and Equity Funding computer-assisted fraud cases, however, are generally well-known to many DoD auditors; and these kinds of well-known computer-assisted fraud cases are used in audit training programs to emphasize the need for audit in the ADP environment.

Ken Pollock, Assistant Director, Division of Financial and Management Studies, United States General Accounting Office, noted in part in a letter:

---

[14]Questionnaire returned from Alan R. Kaplan, Editor, Modern Data, Framingham, MA., July 18, 1973.

[15]Letter from M. B. Woodbury, Deputy Comptroller for Audit Policy, Office of the Assistant Secretary of Defense, Washington, D.C., August 16, 1973.

> We are extremely interested in your doctoral dissertation subject. We hope in the near future to embark on a study of this nature ourselves, as we have viewed with concern the developments in this area. Considering the magnitude of Government computer operations and the amounts of Government funds received and disbursed using computerized methods, the reason for our concern is obvious.
>
> At present, we have only some rough files composed of news media reports and these have generally been the well-publicized affairs. I am sure you are aware of Donn Parker's work at SRI. I believe he recently received some sort of Government grant to investigate anti-social problems with computers and that this involves frauds, embezzlements, and destruction of computer systems and records by disgruntled employees.[16]

Michael S. Keplinger, Staff Assistant, Institute for Computer Sciences and Technology, National Bureau of Standards, added a note to his questionnaire:

> I am interested in the legal aspects of computer use and the substantive legal problems associated therewith. To that extent I am interested in the subject of computer-assisted fraud.[17]

John C. Burton, Chief Accountant, Securities and Exchange Commission, wrote at some length but noted in particular:

> We must confess to being somewhat perturbed over the inclusion in the title of your doctoral dissertation subject of the words "The Auditor's Responsibility for Prevention and Detection of Fraud," in the light of paragraphs 110.05 to 110.08 of Statement on Auditing Standards No. 1 (AICPA 1973).

---

[16]Letter from Ken Pollock, Assistant Director, Division of Financial and General Management Studies, Unites Stated General Accounting Office, Washington, D.C., August 13, 1973.

[17]Questionnaire returned from Michael S. Keplinger, Staff Assistant, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C., August 7, 1973.

The only amplification given in support of that position was a quotation from SAS No. 1.

> Paragraph 110.05 emphasizes that ". . . the ordinary examination directed to the expression of an opinion on financial statements is not primarily or specifically designed, and cannot be relied upon, to disclose defalcations and other similar irregularities, although their discovery may result."[18]

Within six months, Mr. Burton's views seem to have changed to some degree. In a speech, he included the following remarks:

> . . . the question of the auditor and fraud is one that has to be attacked this year. The historical posture of the auditor, which seems to be that fraud is not what the CPA is responsible for finding, has to be reconsidered. This is not to say that the auditor should devote his attention to looking for thefts from the petty cash fund, which I think is what the auditor is primarily talking about when he says he is not responsible for fraud. We have seen too many cases of massive management fraud where management has obscured the reality of corporate activity from the auditor. This is something to which the accounting profession has to turn its attention.[19]

Leonard Landsman, Director of Inquiries Department, Legal and Compliance Division, American Stock Exhange Inc., advised in his letter that "computers represent an important element in our surveillance programs, however, up to the present time, we have yet to uncover a

---

[18]Letter from John C. Burton, Chief Accountant, Securities and Exchange Commission, Washington, D.C., July 30, 1973.

[19]John C. Burton, "The SEC and the World of Accounting in 1974," Journal of Accountancy (Statements in Quotes), July 1974, pp. 59-60. (Excerpts from a speech before The Dean's Forum in Los Angeles, California, on January 17, 1974. The author notes that the comments are his own view and do not necessarily represent the SEC's position.)

situation whereby the use of computers served to perpetrate fraudulent activity in an Amex listed security."[20]

James K. Steen, Deputy Director, Financial-Regulatory Branch, Department of Insurance, State of Illinois, wrote with some fervor:

> At the present time in the Illinois Insurance Department this is a subject very close to us. Although we are not conducting any search for computer assisted fraud in insurance companies, nor do we maintain files of cases of computer assisted fraud, we are involved in one of the twentieth century's most vivid examples--Equity Funding Life Insurance Company. I am sure that a study of the Equity Funding Life Insurance Company scandal is a study in itself . . . . I think your subject is one of extreme importance to independent accountants, state and federal regulators, investors and other users of financial statements.[21]

Some responses either referred to or mentioned directly one or more established reporting systems for the collection and dissemination of information about fraud cases. Only the following agencies or activities, however, have formalized systems:

Bank Administration Institute (BAI)
Federal Bureau of Investigation (FBI)
Internal Revenue Service (IRS)
Insurance Security Association (ISA)
National Criminal Justice Information and Statistics Service (NCJISS)
Stanford Research Institute (SRI)

None of these was established with the declared objective of

---

[20]Letter from Leonard Landsman, Director of Inquiries Department, Legal and Compliance Division, American Stock Exchange Inc., New York, NY., July 23, 1973.

[21]Letter from James K. Steen, Deputy Director, Financial-Regulatory Branch, Department of Insurance, State of Illinois, Springfield, August 27, 1973.

being in support of the CPA or any of his professional organizations. As one might expect, the BAI Fraud Bulletins describe cases occurring within a banking environment. The FBI investigates criminal acts of fraud and embezzlement and reports such cases only as statistics within the U.S. Uniform Crime Report. The IRS handles tax fraud investigations and reports only case statistics in the Commissioner's Annual Report. The NCJISS is primarily concerned with the retrieval of statistics and information for all criminal acts, which of course include fraud and embezzlement. The ISA Insurance Fraud Analysis form is used to capture the facts and modus operandi of fraudulent insurance claims.

The SRI studies on computer abuse will provide the "core" material for this dissertation project. The second report contains analyses, discussion and descriptions relevant to the reported 150 computer abuse cases.[22] While not all of these cases are relevant to consideration of the question of the CPA's responsibility for the prevention and detection of fraud, familiarity with them will serve to broaden the CPA's knowledge.

Stanford Research Institute is continuing to build up "a file of information . . . [with] a new case being added about every two weeks."[23]

---

[22]Donn B. Parker, Susan Nycum, and S. Stephen Oura, Computer Abuse, Prepared for The National Science Foundation RANN SNF/RA/S-73-017, under Grant No. GI-37226 (Menlo Park, CA: Stanford Research Institute, 1973). As provided by SRI and NSF agencies, permission is granted to reproduce or quote all or parts of the report with appropriate acknowledgement.

[23]Ibid., p. 25.

In mid-1974 this author attended a conference[24] in which Parker announced that SRI had assembled in excess of 200 computer abuse cases. However, no new report was contemplated in the near future.

Most case reports are garnered from newpaper and trade journal articles, technical papers, legal documents, interviews with involved persons, and responses from audiences attending such presentations. Some are privately reported; often confidentiality is requested and assured.

A typology of computer abuse is being formed at Stanford Research Institute based on the recorded cases that have occurred since 1964. Cases are identified by year of occurrence and by type--vandalism, financial theft, other theft, and unauthorized use of services.[25] Summaries of the computer abuse cases[26] appear in Appendix A of this paper.

A brief chronology of SRI involvement in the development of research in the area of computer abuse is presented in the following paragraphs. This information is excerpted from the SRI Computer Abuse report.

> The project leader of . . . [that] study became aware of computer abuse problems in 1966 while engaged in the development of a code of professional ethics for the Association for Computing Machinery. Subsequent monitoring and reporting of abusive acts associated with computers demonstrated the need for more professional attitudes in the computer field. This gathering of

---

[24] American Institute of Certified Public Accountants Tenth Annual Conference on Computers and Information Systems, Chicago, Illinois, May 6-8, 1974.

[25] Parker et al., Computer Abuse, pp. 5, 26-27.

[26] Ibid., pp. 91-112.

information continued as an avocation until late 1971, when an opportunity arose to report on the growing problem as a part of an NSF funded project at SRI on Criminalistics and the World of the Future, led by Dr. Brian Parker. At that time, business and government were becoming concerned about the vulnerability of their electronic data processing (EDP) activities; further, proposed computer data banks focused attention on the need for confidentiality to protect the right of privacy.

In 1972 an eight-month study of Computer-Related Crime and Data Security was published by SRI's Long Range Planning Service, informing 500 business participants of the nature of the problem and how to control it. Extensive research was started in other organizations to develop methods of controlling access to computer systems and protecting their contents. However, such research was (and still is) mostly based on presumed and potential problems, rather than on accurately documented actual cases of computer abuse.

Also in 1972 Donn B. Parker performed a study on Threats to Multiaccess Computer Systems for the U.S. Atomic Energy Commission at Lawrence Livermore Laboratory, Project RISOS, sponsored by the U.S. Department of Defense Advanced Research Projects Agency . . . .

Late in 1972 a proposal was made to NSF to conduct a broad interdisciplinary study of Computer-Related Crime. The name of the proposed study was changed to Antisocial Use of Computers and, finally, to Computer Abuse, a title that better reflects the interdisciplinary and broad approach of this study. The proposed study was then divided into three major parts: problem existence, assessment, and solution. This report concludes the first part by identifying the computer abuse problem and presenting data showing its existence.

The project was conducted at Stanford Research Institute's Information Science Laboratory under the direction of Donn B. Parker. S. Stephen Oura in the Urban and Social Systems Division brought a sociological perspective to the study and wrote the section . . . on Social Implications of Computer Abuse. Susan Nycum at the Stanford University Law School contributed her legal expertise and wrote the section on Legal Aspects of Computer-Related Crime.

> Four consultants were retained to review and comment on the study: Professor Donald R. Cressey, Department of Sociology at the University of California at Santa Barbara; Professor John Kaplan, Stanford University Law School; Lt. Col. Philip H. Enslow, Jr., U.S. Office of Telecommunications, Executive Office of the President; and Mr. Tom Crockett, Director of Research, International Association of Chiefs of Police.[27]

In addition to being a chronology of research development covering computer abuse cases. the above brief recitation of SRI involvement establishes a most important benchmark in the accumulation of literature on the subject. The four reports prepared from SRI research findings may even constitute a new baseline since the literature on computer fraud cases, as discussed in the next chapter, seems to be widely scattered in the form of articles in many periodical sources.

---

[27] Ibid., pp. 3-4.

CHAPTER 3

COMPUTER FRAUD: SEARCH FOR LITERATURE

One of the methods of prevention and detection of computer fraud entails "keeping current" with the literature on the subject. Individual auditors seldom have an opportunity to observe personally, or to be exposed directly to more than a very limited number of the multiplicity of computer fraud activities that may occur. Thus, adequate and timely reporting of computer fraud cases should be available in the professional journals, collected and analyzed in the more permanent form of books, and subsequently used as teaching material in the college classroom or in other training programs for prospective and practicing auditors.

In another study, this author has indicated that "the 'fraud' expertise level achieved by the typical CPA or internal auditor would seem to depend in a large part upon his actual experience with, and exposure to, fraud cases, and his reading of expository and analytical writings on fraud techniques that he has not encountered."[1] What is true for fraud in general would seem true also for computer fraud.

Some of the problems that have been noted for fraud in general also seem to persist in the area of computer fraud. More than forty years ago, A. P. Richardson observed in a preface to a book on fraud

---

[1]Charles R. Wagner, "Availability of Fraud Literature," (Education) Internal Auditor, November/December, 1973, p. 82.

written primarily for the professional practitioner and the student of accountancy that "there is very little in print upon the details of fraudulent practice in accounts and its prevention or detection . . . ."[2] Computer fraud literature seems limited in auditing coverage and not readily accessible to prospective or practicing CPAs. In 1960 Harvey Cardwell pointed out that the literature on fraud is not available "except by extensive research . . . [but is] . . . contained in miscellaneous passages in the many books on general auditing theory and practice and on internal control, in a surprisingly large number of magazine articles, in brochures published by bonding companies, and in three books."[3] Much the same conditions exist today for computer fraud literature.

Cardwell also observed that the AICPA and Journal of Accountancy had followed for some years "the policy of not publishing case histories of fraud and of not publishing articles on methods of detecting fraud."[4] To the best of the knowledge of this author, neither a declaration nor a denial of the existence of a similar policy for computer fraud cases has been made by either the AICPA or the Journal. An analysis later in this chapter of entries in the Accountants' Index should provide some evidence about the existence of such a policy.

---

[2]George E. Bennett, Fraud, Its Control Through Accounts (New York, NY: The Century Co., 1930), p. vii.

[3]Harvey Cardwell, The Principles of Audit Surveillance (Princeton, NJ: D. Van Nostrand Company, Inc., 1960), pp. 9-10.

[4]Ibid., p. 406.

In 1964, Bruce P. Olson, an Ernst and Ernst partner, addressed a conference audience on auditing and EDP. In regard to then existing literature he noted:

> I might say that there is very little which has been written on the subject of auditing EDP records. To my knowledge, there is only a pamphlet published by the Air Force and one text book. On the other hand, there has been a great deal published on the development of EDP systems and techniques which has driven the methodology of data processing techniques at a hurtling speed.[5]

Also in 1964, T. W. McRae, another author writing "early on" about the computer and accounting notes that "much has been written on the problems arising out of the computer audit . . . [and] the author has collected to date four books and thirty-two articles concerning the audit of EDP systems."[6] In a chapter devoted to discussion of a bibliography of data processing, McRae laments the passing of the magazine Accounting Research, which, in its final issue in October 1958, carried an excellent comprehensive bibliography of data processing. He was also concerned that "the EDP market has been flooded with an assortment of books, pamphlets and magazine articles, many of them of dubious value." The portion of his bibliography on auditing and control carried just three entries, which were:

---

[5]Bruce P. Olson, "Controls and the Audit Trail," Data Processing, Volume VII, Proceedings of the 1964 International Data Processing Conference (New Orleans, LA: Data Processing Management Association, 1964), p. 209.

[6]T. W. McRae, The Impact of Computers on Accounting (London, UK: John Wiley & Sons, 1964), p. 158.

Kaufman, F. Electronic Data Processing and Auditing, Ronald Press Co., 1961, 180 pp.

Frielink, A. B. Auditing Automatic Data Processing: "A Survey of Published Papers," Elseveir, 1961, 70 pp.

Guide for Auditing A.D.P. Systems, prepared by U.S. Air Force, U.S. Gov't Printing Office, 1962, 121 pp.

He was seemingly enthusiastic about all of these declaring the Air Force Guide "probably the clearest exposition of the methodology of auditing an accounting system based on a computer"; Kaufman's doctoral thesis as "thorough and technically knowledgeable"; and, Frielink's "excellent" bibliography, which lists several books and "no less than seventy-one separate articles" about auditing EDP systems, as "most useful."[7]

McRae was one of the first to raise the question, "Can new types of fraud be perpetrated by a programmer?"[8] Except for what he termed "salami fraud"[9] he believed that "on the whole the types of fraud one expects within an EDP system are much the same as one meets under a conventional system: alteration, omission and such like." His discussion of types of fraud required only seventeen lines of print.

Another "early on" (1965) author, Wayne S. Boutell, has become

---

[7] Ibid., pp. 158, 280, 284, 289.

[8] Ibid., pp. 158-159.

[9] Ibid., p. 171. A "salami fraud, which is peculiar to EDP accounting systems" was defined essentially as one which involves truncating portions of decimal fractions rather than using a rounding rule. Such truncated portions of factions are accumulated in a particular account for manipulative purposes by the programmer or an accomplice.

a noted researcher, lecturer, educator and authority in the area of auditing with the computer. Like McRae, Boutell felt the then "current literature unfortunately muddles the traditional approach and the more progressive viewpoint." There is a need "to sort out significant statements in the literature." For the purposes of this chapter, it is sufficient to identify only the most significant works--books and articles--rather than to present a critique as Boutell did. In addition to the Kaufman and Air Force items noted above, Boutell evaluated the following as significant:

> Richard G. Canning, Electronic Data Processing for Business and Industry (New York, NY: John Wiley & Sons, 1956).
>
> International Business Machines Corporation, The Auditor Encounters Electronic Data Processing, General Information Manual (New York, NY: IBM Corporation, 1956). (Note: This was actually written by Price Waterhouse & Co.)
>
> Ned Chapin, An Introduction to Automatic Computers (Princeton, NJ: D. Van Nostrand Company, 1957).
>
> C. R. Jauchem, "Impact of Electronic Data Processing on Auditing," N.A.A. Bulletin, XXXIX (May 1958), 53-59.
>
> International Business Machines Corporation, In-line Electronic Accounting, Internal Control and Audit Trail (New York, NY: IBM Corporation, 1958). (Note: This was actually written by Price Waterhouse & Co.)
>
> Arthur B. Toan, Jr., "The Auditor and EDP," Journal of Accountancy, CIX (June 1960), 42-46.
>
> Frank J. Curka, "The Effect of Electronic Data Processing on Auditing," N.A.A. Bulletin, XLIII (April, 1961), 85.[10]

---

[10]Wayne S. Boutell, Auditing with the Computer (Berkeley, CA: University of California Press, 1965), pp. 60-70.

In Boutell's bibliography are listed 66 books and 74 monographs and articles that were related to the subject matter of his 1965 work.[11] However, computer fraud is not treated in any way. But, he was one of the first to push for auditing "through the computer"[12] rather than "around the computer."

In the search for literature, some large information retrieval systems were interrogated as likely sources of computer fraud writings. The New York Times Information Bank[13] is a computer repository for "virtually all materials covered in The New York Times plus selected materials from other publications." According to John Rothman, Director of Information Services "it therefore includes published material dealing with 'computer frauds'." He indicates that "it would be retrievable from The Information Bank . . . by search using the terms 'Data Processing,' 'Frauds' and 'Embezzlement'."[14] Access to the Information Bank must be purchased but is available in different modes depending upon the search and retrieval requirements. In general, these modes utilize either remote terminal or batch processing approaches.

---

[11] Ibid., pp. 175-180.

[12] Ibid., pp. 83-98.

[13] The New York Times Company, The New York Times Information Bank (New York, NY: Information Services, The New York Times, 1972). This brochure describes subscription service to computerized storage and retrieval system.

[14] Letter from John Rothman, Director, Information Services, The New York Times, New York, NY, September 5, 1973.

The Law Enforcement Assistance Administration (LEAA) offers several services to those persons interested in activities falling within its purview. Information may be retrieved in different ways. Issues of the LEAA Document Retrieval Index for September 1973, January 1974 and September 1974 were reviewed.[15] None showed a classification for computer fraud but the latest issue had a "Computer security" category. The LEAA also offers a monthly service of sending card abstracts of documents to participating members who have indicated a particular interest profile.[16] These abstracts have produced several computer security references but none on computer fraud.

The National Technical Information Service, which has a collection that exceeds 730,000 titles, is a central source for the public sale of Government-sponsored research, development and engineering reports and other analyses prepared by Federal agencies, their contractors or grantees. It is also a central source for Federally-generated machine processable data files and programs. According to Mary Jane Ruhl, NTIS Program Manager:

> We have nothing on computer-assisted fraud per se since the words "fraud" and "crime" are not used

---

[15] U.S. Department of Justice, Document Retrieval Index (Washington, D.C.: Law Enforcement Assistance Administration, National Criminal Reference Service, U.S. Department of Justice, September 1973, January 1974, September 1974).

[16] U.S. Department of Justice, Selective Notification of Information (Washington, D.C.: Law Enforcement Assistance Administration, National Criminal Justice Service, U.S. Department of Justice). Monthly service of abstracts of documents which relate to participants' profile of interest.

> in combination with computer(s). The only words turned up by the computer were those in connection with law agencies and courts. Therefore, we tried terms on computer information security, computer privacy and security, data processing systems and protection. Seventy-one terms, which seem peripheral to your needs, were turned up.[17]

The University Microfilms Dissertation Abstract Index (DAI) data base was searched for the period "year 1965 to 1970." Although the DAI data base extended from 1938, entries for 1971 and later had not been updated as of the time of the search. Since "auditing" was not in the keyword list, the primary search term was "fraud" used with "auditing, computers, computer, [and] audit." There were (zero) "0 references found."[18]

A search of certain Commerce Clearing House publications was conducted. Selected editions of CCH Accounting Articles and (CCH) Monthly Reporter contained digests (12-20 column lines, typically) of articles from the accounting journals and periodicals published by professional accounting societies and educational institutions as well as business and management periodicals. Fraud classifications were not contiguous but rather were interspersed with other subjects in the CCH references so that the writings pertaining to "fraud prevention," to "fraud examination," to "responsibility for fraud detection," and to "fraud

---

[17]Letter from Mary Jane Ruhl, NTI Search Program Manager, National Technical Information Service, U.S. Department of Commerce, Springfield, VA, August 21, 1973.

[18]Computer printout from DATRIX, University Microfilms, Ann Arbor, MI, October 10, 1973.

through computers" did not make a neat condensed, sequential package. The 1963-1966 volume contained 30 article digests while the 1967-1970 volume condensed 20 articles. These writings were classified under the above four major headings but within a numerical schema for paragraphs that used seven different locations (5100.30/5200.30/9686.30; 5800.32/ 9874.32; 8100.71; 9448.58).

The American Institute of Certified Public Accountants indicated the need for a conceptual approach to teaching auditing as long ago as 1962. Since about 1968, the official AICPA position has emphasized the concept of the Common Body of Knowledge for CPAs with stress being laid on the learning of "how" and "why" by students rather than on detailed procedures or techniques. More recently, the Institute of Internal Auditors has also issued a report on the Common Body of Knowledge for Internal Auditors. No quarrel with that philosophy can be broached. However, auditing textbooks devote varying amounts of explanation to auditing and EDP (or computers) and virtually no mention of the possibility of computer fraud.

A recent study indicated that for the typical auditing student "only one course in auditing will be available to him at the undergraudate level" and that the "chances are four out of five that he will be studying from one of three texts--Holmes, Meigs and Larsen, or Stettler."[19] Examination of these and other authors' recent editions revealed that none included any definition or discussion of computer

---

[19]John H. Ziegler, "Current Trends in the Teaching of Auditing," Accounting Review (Academic Notes), January, 1972, p. 170.

fraud per se. However, all texts examined incorporated either a chapter or several dispersed sections on the subject of auditing and EDP systems and most made some mention of "fraud." Holmes and Overmyer devoted more than half of a chapter to fraud, using several pages to define crime, fraud, larceny, and embezzlement.[20] Meigs and Larsen indexed fraud in their 1969 edition but not in the 1973 edition.[21] Stettler had two auditing texts in use at the time of the referenced study. The regular text indexed fraud coverage as 17 pages;[22] the "systems based" text shows six pages.[23] Mautz devotes a chapter to errors and adjustments (38 pages) but does not index fraud.[24] Grinaker and Barr refer to fraud per se on only one page.[25] Porter and Burton in utilizing

---

[20]Arthur W. Holmes and Wayne S. Overmyer, Auditing Principles and Procedures, 7th ed. (Homewood, IL: Richard D. Irwin, Inc., 1971), pp. 82-130.

[21]Walter B. Meigs and E. John Larsen, Principles of Auditing, 4th ed. (Homewood, IL: Richard D. Irwin, Inc., 1969), p. 852. See also their 5th ed., 1973.

[22]Howard F. Stettler, Auditing Principles, 3rd ed. (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1970), pp. 34-326, passim. See also 2nd ed., 1961, Appendix B for discussion entitled, "McKesson and Robbins Fraud: A Milestone," pp. 725-734.

[23]Howard F. Stettler, Systems Based Independent Audits (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1967), p. 736. See also 2nd ed., 1974, which has the same coverage.

[24]R. K. Mautz, Fundamentals of Auditing, 2nd ed.(New York, NY: John Wiley & Sons, Inc., 1964), pp. 16-53, 579.

[25]Robert L. Grinaker and Ben B. Barr, Auditing, the Examination of Financial Statements (Homewood, IL: Richard D. Irwin, Inc., 1965), p. 492.

the systems approach to auditing refer to fraud on 13 pages.[26] Willingham and Carmichael show six pages, which include references to the Ultramares case and to data processing errors.[27] In all fairness, it should be noted that certain techniques of fraud, such as kiting, lapping, defalcations, forgery and alteration of checks, and others, are dealt with under other labels such as errors or controls. However, this very dispersion may be an underlying cause for the failure of the prospective and practicing auditor to formulate a clear-cut concept of fraud, especially computer fraud.

As Roy and MacNeill were starting the "'common body of knowledge for CPAs' project" they sought to assess the changes in accounting literature. In contrasting the 1944-47 and 1959-60 periods, they noted the change in headings and number of entries thereunder in the Accountants' Index. Although 18 classifications were noted by the pair, only four can be related to this study. The number of papers for the headings and periods indicated were:[28]

	1944-47	1959-60
Integrated data processing	0	42
Mechanical devices	69	216
Operations research	0	27
Systems and procedures	0	17

---

[26]W. Thomas Porter, Jr. and John C. Burton, Auditing: A Conceptual Approach (Belmont, CA: Wadsworth Publishing Company, Inc., 1971), p. 541 and Preface.

[27]John W. Willingham and D. R. Carmichael, Auditing Concepts and Methods (New York, NY: McGraw-Hill Book Company, 1971), pp. 18-21, 232, 293.

[28]Robert H. Roy and James H. MacNeill, "Study of the Common Body of Knowledge for CPAs," Journal of Accountancy, December 1963, pp. 56-57.

A review of selected headings in all editions of the Accountant's Index covering the years 1950 to 1973 inclusive was made by this author. The intent was also to assess the changes in accounting literature relevant to the subject of this thesis. Table 3-1 identified the classification headings reviewed and the inclusive years in which the headings appeared during the period 1950-1973.

It is significant that "computers" did not become a major heading until 1971. Note that "computer fraud" is not listed as a heading, however that term or an equivalent may be found in some titles listed in the Index. The use of the heading, Mechanical Devices, as evidenced by Roy and MacNeill's study and Table 3-1, suggest a reluctance to recognize that the "computer is here to stay." Certainly there seems to be no recognition by the AICPA that computer fraud is a subject of importance. Even the "computer auditing" heading revealed that there was only a total of two entries for the 1971-73 period.

A review of the Accountants' Index entries under the headings indicated above was utilized to prepare listings of the articles, monographs, and books deemed pertinent to a study of computer fraud. These are presented in Tables 3-2 and 3-3 by year of publication. For purposes of comparison of availablity of books, a review was also made of Subject Guide to Books in Print, 1974. Pertinent entries therefrom are listed in Table 3-4 by year of publication.

The AICPA has not been prolific in publishing material on the subject of computer fraud or fraud in general. Over a 24-year span Journal of Accountancy articles on the average account for less than

TABLE 3-1

SELECTED HEADINGS REVIEWED IN ACCOUNTANTS' INDEX (1950-1973)

Headings	Years Present
Accountants--Duties and Responsibilities	1950-1973
Accountants--Liability	1950-1973
Auditing--Data Processing	1965-1973
Auditing--Mechanized Records	1950 through 1964
Banks and Banking--Fraud and Defalcations	1950-1973
Commercial Crime	1950-1973
Computer Auditing	1971-1973
Computers--Effect on Accountants	1971-1973
Computers--Security Measures	1971-1973
Data Processing--Computers	1965 through 1970
Data Processing--Effect on Accountants	1965 through 1970
Data Processing Departments--Internal Auditing	1967-1973
Data Processing Departments--Internal Control	1969-1973
Defalcations	1950-1973
Embezzlement	1950-1973
Forgery	1950-1973
Fraud	1950-1973
Insurance, Accountants' Liability	1950-1973
Internal Auditing--Data Processing	1965-1973
Internal Control--Data Processing	1963-1973
Mechanical Devices--Automatic Computers	In 1950 only
Mechanical Devices--Computers	1951 through 1964
Mechanical Devices--Data Processing	1955 through 1964
Mechanical Devices--Electronic Machines	1951 through 1964
Negligence	1950-1973
Shortages	1957-1973
Theft	1950-1973

SOURCE: AICPA (AIA), Accountants' Index, 9th through 22nd Supplements, 1951-1974.

TABLE 3-2

ARTICLES ENTERED IN ACCOUNTANTS' INDEX 1950-1973 PERTINENT TO STUDY OF COMPUTER FRAUD

1973

"Computer Skill Brings on Abuses," Savings and Loan News, September, pp. 108-109.

DeMott, John S. "Inside Information: The Equity Funding Aftermath," Institutional Investor, July, pp. 33-37, 101.

Hudes, Albert. "Behind the Scenes at Equity Funding," Touche Ross Tempo, v. 19, no. 1, pp. 12-19.

"Institute and SEC Take Steps in Equity Funding Inquiry," (News Report) Journal of Accountancy, June, pp. 13-14, 20, 22.

McLaughlin, Richard A. "Equity Funding: Everyone Is Pointing at the Computer," Datamation, June, pp. 88-89, 91.

Menkus, Belden. "Computerized Information Systems Are Vulnerable to Fraud and Embezzlement," (Auditing and Reporting) CPA Journal, July, pp. 617-19. (Also appears in Retail Control, January, pp. 54-59.

Parker, Donn B. "What to Do to Keep Light Fingers off a Bank's Computer," Banking, June, pp. 34-35, 50.

Robertson, Wyndham. "Those Daring Young Con Men of Equity Funding," Fortune, August, pp. 81-132, passim.

1972

Allen, Brandt R. "Computer Security," Data Management, January, pp. 18-24; February, pp. 24-30.

Peck, Paul S. "Data Processing Safeguards," Journal of Systems Management, October, pp. 11-17.

Scoma, Louis. "Catastrophe Prevention in the Computer Complex," Retail Control, August, pp. 48-55.

Sorenson, Jim L. "Common Sense in Computer Security," CPA Journal, May, pp. 379-82.

TABLE 3-2 (continued)

1972 (continued)

Wofsey, Marvin M. "Data Security," Data Management, September, pp. 80-86.

1971

Allen, Brandt R. "Computer Fraud," Financial Executive, May, pp. 38-42, 44.

Astor, Saul D. "Investigator Talks of Embezzlement and Robbery," Office, September, pp. 55-57.

Brown, Roger J. "Data Processing: Protection and Insurance," (Dialogue) SDL Newsletter, Summer, pp. 11-13; Fall, pp. 11-12, 16.

Chu, Albert L. C. "Computer Security: The Corporate Achilles Heel," Business Automation, February, pp. 32-38.

Cole, Kenneth O. "Embezzlement through the Computer," (In Haskins and Sells, Selected Papers 1970, NewYork, pp. 377-89.

Gellman, Harvey S. "Using the Computer to Steal," Computers and Automation, April, pp. 16-19.

Gregg, Maurice W. "Shortage Control through Computerized Error Detection and Correction," Retail Control, March, pp. 58-63.

Howes, Paul R. "EDP Security: Is Your Guard Up?" Price Waterhouse Review, Spring, pp. 46-53.

Reider, Harry R. "Maintaining the Security of Computer Records," Burroughs Clearing House, February, pp. 28-29, 68-70.

Reynolds, Jayne H. "Computer Misuse: A Look at Vulnerable Areas," Best's Review, May, pp. 76, 78, 90-92.

Scoma, Louis. "Protecting Your EDP," Office, September, pp. 53-54.

Zaiden, Dennis J. "Computer Safety Must Go Right Down to Final Wire," College and University Business, August, pp. 37-41.

TABLE 3-2 (continued)

1970

Burt, Kenneth H. "Computer Center Security: Protecting the Achilles Heel," Magazine of Bank Administration, April, pp. 36-39.

Carmichael, Douglas Roy. "Fraud in EDP Systems," New York Certified Public Accountant, January, pp. 70-72. (Reprinted from Internal Auditor, May-June, pp. 28-38.

Pratt, Lester A. "Loss Exposure Hazards under Bank Automation," Burroughs Clearing House, October, pp. 18-60, passim.

1969

"Computers: Embezzlement from Banks," Certified Accountants Journal, November, pp. 639-40.

Freed, Roy N. "Computer Fraud--A Management Trap," Business Horizons, June, pp. 25-30.

Shelton, L. Beck. "Unauthorized Intervention in Computer Processing," by L. Beck Shelton and Edward W. Reed, Internal Auditors, November-December, pp. 59-64.

Van Tassel, Dennie. "Information Security in a Computer Environment," Computers and Automation, July, pp. 24-25, 28.

Wasserman, Joseph J. "Plugging the Leaks in Computer Security," Harvard Business Review, September-October, pp. 119-29.

1968

Allen, Brandt. "Danger Ahead! Safeguard Your Computer," (Management Memo) Harvard Business Review, November-December, pp. 97-101.

1967

Dansiger, Sheldon J. "Embezzlement Primer," Computer and Automation, November, pp. 41-43.

TABLE 3-2 (continued)

1966

Dillon, Gregory M. "How Much Protection for Magnetically Recorded Data?" Systems and Procedures Journal, September-October, pp. 30-33.

Garland, Robert F. "Computer Programs--Control and Security," Management Accounting, December, pp. 43-45.

Olson, Brice P. "EDP--The Embezzler's Tool." (In Institute of Internal Auditors, Proceedings 25th International Conference, 1966, pp. 41-49.)

1965

Price Waterhouse and Company. "Possibilities of Fraud." (In its Use of Computers in Auditing, pp. 27-28.)

1963

Bolden, Stanley J. "Special Hazards of EDP," Credit and Financial Management, October, pp. 11, 22, 36.

Sapega, Andrew. "Plugging EDP Loopholes with Internal Controls," Lybrand Journal, v. 44, no. 3, pp. 11-17.

1962

Elliott, Norman J., ed. "Story of the Misapplied Computer," (Management Controls and Information) Journal of Accountancy, October, pp. 80-82.

Graese, C. E. "Are You Part of a Computer Holdup?" Management Controls (PMM & Co), August, pp. 125-27.

1960

"Embezzlement by Computer," (News Report) Journal of Accountancy, April, pp. 16, 18.

"Punch Cards Cover Up a Thief's Tracks," Internal Auditor, June, pp. 58-60.

TABLE 3-3

BOOKS ENTERED IN ACCOUNTANTS' INDEX 1950-1973
PERTINENT TO STUDY OF COMPUTER FRAUD

1973

Curtis, Bob. Security Control: Internal Theft. (Chain Store Age Books)

Lipman, Mark. Stealing; How America's Employees Are Stealing Their Companies Blind. (Harper's Magazine Press)

1972

Barmash, Isidore (ed.). Great Business Disasters: Swindlers, Bunglers and Frauds in American Industry. (Playboy Press)

Krauss, Leonard I. SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems. (Firebrand, Krauss & Co.)

Van Tassel, Dennis. Computer Security Management. (Prentice-Hall).

1970

Bakay, Virginia Hicks. "Liability of Certified Public Accountants Related to the Auditing and Accounting Functions as Indicated by a Review of Selected Claims." (Thesis (Ph.D.) University of Alabama)

National Consumer Finance Association, Committee on Accounting and Finance. Internal Control Procedure; Prevention and Detection of Fidelity Losses, 3d ed.

Pratt, Lester A. Embezzlement Controls for Business Enterprises. (Fidelity and Deposit Company of Maryland, 13th printing, revised 1966, c 1952)

Samson, James Edward. "Study of the Auditor's Contemporary Legal Hazards and Remedial Action." (Thesis (M.S.) Texas Tech University)

United States Fidelity and Guaranty Company. Forty Thieves.

Young (Arthur) and Company. Computer Auditing in the Seventies.

TABLE 3-3 (continued)

1969

Ray, Anne Morris. "Auditor's Indenditication [sic] and Evaluation of Internal Controls with EDP System." (Thesis (M.S.) Texas Tech University)

1968

Brown, Harry L. EDP for Auditors. (Wiley & Sons)

Carmichael, Douglas Roy. "Conceptual Model of Employee Fraud: A Critique of Accounting Literature and an Interdisciplinary View." (Thesis (Ph.D.) University of Illinois)

Davis, Gordon B. Auditing and EDP. (AICPA)

1966

American Management Association. EDP and the Auditor.

1965

Boutell, Wayne S. Auditing with the Computer. (University of California Press)

Haskins & Sells. Internal Control in Electronic Accounting Systems.

Pratt, Lester A. Bank Frauds; Their Detection and Prevention. (Ronald Press Co.)

1964

American Management Association. Preventing and Detecting Fraud in Business. (Management Bulletin 43)

Keats, Charles. Magnificent Masquerade: The Strange Case of Dr. Coster and Mr. Musica. (Funk and Wagnalls)

1963

NABAC, The Association for Bank Audit Control and Operation. Bank Fraud Prevention; An Analysis of Bank Fraud Losses--Case Histories. (NABAC Bulletin No. 37)

TABLE 3-3 (continued)

1962

McNew, Bennie B. and Prather, Charles L. Fraud Control for Commercial Banks. (Irwin)

Rogers, Keith M. Detection and Prevention of Business Losses. (Arco Publishing)

1960

Cardwell, Harvey. Principles of Audit Surveillance. (Van Nostrand)

Roady, Thomas I., Jr. and Andersen, William R., eds. Professional Negligence (Vanderbilt University Press)

Shaplen, Robert. Krueger--Genius and Swindler. (Knoff)

1958

Pratt, Lester A. Embezzlement Controls and Other Safegaurds for Banks. (Fidility and Deposit Co.)

1956

Surety Association of America. How Much Honesty Insurance?

1955

Bowles, Leonard B. Embezzlement Controls and Other Safeguards for Savings and Loan Associations (Fidelity and Deposit Company of Maryland and American Bonding Company of Baltimore)

Eddy, J. P. Professional Negligence. (London: Stevens & Sons)

1954

Levy Saul. Accountants' Legal Responsibility. (American Institute of Accountants)

Surety Association of America. Safeguards Against Employee Dishonesty in Business

TABLE 3-3 (continued)

1953

Cadmus, Bradford and Child, Arthur J. E. Internal Control Against Fraud and Waste (Prentice-Hall)

1950

American Mutual Liability Insurance Co. Crime Loss Control.

Liberty Mutual Insurance Company. Loopholes and Losses

Maryland Casualty Company. Businessman's Check List of Dishonesty Controls.

United States Fidelty and Guaranty Co. 1001 Embezzlers--Post War; A Study of Defalcations in Business 1947-1948-1949.

TABLE 3-4

BOOKS ENTERED IN SUBJECT GUIDE TO BOOKS IN PRINT 1974
PERTINENT TO STUDY OF COMPUTER FRAUD

1974

Clifford, Martin. Security: How to Protect Yourself, Your Home, Your Office and Your Car. (Drake Publications)

Dallas, Robert and Ronald Soble. The Impossible Dream--The Equity Funding Story: The Fraud of the Century (Putnam's Sons)

Dirks, Raymond L. and Leonard Gross. The Great Wall Street Scandal. (McGraw-Hill)

Glick, Rush C. and Robert S. Newsom. Fraud Investigation: Fundamentals for Police (C. C. Thomas)

Hutchison, Robert. Vesco. (Praeger Publishers)

Leibholz, S. Q. and L. D. Wilson. User's Guide to Computer Crime: Its Commission, Detection and Prevention. (Chilton)

Strobl, W. Security. (Industrial Press).

Thorsen, June - Elizabeth, ed. Computer Security: Equipment, Personnel, and Data. (Security World)

Ursic, Henry S. and LeRoy E. Pagano. Security Management Systems. (C. C. Thomas)

Williams, Alden and David W. Tarr. Modules in Security Studies. (University Press of Kansas)

Woodruff, Ronald S. Industrial Security Techniques. (Merrill Publishing)

1973

Hamilton, Peter. Computer Security. (Petrocelli Books)

Hemphill, Charles F., Jr., and John M. Hemphill. Security Procedures for Computer Systems (Dow Jones - Irwin)

Hoffmann, L. J. Security and Privacy in Computer Systems. (Wiley-Melville)

TABLE 3-4 (continued)

1973 (continued)

Kahn, E. F., Jr. Fraud: The United States Postal Inspection Service and Some of the Fools and Knaves It Has Known. (Harper-Row)

Katzan, Harry, Jr Computer Data Security. (Van Nostrand Reinhold)

Kwitny, Jonathan. Fountain Pen Conspiracy. (Knopf)

Mandell, M. Handbook of Business and Industrial Security and Protection. (Prentice-Hall)

Martin, James. Security, Accuracy, and Privacy in Computer Systems. (Prentice-Hall)

Post, Richard S. and A. A. Kingsbury. Security Administration (C. C. Thomas)

Walsh, Timothy J. and Richard J. Healy. Protecting Your Business Against Espionage. (American Management Association)

Wright, K. Cost Effective Security (McGraw-Hill)

1972

Haldane, R. A. With Intent to Deceive: Frauds Famous and Infamous. (British Book Center)

1971

Cressey, Donald R. Other People's Money: A Study in the Social Psychology of Embezzlement. (paperback, Wadsworth Publishing) (Also, 1973 reprint of 1953 ed. available from Patterson Smith)

Healy, Richard and Timothy J. Walsh. Industrial Security Management: A Cost-Effective Approach. (American Management Association)

Hemphill, Charles F., Jr. Security for Business and Industry. (Dow Jones-Irwin)

1970

Cole, Richard B. Application of Security Systems and Hardware. (C. C. Thomas)

TABLE 3-4 (continued)

1970 (continued)

Cunningham, John E. Security Electronics. (Howard W. Sams & Co.)

Lipman, Mark. Stealing: How America's Employees Are Stealing Their Companies Blind (Harper Magazine Press)

Slee-Smith, Paul T. Industrial Intelligence and Espionage (Cahners Publishing)

1969

Oliver, Eric and John Wilson. Security Manual. (Beekman Publishing)

1968

Healy, R. J. Design for Security. (Wiley & Sons)

1965

Miller, Norman C. Great Salad Oil Swindle. (Coward, McCann, and Geoghegan) (Also paperback by Penguin)

Pratt, Lester A. Bank Frauds: Their Detection and Prevention, 2nd ed.

1963

Knight, Paul E. and Alan M. Richardson. Scope and Limitation of Industrial Security. (C. C. Thomas)

1962

McNew, Bennie B. and Charles L. Prather. Fraud Control for Commerical Banks. (Irwin)

1961

Rudnitsky, Charles P. and Leslie M. Wolff. How to Stop Pilferage. (Pilot Books)

Sutherland, Edwin H. White Collar Crime. (orig. paperback; Holt, Rinehart & Winston)

TABLE 3-4 (continued)

1960

Roady, Thomas G. Jr., and William R. Andersen, eds. Professional Negligence (Vanderbilt University Press)

1952

Hall, Jerome. Theft, Law and Society, 2nd ed. (Bobbs-Merrill)

1950

Lawson, Frederick H. Negligence in the Civil Law (Oxford University Press)

SOURCE: R. R. Bowker, Co., Subject Guide to Books in Print 1974. Reviewed entries under following headings: Commerical Crimes; Electronic Data Processing Departments--Security Measures; Embezzlement; Forgery; Fraud; Internal Security; Industry--Security Measures; Larceny; Negligence; Stealing; Swindlers and Swindling; Torts; and, White Collar Crime.

ten percent of the annual writings on fraud.[29] Note that only three of the forty-five articles in Table 3-2 were published in the Journal of Accountancy. Not one offering--hard copy or cassette--on the specific subject of computer fraud is listed in the AICPA Publications and . . . Materials catalogs for the years 1973, 1974 or 1975. A cassette entitled "Computer Security and the Auditor's Responsibility" is available from the 1973 series. Two publications of the Canadian Institute of Chartered Accountants--Computer Control Guidelines (1970) and Computer Audit Guidelines (1975)-- are offered for the first time in the AICPA 1975 catalog. Also, in the same catalog edition the Computer Systems Exchange, a directory describing over 380 computer systems in 52 industries, is offered to AICPA members in public practice only. The AICPA Library Committee included only one book concerning fraud in a suggested list for an accountant's library.[30] It is the Cadmus and Child book referenced in Table 3-3; however, it has been "out-of-print" for some time.

Although the Stanford Research Institute reports cited in Chapter 2 clearly establish a definitive baseline for publication of computer fraud cases, there are several other works that appear quite useful in any computer fraud research. These are as follows:

---

[29] Counts were made of entries under each Accountants' Index heading listed in Table 3-1.

[30] AICPA Library Committee, Books and Publications Suggested for an Accountant's Library. AICPA, May 1970. Reprinted in (Practitioners Forum) Journal of Accountancy, December 1971, pp. 78-82.

Ciel Carter, Guide to Reference Sources in the Computer Sciences (New York, NY: Macmillan Publishing Co., Inc., 1974).

Michael A. Duggan, Law and the Computer, A KWIC Bibliography (New York, NY: Macmillan Publishing Co., Inc. 1973.

Roy N. Freed, Computers and Law--A Reference Work, 4th ed. (Boston, MA: Roy N. Freed, Esq., 1968, 1969, 1971, 1974).

Javier F. Koung, Computer Security, Auditing and Controls--A Bibliography (Wellesley Hills, MA: Management Advisory Publications, 1973).

Harold Witzer, Computer Security Bibliography, 2d rev. (Santa Clara, CA: Avco Computer Services, January, 1971)--out of print.

The Witzer, Kuong and Duggan works utilize the "computer fraud" classification. Witzer has 17 entries thereunder plus 35 entries under "case-histories." Kuong lists 18 entries which include eight "case-histories articles"; however, he has continued his effort by publishing a semi-annual review or bibliography. Duggan lists only three articles under "computer fraud."

As Carter points out, the literature has proliferated during the thirty some years in which the computer industry has been developing.

> . . . Twenty-five years ago there was no substantial body of literature on the subject. As recently as a decade ago there was little that could be identified as reference literature. In 1971, . . . the amount and quality of substantial information sources was primitive by comparison with other disciplines. Since that time, . . . the continuing proliferation of the technical literature has contained a major amount of pure reference material . . . a significant proportion of what is now available bears a date of 1968 or later.[31]

---

[31]Ceil Carter, Guide to Reference Sources in the Computer Sciences (New York, NY: Macmillan Publishing Co., Inc., 1974), p. vii.

Similarly, computer fraud literature dates from approximately 1971 even though a few scattered, earlier articles may be found. Parker's work published in 1973 clearly marks the beginning of a definitive study of the extent and nature of computer fraud.

CHAPTER 4

COMPUTER FRAUD: SEARCH FOR A PERSPECTIVE

Among the objectives of any research or study of the nature of some particular subject or topic is the desire to achieve a proper perspective of the elements or parameters involved. Accordingly, if we are to achieve the ability to see and consider all aspects of computer fraud relevant for the CPA, we must look at its distinguishing characteristics. The material in this chapter is presented in such fashion that definitions and interpretations from the pre-computer era and non-computer sectors form a foundation for development of an understanding of "computer fraud" as it is interpreted today.

The concept of fraud has been in existence for many years. This frailty of man seems to have been present from the earliest recorded times. Several references to "fraud" and "defraud" as used in the Bible may be found in Strong's Concordance.[1] Admittedly, the meanings as then used would not correspond exactly to an auditor's application of the terms, or even to the interpretations by the courts.

The law of fraud has been in the process of development for more than 500 years. Although there have been a number of landmark cases over the years, the courts, in the past, have been reluctant to

---

[1]James Strong, The Exhaustive Concordance of the Bible (New York, NY: Abingdon Press, 1890), pp. 251, 371.

define fraud.[2] However, there is evidence that the definition and meaning of fraud have been considered at the supreme court level of state and federal jurisdictions. Wiley Daniel Rich references a number of decisions presented by state supreme courts. He also notes:

> In 1887, the supreme court of the United States gave a definition of fraud, which is in agreement with the usual meaning attached to the word by both eminent legal authority and laymen: "In order to establish a charge of this character the complainant must show, by clear and decisive proof, first that the defendant has made a representation in regard to a material fact; secondly that such representation is false; thirdly that such representation was not actually believed by the defendant, on reasonable grounds, to be true; fourthly that it was made with intent that it should be acted on; fifthly, that it was acted on by complainant to his damage; and, sixthly, that in so acting on it the complainant was ignorant of its falsity and reasonably believed it to be true." There have been deviations from the conception of fraud as set forth in this decision of the supreme court of the United States. In fact, the majority of American courts do not adhere strictly to this definition of fraud.[3]

Bouvier's Law Dictionary, 1914 edition, deals with "fraud" at some length in defining the several types of fraud and by giving examples with case citations. For the moment, it is important to note the court's policy of not defining fraud.

> . . . . It is, indeed part of the equity doctrine of fraud not to define it, not to lay down any rules as

---

[2]M. Frances McNamara, 2,000 Famous Legal Quotations (Rochester, NY: Aqueduct Books, 1967), p. 220 quotes an 1887 decision that "no court has ever attempted to define fraud." (Lindley, L. J., Allcard v. Skinner (1887) 36 Ch. 145, 183).

[3]Wiley Daniel Rich, Legal Responsibilities and Rights of Public Accountants (New York, NY: American Institute Publishing Co., Inc., 1935), pp. 88-94. His reference is to "Southern Development Co. v. Silva, 125 U.S. 247, 8 S. C. Rep. 881, 31 L. Ed. 678."

> to the nature of it, lest the craft of men should find ways of committing fraud which might escape the limits of such a rule or definition. "The court very wisely hath never laid down any general rule beyond which it will not go, lest other means for avoiding the equity of the court should be found out." Per Hardwicke, C., in 3 Atk. 278.[4]

Bennett notes in 1930 that "fraud has not been defined by the courts in unequivocal language . . . what amounts to fraud in one case may not in another; the courts, in order to deal ably with fraud as it arises, apply no absolute test, but judge each case separately."[5]

A legalistic viewpoint of fraud has been developed through the respective opinions rendered in court cases. Through the years, these viewpoints have been summarized and reported as consensus definitions in notable law dictionaries. One of these, Bouvier's Law Dictionary, devotes more than three pages to a definition of fraud. Most important for the purposes of this author's research, however, are the paragraphs which describe what constitutes fraud:

> 1. It must be such an appropriation as is not permitted by law. 2. It must be with knowledge that the property is another's, and with design to deprive him of it. 3. It is not in itself a crime, for want of a criminal intent; though it may become such in cases provided by law . . . . It [in the view of courts of equity] includes all acts, omissions, or concealments which involve a breach of legal or equitable duty, trust or confidence justly reposed, and are injurious to another,

---

[4]John Bouvier, Bouvier's Law Dictionary and Concise Encyclopedia, 2 vols., 3rd rev. (being the 8th ed) by Francis Rawle (St. Paul, MINN: West Publishing Compnay, 1914), p. 1306.

[5]George E. Bennett, Fraud: Its Control Through Accounts (New York, NY: The Century Co., 1930), p. 5.

> or by which an undue and unconscientious advantage is taken of another.[6]

Black's Law Dictionary, in both the 1957 and 1968 editions describes fraud as:

> An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right; a false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury . . . . A kind of artifice employed by one person to deceive another . . . . A generic term, embracing all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated . . . . "Bad faith" and "fraud" are synonyms of dishonesty, infidelity, faithlessness, perfidy, unfairness . . . .[7]

Both Bouvier's and Black's dictionaries distinguish among several classifications of fraud. Each describes actual or positive fraud and legal or constructive fraud but not with exactly the same words. Bouvier's distinguishes between felony and fraud in considering fraud in its criminal aspect. Black's makes the distinction between fraud in fact and fraud in law. It is quite interesting to note that Black's definition under the equity doctrine of fraud repeats--word for word--that noted by Bouvier's some 54 years earlier.

---

[6] Bouvier, Bouvier's Law . . . , pp. 1304, 1306.

[7] Editorial Staff, Black's Law Dictionary, 4th ed. (St Paul, MINN: West Publishing Co. 1957), pp. 788-790 and (rev. 4th ed., 1968), pp. 788-789.

Publishers of (standard) dictionaries and other references have not been as reluctant as the courts to describe fraud. Many distinctions and synonyms can be found by the layman. Most of these definitions however have their foundation in authoritative documents such as the previously mentioned law dictionaries. It seems that these writers combine legal and common law interpretations into a condensed definition or select a particular aspect of fraud and expound upon it from a sociological viewpoint.

One encyclopedia (1950 edition) separates "fraud, in law," being either "actual" or "constructive" under "willful misrepresentation intended to deprive another of some right." It defines the offense as generally being a "tort" but notes it may constitute a crime. The passage goes on:

> An actual fraud requires that the act be motivated by the desire to deceive another to his hurt, while a constructive fraud is a presumption of overreaching conduct which arises when a profit is made from a relation of trust (see FIDUCIARY). The courts have found it undesirable to make a rigid definition of the type of misrepresentation which amounts to actual fraud and have preferred to consider individually the factors in each case. The misrepresentation may be a positive lie, a failure to disclose information, or even a statement made in reckless disregard of possible inaccuracy. Actual fraud can never be the result of accident or NEGLIGENCE, because of the requirement that the act be intended to deceive . . . . A lawsuit based upon actual or constructive fraud must specify the fraudulent act, the plaintiff's reliance on it, and the loss suffered.[8]

One dictionary (1958 edition) lists artifice, cheat, cheating,

---

[8]William Bridgwater and Elizabeth J. Sherwood, eds, The Columbia Encyclopedia, 2d ed. (Moringside Heights, NY: Columbia University Press, 1950), p. 717.

deceit, deception, dishonesty, duplicity, imposition, imposture, swindle, swindling, treachery, treason and trick as synonyms in its entry for fraud definition. It goes on to explain these as follows:

> A fraud is an act of deliberate deception with the design of securing something by taking unfair advantage of another. A deceit or deception may be designed merely to gain some end of one's own, with no intent of harming another; an imposition is intended to take some small advantage of another, or simply to make another ridiculous. An imposture is designed to obtain money, credit or position to which one is not entitled, and may be practiced by a street beggar or by the pretender to a throne. All action that is not honest is dishonesty, but the term dishonesty is generally applied in business, politics, etc., to deceitful practices which are not distinctly criminal. Fraud includes deceit, but deceit may not reach the gravity of fraud; a cheat is of the nature of fraud, but of a petty sort; a swindle is more serious than a cheat, involving larger values and more flagrant dishonesty. Fraud is commonly actionable at law, cheating and swindling are for the most part out of the reach of legal proceedings.[9]

Another well-known dictionary (1961 edition) separates the definition of fraud into "fraud in fact . . . called also actual fraud" and "fraud in equity . . . called also equitable fraud or legal fraud." Defraud is defined as taking or withholding "from one some possession, right, or interest by calculated misstatement or perversion of truth, trickery or other deception." Cheat, deception and imposture are given as synonyms.[10]

---

[9]Funk and Wagnalls Company, Standard Dictionary of the English Language, International Edition (Chicago, IL: Encyclopaedia Britannica, Inc., 1958), p. 502.

[10]Philip Babcock Gove, ed., Webster's Third New International Dictionary of the English Language Unabridged (Springfield, MASS: G. & C Merriam Company, 1961), pp. 593, 904.

Webster's New World Dictionary, College Edition, 1968 defines fraud as "deceit; trickery; cheating; [and] in law, intentional deception to cause a person to give up property or some lawful right." It also lists "something said or done to deceive; trick; artifice."

A 1974 edition of a popular home encyclopedia describes fraud in law as "misrepresentation of facts intended to deprive one who relies on it of some valuable possession." An act to defraud may be a crime in itself or "an element of a more specific crime such as obtaining money by false pretense."[11]

This frailty of man has been especially noted in a business context. An early sociological study concerning crime and criminal law had this to say:

> It is a sad commentary upon the civilization of today that there are few contrivances or processes introduced into the business world but what are immediately seized upon for the advancement of criminal ends. There are certain forms of offenses against property for gain, especially embezzlement and offenses on the order of fraud, cheating, swindling, etc., together with various credit frauds, for which, under modern economic and commercial conditions, a rather special technique of protection will have in greater or less part to be built up.[12]

Further study of criminal behavior concerning certain social and personal pathologies led Edwin H. Sutherland, a sociologist, to coin the phrase "white collar crime." This term was defined "approximately

---

[11]Editorial Staff, The New Encyclopaedia Britannica Micropaedia, Volume IV, Ready Reference and Index (Chicago, IL: Encyclopaedia Britannica, Inc., 1974), pp. 287-288.

[12]Harry Best, Crime and the Criminal Law in the United States (New York, NY: The Macmillan Company, 1930), p. 308.

as a crime committed by a person of respectability and high social status in the course of his occupation."[13]

A study of embezzlers in this same era has become a "classic." Cressey, noting legal and scientific difficulties with his research parameters if he used the legal concept of embezzlement, abandoned that approach. Instead he chose two criteria:

> . . . . First, the person must have accepted a position of trust in good faith . . . . Second, the person must have violated that trust by committing a crime. These criteria permit the inclusion of almost all persons convicted of embezzlement and larceny by bailee and, in addition, a proportion of those convicted of confidence game, forgery, and other offenses.[14]

A great deal of literature on the subject of the offender in business and the professions has been generated. As might be expected there is not complete agreement as to the offenders and the kinds of crimes that should be classified as white collar. Perhaps this can best be illustrated by an excerpt from a description contained in a popular home encyclopedia.

> Occupational offenders and white-collar criminals. Offenders in this category include businessmen, politicians, government employees, doctors, and others who commit crimes that are closely related to their work. . . . Violations of the law by businessmen include those related to receiverships and bankruptcies, restraint of

---

[13]Edwin H. Sutherland, White Collar Crime (New York, NY: The Dryden Press, 1949), p. 9. See also his three earlier articles published in 1940, 1941, and 1945.

[14]Donald R. Cressey, Other People's Money (Belmont, CA: Wadsworth Publishing Company, Inc., 1971), p. 20. (Reprint of 1953 edition.)

trade such as monopoly, illegal rebates, infringement of patents, trademarks, and copyrights, and misrepresentation in advertising. Norms concerning food and drugs sale and antipollution regulations also may be violated. Employers have been found to violate laws regarding wages, hours, and public contracts. Politicians and government employees may obtain illegal financial gains by furnishing favours or confidential information to business firms and obtaining illegal commissions. In the medical profession, doctors may give illegal prescriptions for narcotics and give false testimony in accident cases. Lawyers may misappropriate funds and secure perjured testimony from witnesses. Embezzlement is a common form of occupational crime.

The major difference between occupational offenders and other offenders lies in the offender's conception of himself. The occupational offender rarely sees himself as a criminal. He may, in fact, see himself as a respectable citizen. In addition, the usual middle or high social status of these offenders is such that it also makes it difficult for the public to conceive of them as criminals.

The consideration of white-collar crime in criminology has introduced an important balance to an otherwise distorted picture that is presented by the exclusive study of conventional crime in society. Perpetrators of white-collar crime, who are usually better educated are less often sentenced to imprisonment and are often not prosecuted formally by the system of criminal justice. Instead, they may be disbarred from their profession or receive fines that they are usually able to pay more easily than are conventional criminals. In purely monetary terms, it has been estimated that the cost of conventional crime is trivial compared to the millions involved in the crimes of fraud and embezzlement. Studies of the activities of large corporations have suggested that their illegal activities may be highly organized and persistent and, as a whole, show clear disregard for the government, the law, and the people who administer it. But the concept of white-collar crime has been strongly criticized from some quarters because it has expanded the concept of crime beyond what has conventionally been considered the proper area of study for criminology--the study of the overt acts of convicted offenders. These critics also insist that there is a basic incongruity involved in the proposition that implies that a community's political and business leaders may also be criminals. Proponents of the concept of

> white-collar crime are accused of being unrealistic and of having diverted attention away from the serious nature of conventional crime.[15]

The Chamber of Commerce of the United States has recently created a short, workable document for the purpose of disseminating condensed, compact information on white collar crime to those in business, industry, and the professions. It defines "white-collar crime" as follows:

> . . . illegal acts characterized by guile, deceit, and concealment--and are not dependent upon the application of physical force or violence or threats thereof. They may be committed by individuals acting independently or by those who are part of a well-planned conspiracy. The objective may be to obtain money, property or services; to avoid the payment or loss of money, property, or services; or to secure business or personal advantage . . . committed by, and perpetrated against, (1) corporations, partnerships, professional firms, nonprofit organizations, and governmental units and/or (2) their executives, principals, and employees as well as such "outsiders" as customers, clients, suppliers and other organizations or individuals.[16]

When fraud or embezzlement are involved in an employee's dishonest activity, the determination of whether it constitutes a crime may be important. For such an act to be a crime, it must fall under the following definition.

> The Elements of Crime. It is generally agreed that the essential ingredients of any crime are (1) a voluntary act or omission (actus reus) accompanied

---

[15] Editorial Staff, The New Encyclopaedia Britannica Macropaedia, Volume 5 (Chicago, IL: Encyclopaedia Britannica, Inc., 1974), p. 270.

[16] Chamber of Commerce of the United States, A Handbook on White Collar Crime (Washington, D. C., 1974), pp. 3-4.

> by (2) a certain state of mind (mens rea). An act may be any kind of voluntary human behavior. . . . Criminal liability may also be predicated on a failure to act when the accused was under a legal duty to act and was reasonably capable of doing so . . . . Guilt is attributed to a person who acts "purposely," "knowingly," "recklessly," or "negligently."[17]

Although there are other authors that have dealt with fraud and auditing, Bennett's book is an important major work on the combined subject since it has been used as a reference by numerous accounting researchers. Accordingly, his discussion seems appropriate as a base, or at least a starting point, for the purpose of this study, and for the perspective of an accountant/auditor. He defined fraud in accounting as "all acts, dishonest or deceitful, the object of which is to deprive some person or corporation of property without knowledge or consent of the owner. . . . Although the law is quite clear on the required elements of fraud, the facts which will constitute fraud depend upon the particular circumstances of each case."

In discussion of the legal distinctions, he went on to say:

> . . . Since cases of fraud come into close contact with the law, and since the law has provided a specific vocabulary, it seems necessary and desirable to dwell . . . upon certain definitions . . . [from] the point of view . . . of criminal law, under which fraud cases fall.
>
> The specific crimes which relate to the subject under consideration are larceny, embezzlement, and forgery.

He determined that fraud could be a crime or a tort and could be either a felony or a misdemeanor depending upon the gravity of the

---

[17] The New Encyclopaedia Britannica . . . Volume 5, p. 277.

offense. He indicated that "misappropriation" and "defalcations" were terms with no strictly accurate technical meaning and that "larceny" or "embezzlement" would be more correct. He emphasized, however, "that larceny and embezzlement are not one and the same crime." He pointed out "that the crime of embezzlement is strictly statutory."[18]

Harvey Cardwell recognized that there had long "been a need for a major treatise on embezzlement." He "began an accumulation of notes, cases, and ideas about 1930 in preparation for a fundamental work on fraud." Accordingly, "to the public accounting profession, The Principles of Audit Surveillance presents a challenge to reappraise its position with regard to inside theft and to assume additional duties, responsibilities, and liabilities in an area where only the accountant is qualified to function and has routine access to the confidential records where evidence of crime is concealed."

He was not satisfied with the labels being used: Larceny, theft, embezzlement and related terms. He felt the auditor needed "one general term to include all types of immorally appropriating an employer's assets." As a consequence, Cardwell derived the term "inside theft" to describe all thefts by both employees and employers. Utilizing this concept, he developed an accounting classification schema which may be summarized as follows:

Larcenous Thefts
Fraudulent and illegal transfers of possession accomplished without manipulation of accounts

---

[18]Bennett, pp. 5, 9, 11, 15-16.

Manipulative Thefts
Fraudulent, illegal misrepresentations of accounts with thieves and accomplices of thieves

Legal Thefts
Fraudulent transfers of legal title

Miscellaneous Thefts
Thefts of unrecorded assets, and thefts from other employees and from debtors and creditors of the employer[19]

Note that the concepts contained in Cardwell's 1960 classification of inside thefts are quite similar in nature to those presented by Dr. Carmichael and Belden Menkus in their later discussion of methods of fraud in "an EDP system" or "computerized information systems."[20]

One way for the prospective or practicing CPA to gain a perspective of fraud or computer fraud is through reference to auditing texts. None of the popular texts—or any of the others—noted in Chapter 3 used the term computer fraud in any way. Most did not even define fraud. Of the popular texts that defined fraud one was written by Holmes and the other by Stettler.

Holmes uses substantially the same definitions for larceny, embezzlement and fraud in the various editions of his texts starting in 1939 and running through 1971. Although he devotes a number of pages to these definitions, he summarizes the latter by stating that

---

[19]Harvey Cardwell, Principles of Audit Surveillance (Princeton, NJ: D. Van Nostrand Company, Inc., 1960), pp. v, vi, 18-19, 31-65.

[20]See Chapter 1 for each author's classification list and especially footnotes 19 and 20 for references to their respective articles in which more complete discussion can be reviewed.

it "may constitute embezzlement or larceny, or both, and may be a misdemeanor or a felony and is always a crime or a tort, and legal action may originate by the state or its subdivisions or by an injured person.[21]

Stettler also uses a similar definition over a span of years in 1961 and 1967 texts. He stated that fraud involves "trickery or deceit, and is the frequent handmaiden of embezzlement, since the embezzler usually seeks some means of concealing his misappropriation . . . [and may] . . . conceal otherwise honest errors, or . . . create an appearance when such is not the case."[22]

There does seem to be a reluctance to define fraud, just as there seems to be a reluctance by victims to admit that fraud has occurred. An analogy might be developed along the lines that if we did not define promiscuity, sex, love or intercourse, our society would thus be able to eliminate--or at least reduce the number of--illegitimate children.

In the search for a perspective about computer fraud, definitions and interpretations relating to "just plain" fraud have been

---

[21]Arthur W. Holmes, Auditing Principles and Procedure (Business Publications, Inc., 1939), p. 96. Six later editions published in 1945, 1951, 1956, 1959, 1964, and 1971 by Richard D. Irwin, Inc., contain nearly identical language in defining fraud. In another text, Basic Auditing Principles (Homewood, IL: Richard D. Irwin, Inc., 1957), p. 27, substantially the same langauge may also be found.

[22]Howard F. Stettler, Auditing Principles, 2nd ed. (Englewood Cliffs, NJ: Prentice-Hall Inc., 1961), p. 54. See also Systems Based Independent Audits (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1967), p. 49.

examined. Despite the reluctance of the courts to finitely define fraud and despite the reluctance of victims to admit occurrence--let alone to disclose the salient facts--a rather extensive accumulation of court findings and resultant publicity has caused a body of knowledge to be developed. This provides the basis for classification of fraud within a fairly rigid terminology structure.

Computer fraud as yet does not have any such uniformity in the terminology used to define such acts. An extensive review of the available literature--both books and periodicals--was made in an attempt to ascertain the degree of commonality of terminology used by the various authors. The writings examined were too numerous to cite in footnotes. Most authors had one seemingly favorite term but generally used several in referring to the various aspects of computer fraud. The computer fraud terminology found in the literature included the following:

Computer abuse
Computer-assisted fraud
Computer-based fraud
Computer capers
Computer crime
Computer crooks
Computer-directed fraud
Computer embezzlement
Computer fraud
Computerized fraud
Computer-managed fraud
Computer-oriented fraud
Computer-related crime
Computer-related fraud
Computer swindler
Computer theft
Computer threat
Data processing fraud
EDP-assisted fraud
EDP-based fraud
EDP-directed fraud
EDP fraud
EDP-managed fraud
EDP-oriented fraud
EDP-related fraud
Embezzlement by computer
Fraud in EDP systems
Operator fraud
Programmer fraud
Stealing by computer
Steal via computer
Theft by computer

No attempt was made to determine the popularity of any given term. It was considered sufficient to know that some author elected

to use it. Actually, each "computer fraud" term does tell something of the author's background and outlook merely by being used in such a writing. Many of the authors of the works reviewed are considered to be substantive experts in the field.

One of these experts, Donn B. Parker, described in a 1973 study the results of analysis of threats to the security of multiaccess, on-line computer systems. He noted:

> . . . . Computer-related crime runs the gamut from someone attempting to administer the coup-de-grace to a computer--several shots were fired at one, denting a cabinet but leaving the machine itself undamaged--to the actual piece-by-piece theft of a complete computer. Between these extremes are the really sophisticated security threats that involve the compromise or subversion of programs and operating systems.
>
> Computer-related crime is a term frequently used to describe the subject of this study. This impact term might be more accurately replaced by the following description: computer-related incidents of intentionally caused or threatened losses, injuries, and damage. This description covers the entire spectrum from crimes as defined by legislative action to unauthorized acts and disputed incidents.[23]

In a later 1973 study, Parker decided that a more all-inclusive term was needed in keeping with the scope of the cases investigated and analyzed. He notes:

> . . . computer abuse is defined as all types of acts distinctly associated with computers and data communications in which victims involuntarily suffer or could have suffered losses, injuries or damage, or in which perpetrators receive or could have received gain. . . .

---

[23]Donn B. Parker, Threats to Computer Systems (Menlo Park, CA: Stanford Research Institute, March 1973), pp. viii, xi, 1.

> The studies support many of the findings of criminology research on white-collar crime. However, there are indications of new characteristics and changed importance of known characteristics noted in computer abuse.
>
> Assigned types are as follows:
>
> (1) Vandalism
> (2) Information or property theft
> (3) Direct financial fraud or theft
> (4) Unauthorized use or sale of services
>
> . . . . The cases have also been classified in other ways for special purposes:
>
> Involvement of time-shared computers
> Banking
> Bank embezzlements
> Civil government
> Circumstances of discovery of perpetration
> Consumer fraud[24]

As noted earlier, in a recent handbook, the Chamber of Commerce indicated concern with the problem of white-collar crime and its impact upon businesses and the professions. In the section on computer-related crime, the handbook noted:

> . . . . Computer abuse can take the form of embezzlement, misappropriation of computer time, theft of programs, and illegal acquisition of such proprietary information as marketing plans and forecasts, product design, secret manufacturing processes, and confidential technical data.
>
> . . . . Although the methods of computer-related fraud are limited only by one's imagination, they generally fall within the categories below.
>
> 1. Programs and programming . . . .
> 2. Computer time . . . .

---

[24]Donn B. Parker, Susan Nycum, and S. Stephen Oura, Computer Abuse (Menlo Park, CA: Stanford Research Institute, November 1970), pp. 5, 27.

3. Input data . . . .
4. Computer output . . . .
5. Data communications . . . .
6. Computer hardware . . . .[25]

By utilizing the conceptual classification described by Parker, it is possible to begin to see the implications of computer fraud for the CPA. Parker reports 148 computer abuse cases by type as follows:[26]

Vandalism	26
Information or Property Theft	49
Financial Fraud or Theft	50
Unauthorized Use or Sale of Services	23
	148

In consonance with the definitions noted above, it seems safe to say the CPA would be interested only in the latter three types as falling within the meaning of computer fraud. In all probability the last type listed would not be of dire consequence to the CPA's opinion on the financial statement. Such computer activity ordinarily would not serve to mis-state either real or nominal accounts, except that the business might well have acquired more computing power than it actually needed.

Cardwell's theft classification schema may be appropriate as a means of analyzing Parker's computer abuse cases that relate to fraud. The CPA, the lawyer, the law enforcement official, and the judge all seem to need a more definitive perspective if societal

---

[25]Chamber of Commerce, Handbook on White . . . , pp. 20-23.

[26]Parker, Computer Abuse, p. 26.

goals are to include the more rigid assignment of responsibility for the prevention and detection of computer fraud.

Cardwell notes that there are distinctive and separable categories of sequences and/or phenomena related to theft. These consist of the theft act itself, concealment manipulations, and conversions (or changing the forms of that which is stolen to forms which are more usuable to the thief). By utilizing the same definitions and interpretations assigned by Cardwell to these terms, it is possible, and reasonable, to apply his classification structure to Parker's computer abuse types when such acts are perpetrated against or within a given computer system.

As explained in more detail elsewhere in this study, access to a computer system may be gained by probes from within or external to a firm's resource environment. Consequently, the perpetrator may be "inside" or "outside" the firm. The "inside" perpetrators may, or may not, have authority to access the computer system. At any rate the key phenomena concern concealment. If no concealment attempts are made, the obtaining of resources--information, property, financial, or computer usage--via unauthorized access to the computer system constitutes larceny, theft, or stealing. Conversion may, or may not, take place depending upon the form and value of the resources taken. Any concealment effected either before, during, or after the unauthorized computer access in order to conceal would cause the obtaining of resources to constitute fraud. As Cardwell notes the various types of theft acts, concealment, and conversion "can be combined in countless

patterns." Regardless of the approach utilized, "the imposition of a burden of discovery and action on the employer is the essence of the accounting concept of"[27] the computer fraud attempt. This should be of primary concern to the prospective or practicing CPA.

---

[27]Cardwell, pp. 66-107.

CHAPTER 5

COMPUTER FRAUD: SEARCH FOR A CPA'S EXPOSURE INDEX

The introductory chapter of this study provided a brief picture of the historical and technological development of accounting systems, data processing, computer generations, data communications, and adaptation of auditing--particularly by CPAs--to resultant changes in the business environment. In fulfilling the objectives of this chapter, it will be necessary to select pertinent quantitative data relating to specific factors that exist within the several environments enumerated above. The primary purpose of this chapter is to attempt to determine an index of a CPA's exposure to computer fraud.

It can be established that there are a certain number of access points to a computer system and a certain number of persons who have the requisite knowledge to commit computer fraud. It can also be determined that there are a certain number of business firms in operation and a certain number of CPAs. From these factors and Parker's classification of cases by computer abuse type, we should be able to draw some generalization about the CPA's risk of exposure to computer fraud.

It is generally conceded that the first "business" computer was introduced in 1954. Since that time, the numbers of computers used for business purposes seem to have multiplied by some exponential factor. As might be expected, great numbers of the business computers are utilized within accounting systems. Recent trends have indicated

that computer systems and communications systems have been combined to expand the geographical limits and to increase the number of access or entry (input/output) points for any given data processing environment.

Although data for other years will be presented, it is believed that 1970 figures are most appropriate and provide the most complete set of data for the above described model to be developed. Even though the availability of the 1970 census data is a prime consideration in the selection of a model year to be used, it should also be noted, as is indicated in earlier discussions in this study, that 1970 may be considered the turning point in the recognition of the problem of computer fraud. By then, the first literature on the subject per se had appeared, auditors were becoming more involved in EDP auditing, development of computer technology included considerable concern with security over access and data files, and the gathering of "computer abuse" information was in transition from avocation to funded research.

Table 5-1 shows the number of computers installed for various years. For the most part these data represent general purpose computers which may easily be used for either business or scientific applications. Generally, the distinction rests on the type of programs utilized. Although many sources were used as references (too many to footnote), it was determined that figures representing a consensus of estimates would be most accurate for the purposes of this study.

An example of the wide-ranging estimates is illustrated by reference to a very recent survey conducted by market research

TABLE 5-1

NUMBER OF COMPUTERS INSTALLED IN UNITED STATES

Year	Number
1950	10-15
1955	1,000
1960	6,000
1965	30,000
1970	85,000
1971	100,000
1972	128,000
1973	140,000
1974	155,000
1975	200,000
1980 (estimated)	425,000

SOURCE: Estimates based primarily on data in various AFIPS and other EDP industry publication.

specialists Frost & Sullivan, Inc. The results indicate the extent of advances in circuit sophistication and miniaturization and reflect the movement on the continuum of techniques and equipment from third to fourth generation computers (as discussed in Chapter 1).

The silicon chip approach has resulted in the application of microprocessors to intelligent peripherals and dedicated processors--most often within a computer network environment. Point-of-sale and CRT terminals as well as a variety of other data entry devices have new capabilities as a result of microprocessor technology.

The survey was the basis for a forecast that there would be "two million minicomputer and 15 million microcomputer installations over the next decade." These would be used primarily in "three major

application areas--business data processing, industrial automation and data communications." In accounting computers, Frost & Sullivan "anticipate a revolution as the microcomputer and minicomputer reenter this lucrative market."[1]

The count of terminals has not been rigorous over the years. Although the Teletype Corporation recently noted the shipment of its 500,000th teletypewriter Model 33 terminal and Western Union now claims that there are more than 100,000 terminals in their network, other surveys have not been completely reliable. However, several recent surveys have been conducted by reliable trade media. These various sources have been utilized to formulate the best estimate of the number of terminals for the years indicated in Table 5-2.

As was the case with computer estimates, the experts on data communications usage appeared to be optimistic. The Frost & Sullivan marketing research survey results indicate that the data communications suppliers expect sales to increase at a real (excluding inflation) rate of about 23% annually for the next three years and then edge down for an overall, ten-year compounded growth rate of 15%.[2]

Variances in terminal count may be illustrated by another expert's prediction. According to Richard A. Kuehn, "the number of

---

[1]Infosystems Staff, "Microcomputers--Mind-Boggling Potential," Infosystems, June 1975, p. 54.

[2]"Datacomm to Jump Fivefold in Decade," The Data Communications User (Datacomm Developments), May 1975, pp. 25-26. See also, "Data Communications Growing at 22.5% a Year," Data Communications (Newsfront), May/June 1975.

TABLE 5-2

NUMBER OF COMPUTER TERMINALS

Year	All Terminals	CRT Terminals
1970	220,000	70,000
1971	500,000	100,000
1972	750,000	250,000
1973	1,100,000	400,000
1974	1,350,000	600,000
1975	1,650,000	750,000
1976	1,900,000	1,100,000
1977	2,250,000	1,300,000
1978	2,500,000	1,600,000
1979	2,750,000	1,800,000
1980	3,000,000	2,000,000

SOURCE: Various issues of Computer Decisions, Datamation, Data Communications, Infosystems, and Modern Office Procedures for 1970 to 1975.

computers with communications capability was projected to increase from 38,700 today to 114,000 by 1980--or an increase of 195%. Terminals are expected to increase from 960,000 to 4.9 million in the same time span."[3]

As indicated in Chapter 1 in the description of computer generations and their further development, teleprocessing networks will become more popular. This technological advance will have an impact on the number of terminals utilized. IBM's G. P. Fusco noted that "of the 350,000 computer-linked terminals in the United States

[3]Richard A. Kuehn, "Systems Planning & Control," The Data Communications User (Tutorial Handbook edition), December 1974, p. 15.

in 1972, 40% of them were remote." He predicts that "by 1978, there will be more than one-million terminals, with 80% of them remote." He went on to note that "the ten or so very large communications networks of 1972, each with 500 or more terminals, will by 1978 have increased 25-fold--to more than 250 networks, each with more than 2,000 terminals."[4]

The disparity in the estimates for computers and terminals is virtually impossible to reconcile. However, as stated earlier, the data furnished in Tables 5-1 and 5-2 are deemed to be reasonably accurate--though somewhat conservative. In reaching the pertinent judgments it was necessary to accept some data and reject other data published by the Bureau of Labor Statistics (BLS).

Although the BLS computer count was judged to be much too low, the distribution of computers by percentages among the various industry classifications was thought to be reasonably correct. Based on the information about terminals and data communications, a realistic estimate would be that 25% of the computers have terminals. Accordingly, these percentages are applied to the consensus data presented in Tables 5-1 and 5-2 to give a "most likely" breakout of computer and terminal distribution by industry. Table 5-3 shows such distribution for 1970 since that is the year, as noted earlier, that has been selected as the time base for the model.

---

[4]G. P. Fusco, "IBM Unifies Structure for Teleprocessing," The Data Communications User, December 1974, p. 24.

TABLE 5-3

ESTIMATED DISTRIBUTION OF COMPUTERS AND TERMINALS
BY INDUSTRY CLASSIFICATION FOR 1970

	BLS Percentage	Computers	Terminals	Total Access or Entry Points
Agriculture, forestry, and fisheries	0.2	170	440	660
Mining	1.8	1,530	3,960	5,490
Construction	.7	595	1,540	2,135
Manufacturing	34.4	29,240	75,680	104,920
Transportation, communications, electric, gas and sanitary services	6.1	5,185	13,420	18,605
Wholesale and retail trade	7.0	5,950	15,400	21,350
Finance, insurance, and real estate	14.9	12,665	32,780	45,445
Services	22.0	18,700	48,400	67,100
Government	12.9	10,965	28,380	39,345
Total	100.0	85,000	220,000	305,000

SOURCE: Bureau of Labor Statistics, Computer Manpower Outlook (Bulletin 1826), 1974; and data from Tables 5-1 and 5-2.

NOTE: The distribution for computers is based on the BLS percentages and the estimate from Table 5-1. The distribution for terminals is based on the assumption that 25% of the computers utilize terminals and that there are, on the average, about 10 or 11 terminals per computer

In the brief history of the computer's existence there has been a total count of persons employed in such occupations both during the 1960 and 1970 U.S. Census. For the purposes of this study, however, the figures from the 1970 count are most relevant since, for the most part, computer fraud was not recognized as a problem until about 1970.

The 1970 Census of Population listed national totals for computer occupations in six categories. The six categories were designated as follows: Computer Programmers, Computer Systems Analysts, Computer Specialists n.e.c.,[5] Computer and Peripheral Equipment Operators, Keypunch Operators, and Data Processing Machine Repairers. The BLS industry-occupational matrix adopted exactly the same census computer occupational categories. However, for purposes of the BLS computer study, two of these common census and matrix occupational categories were combined. Data for computer specialists n.e.c. were combined with systems analysts because the occupational titles that comprise the computer specialist n.e.c. category seem overwhelmingly to involve systems analysis functions. The job titles included in each of these six categories are as follows:[6]

Computer Systems Analysts
- computer analysts
- computer-systems planning
- computer-systems analyst
- digital-computer systems analyst
- engineer, systems
- health-systems analyst, computer
- manager, computer programming

Computer Specialist, n.e.c.
- computer scientist
- data-processing systems-project planner
- engineer, computer application
- methods analyst, computer
- software specialist

---

[5]Not elsewhere classified.

[6]Bureau of Labor Statistics, Computer Manpower Outlook, 1974, p. 32.

Computer Programmers
- computer programmer
- digital-computer programmer
- electronic data programmer
- programmer, computer
- univac-programmer

Computer and Peripheral Equipment Operators
- card-tape-converter operator
- computer-console operater
- computer operator
- computing-machine operator
- console operator, clerical
- digital-computer operator
- high-speed-printer operator
- K.S.T. operator
- key station terminal operator
- peripheral-equipment operator
- tape-to-card converter operator

Keypunch Operators
- card puncher
- card-punching-machine operator
- encoder
- encoding clerk
- encoding machine operator
- IBM machine operator
- IBM operator
- IBM puncher
- IBM supervisor
- IBM verifier
- key puncher
- keypunch operator
- punch-card operator
- punch operator, office machine
- verifying machine operator

Data Processing Machine Repairers
- computing-systems maintenance workers
- customer's service man-data processing machine rental
- data-processing-machine servicers
- engineer customer's
- IBM installer
- mechanic
    - computing systems
    - data processing
    - electronics computer
    - IBM machine

Since the key and variant job titles do not provide sufficient basis for understanding the extent of an incumbent's duties, it seems appropriate to include descriptions of the respective computer occupations. According to the BLS' Computer Manpower Outlook (1974), the duties are as follows:

Systems analysts

> Analyze business, scientific, and engineering problems for application to electronic data processing systems. Systems Analysts are classified according to their specialty. In business (nonmanagerial) they analyze business problems, such as development of integrated production, inventory control and cost analysis system, to refine its formulation and convert it to programmable form for application to electronic data processing system. In scientific and technical areas (nonmanagerial) they perform logical analyses of scientific, engineering, and other technical problems and formulate mathematical models of problems for solution by digital computer. Those employed as systems engineers analyze electronic data processing projects to determine equipment requirements. Analyze capabilities and limitation of computers and peripheral equipment and plan layout of computer and peripheral equipment to achieve efficient operation. Usually employed by consulting firm or equipment manufacturer.

Computer programmers

> Convert business, scientific, engineering problems to detailed logical flow charts. Computer programmers are classified according to their specialty. In business applications (nonmanagerial) they convert symbolic statement of business problems to detailed logical flow charts for coding into computer language and solution by means of automatic data processing equipment. May convert detailed flow charts to language processable by computer. In scientific and technical applications (nonmanagerial) they convert scientific, engineering, and other technical problem formulation to format processable by computer.

Computer and peripheral equipment operators

> Computer (console) operators--monitor and operate the control console of a computer to process data according

to operating instructions. Study instructions to determine equipment setup and operation; switch necessary auxiliary equipment into circuit and start and operate computer; make adjustments to computer to correct operating problems; review errors made during operation to determine cause; and maintain operating records. Peripheral equipment operators--operate on-line and off-line peripheral machines, according to instructions, to transfer data from one form to another, print output and read data into and out of electronic computer.

Keypunch operators

Operate alphabetic and numeric keypunch machine, similar in operation to electric typewriter, to transcribe data from source material onto punchcards and produce pre-punched data. Attach skip bar to machine and previously punched program card around machine drum to control duplication and spacing of constant data. Load machine with decks of punchcards. Move switches and depress keys to select automatic or manual duplication and spacing, select alphabetic or numeric punching, and transfer cards through machine stations. Depress keys to transcribe new data in prescribed sequence from source material into perforations on card. Insert previously punched card into card gage to verify registration of punches.

Data processing machine repairers

Install and periodically service computer systems. Experience or technical training in electronics often is necessary.

From the descriptions of the computer occupations it should be fairly apparent that nearly all computer employees, with possibly the exception of the keypunch operators, have the knowledge and the opportunity to gain access to the computer system.

As a prelude to a look at total employment by computer occupations, it may be well to think in terms of a single computer installation. Actually, the number of computer employees may range from one to hundreds for any given computer installation. From the standpoint of

risk of exposure to computer fraud, if one is to follow the precepts of good internal control, the computer installation with only one computer employee may have a higher risk of computer fraud than the installation with hundreds of computer employees.

For the purposes of this study and the proposed model in particular it is necessary to deal with averages. The findings of a 1970 survey of computer operations may be helpful in establishing the parameters for a typical computer installation. As part of the survey, an analysis of staffing in the computer occupations was accomplished. It was found that the median user had a staff of about 20, which, in general, included two managers, four operators, five programmers and analysts (sometimes these occupation specialties are combined in a single individual), and nine keypunch operators and EDP clerical personnel.[7] As the reader will note, this breakout does not mesh in all instances with the distribution of persons employed in the computer occupations as shown in the following tables.

Tables 5-4 and 5-5 provide information on employment in computer occupations. For the information in Table 5-5, the indicated sources derived their basic data from the 1970 count taken by the U. S. Bureau of the Census. The BLS also used its Area Wage Surveys which provide data on occupations. The American Federation of Information Processing Societies (AFIPS) also used the BLS and Census studies

---

[7] EDPACS (Abstracts & Commentaries), May 1974, pp. 17-18. See also Vernon W. Ruskin, "Comparing Computer Operations," Journal of Systems Management, December 1973, pp. 34-38.

TABLE 5-4

EMPLOYMENT FOR COMPUTER OCCUPATIONS, 1970 AND 1980

Occupation	1970 Employment AFIPS	1970 Employment BLS	BLS Projected 1980 Requirements
Systems analysts	120,000	102,700	165,000
Programmers	160,000	176,500	250,000
Computer and peripheral equipment operators	130,000	150,000	275,000
Keypunch operators	380,000	300,000	235,000
Data processing machine repairers	*	36,000	72,540
Total	790,000	765,200	997,540

*Not available

SOURCE: BLS, Computer Manpower Outlook (Bulletin 1826), 1974.
AFIPS, Numerical Bias in the 1970 U.S. Census Data on Computer Occupations, July 1974.

TABLE 5-5

EMPLOYMENT IN COMPUTER OCCUPATIONS BY MAJOR INDUSTRY DIVISION, 1970 AND PROJECTED 1980

Industry Division	1970	1980
Agriculture, forestry, and fisheries	710	656
Mining	6,400	6,290
Contract construction	7,335	9,674
Manufacturing	245,550	308,513
Transportation, communication, electronic, gas, and sanitary services	51,645	48,951
Wholesale and retail trade	94,970	107,213
Finance, insurance and real estate	107,460	138,915
Services	188,500	313,858
Government	62,630	63,470
Total	765,200	997,540

SOURCE: BLS, Computer Manpower Outlook (Bulletin 1876), 1974.
AFIPS, Data on Computer Related Occupations Extracted from 1970 Census, October 1974.

as well as other resources in deriving its estimates. This author believes the differences in any of the categories are insignificant for the purposes of this study.

The increasing utilization of computers naturally affects more and more persons in the labor force. Any user not falling within the computer occupation categories may also be sufficiently knowledgeable to gain access to a computer system and then to perpetrate computer fraud. Accordingly, this study needs to be cognizant of the numbers whose jobs involve the use of computers.

A recent AFIPS/Time survey "indicated that the public does have a relatively high degree of job involvement with computers." The study was aimed at providing data on attitudes toward, and impact of, computers.

> Approximately 49% have had a job requiring either direct or indirect contact with a computer, with 30% currently having such a job. In addition, 15% feel their current job requires some knowledge of computing while 7% report their job requires working directly with computers.[8]

Applying those percentages to the total of employed persons in the civilian labor force of 78,627,000[9] in 1970 means that nearly 24 million persons believed their jobs involved either direct or indirect contact with a computer; 12 million persons felt their then current job required some knowledge of computing; and, five and one-half million

---

[8]AFIPS/Time Staff, A National Survey of the Public's Attitudes Toward Computers (New York: Time, Inc., 1971), Not paged.

[9]From Table A-1, Manpower Report of the President (Washington: U. S. Government Printing Office, 1975).

persons would report their job required working directly with computers.

Thus, there appears to be about 7 to 30 times more persons whose jobs involve computers than the count of computer employees included in the 1970 census. This means the opportunity for, and the risk of, computer fraud is considerably greater than might be normally expected. Today nearly seven million persons would have direct access to about 200,000 computers which have more than 1.5 million terminals attached.

Let us now examine the data on number of business firms in operation. Since Table 5-5 shows that about eight percent of computer employment and Table 5-3 shows about thirteen percent of all U.S. computers to be in the government sector, business firms must therefore account for about 90% of computer usuage. However, the growth rate for business firms has not kept pace with that of computers. Table 5-6 shows the count over several years for the three types of business organizations.

Not all of the firms included in the count in Table 5-6 would have sufficient numbers of transactions or data processing requirements to warrant usage of a computer system. Since there is no clear way of making this distinction without extensive research, only limited generalizations may be made by using the above data. However, a different classification structure may be more useful. Table 5-7 gives the number of business firms in the same categories as that used in Tables 5-3 and 5-5 which show numbers of computers and related employment.

TABLE 5-6

NUMBER OF BUSINESS FIRMS BY LEGAL FORM OF ORGANIZATION

Year	Corporations	Partnerships	Proprietorships	Total
1958	990,381	953,840	8,799,711	10,743,932
1962	1,268,042	932,181	9,182,586	11,382,809
1967	1,534,360	906,182	9,126,082	11,566,624
1968	1,541,637	917,500	9,211,613	11,670,750
1969	1,658,744	920,831	9,429,822	12,009,397
1970	1,667,228	936,133	9,399,653	12,003,014

SOURCE: Senate Report No. 93-1168, The U.S.A. Business Community, 1974.

TABLE 5-7

NUMBER OF BUSINESS FIRMS BY INDUSTRY DIVISION
AND LEGAL FORMS OF ORGANIZATION FOR 1970

Industry Division	Corporations	Partnerships	Proprietorships	Total
Agriculture, forestry, and fisheries	37,238	124,165	3,078,255	3,239,658
Mining	14,465	14,383	50,666	79,514
Construction	138,905	51,001	684,643	874,549
Manufacturing	197,807	28,495	183,466	409,768
Transportation, communications, electric, gas and sanitary services	67,398	16,517	296,216	380,131
Wholesale and retail trade	518,062	201,208	1,992,253	2,711,523
Finance, insurance, and real estate	406,235	320,227	565,898	1,292,360
Services	281,218	175,800	2,506,995	2,964,013
Not allocable to above	5,900	4,337	41,261	51,498
Totals	1,667,228	936,133	9,399,653	12,003,014

SOURCE: From Tables 2.4, 3.3, and 5.3, Statistics of Income 1970, Business Income Tax Returns (Publication 428), Department of the Treasury, Internal Revenue Service, October 1973.

It seems fairly clear that a firm's revenue or business receipts amount would be useful as a guide in determining if the firm had the "wealth" to support computer acquisition or usage. If it is recalled that monthly rental costs for a small computer runs from zero to $5,000, we can assume that average costs might well be about $30,000 per year. If only a time-share computer terminal is utilized, a typical cost would be about $1,000-1,500 per month or about $15,000 per year.[10] Accordingly, it would be doubtful that any firm having less than $50,000 annual revenue would be able to afford a computer. Using this assumption to eliminate firms as potential owners or users of computer systems drastically reduces the count of business firms (see Table 5-8).

If a similar approach is used with the assumption that any firm having less than $100,000 annual revenue would be unlikely to acquire or use a computer, a further reduction of about 40% can be noted in the number of business firms. Table 5-9 gives a breakout of the number of firms under several business receipts brackets.

It is interesting to note that the U.S. Senate Report, The U.S.A. Business Community (1974), derived a count for 1970 of 280,000 large firms. That number was established by using a dividing line between small and large firms of $1 million of business receipts. That amount of business receipts translated into an employment of 10 to 60 persons for small firms (assuming a range from about $100,000 revenue

---

[10]This would include equipment rental costs as well as charges for connect time, CPU processing, storage, and long distance tolls (if any). It is assumed the typical user would be on-line for about four hours per work day.

TABLE 5-8

NUMBER OF BUSINESS FIRMS HAVING $50,000 OR MORE BUSINESS RECEIPTS, BY INDUSTRY DIVISION AND BY LEGAL FORM OF ORGANIZATION, FOR 1970

Industry Division	Corporations	Partnerships	Proprietorships	Total
Agriculture, forestry, and fisheries	21,459	31,844	149,608	202,911
Mining	7,698	2,171	5,244	15,113
Construction	105,927	20,496	97,047	223,470
Manufacturing	161,357	13,646	32,750	207,753
Transportation, communications, electric, gas and sanitary services	43,452	5,249	23,999	72,700
Wholesale and retail trade	428,200	119,767	586,961	1,134,928
Finance, insurance, and real estate	121,978	46,294	29,543	197,815
Services	152,247	68,906	220,072	441,225
Not allocable to above	472	866	1,705	3,043
Totals	1,042,790	309,239	1,146,929	2,498,958

SOURCE: From Tables 2.4, 3.3, and 5.3, Statistics of Income 1970, Business Income Tax Returns (Publication 438), Department of the Treasury, Internal Revenue Service, October 1973.

TABLE 5-9

NUMBER OF BUSINESSES WITH AMOUNT OF BUSINESS RECEIPTS INDICATED, 1970

Amount	Corporations	Partnerships	Proprietorships	Total
Under $10,000	289,359	353,304	5,593,667	6,236,330
$10,000-50,000	333,309	273,590	2,659,057	3,265,956
$50,000-100,000	219,757	119,559	660,626	999,942
Totals	842,425	746,453	8,913,350	10,502,228
Over $100,000	824,803	189,680	486,303	1,500,786

SOURCE: From Tables 2.4, 3.3, and 5.3, Statistics of Income 1970, Business Income Tax Returns (Publication 438), Department of the Treasury, Internal Revenue Service, October 1973.

per employee for a wholesale firm down to almost $16,000 per employee for a firm providing a service).

The previously mentioned computer operations survey taken in 1970 indicated that "the median EDP cost for a U.S. computer user is found to be about $300,000 a year." This figure did not include overhead, fringe benefits, amortized start-up costs or certain other costs. Median equipment costs were found to be about 42% of annual costs, staff about 48%, and materials and supplies about 10%. Based on the finding that the percentage of total EDP costs devoted to programmers and analysts did not drop as equipment size increased, it was presumed that was the result of increased complexity of the associated software.

Today, it is estimated that nearly two-thirds of EDP expenditures go toward non-hardware costs.[11]

From the previously referenced Computer Abuse report, a list of recorded cases of computer misuse or abuse can be adapted to the "industry division" classification utilized by the Bureau of the Census, Bureau of Labor Statistics, and Internal Revenue Service. Accordingly, Table 5-10 presents counts of cases by type of computer abuse incident and by industry division. This analysis was accomplished on the basis of the case codes assigned by Stanford Research Institute (SRI) investigators.

With only 96 computer abuse cases having been reported for all business sectors over the period from 1964 to 1973, the probability of a CPA encountering a computer fraud case on any engagement seems practically negligible. For the purpose of this study, "financial fraud or theft" is no doubt the type of computer abuse of primary interest to the CPA. Obviously, the greatest care should be taken on any engagement in the "finance, insurance, and real estate" sector. However, it must be remembered that the 20 such incidents shown in Table 5-10 occurred over a ten-year span. Parker reports six financial

---

[11] EDPACS, Ibid. The survey noted that in over 50 percent of the reporting computer installations, only billing, payroll and general accounting had been implemented. It could be concluded that the average computer user could double or triple the number of computerized business applications, which then were mostly accounting, since it was also noted that less than half were on three-shift operations with about one-fourth on one-shift operations.

TABLE 5-10

COMPUTER ABUSE CASES BY TYPE AND BY INDUSTRY DIVISION, 1964-1973

	Vandalism	Information or Property Theft	Financial Fraud or Theft	Unauthorized Use of Sale or Services	Total Cases
Agriculture, forestry & fisheries	0	0	0	0	0
Mining	1	1	0	0	2
Construction	0	0	1	0	1
Manufacturing	4	10	3	0	17
Transportation, communications, electric, gas, and sanitary services	0	3	0	1	4
Wholesale and retail trade	0	1	0	0	1
Finance, insurance, and real estate	3	7	20	1	31
Services	11	10	3	16	40
Government	2	12	7	3	24
Foreign cases	4	7	16	3	30
Totals	25	51	50	24	150

SOURCE: Donn B. Parker, et al., Computer Abuse (Menlo Park, CA: Stanford Research Institute, 1973), pp. 14-17, 26, 27, 91-112.

NOTE: This summary was derived from an analysis of cases as coded by Parker whereby the first two digits represent the year, and the third digit indicates the type as follows:

1 = Vandalism
2 = Information or property theft
3 = Direct financial fraud or theft
4 = Unauthorized use or sale of services

fraud computer cases for 1970 among a total of twelve abuse cases in which the total loss was $10,920,000.[12]

Code numbers are similarly used to identify the cases in Appendix A of this study. It should also be noted that only 68 of the cases had been verified as of the date of the SRI report. This author believes that there are many more cases of computer fraud that are not reported even when detected, and that there is even a larger number of computer fraud (abuse) cases that are not detected.

Although accounting is not included in the list of "ten most rapidly growing occupations" as are systems analysts, programmers, computer operators, and computer servicemen, it has been declared "among the most dynamic institutions of our times." The number of accountants and auditors in the labor force has approximately doubled since 1950--moving from a count of 376,650 to 714,120 in two decades. This equated to a "compound annual growth rate of 3.3%."[13] The distribution of accountants and auditors by industry classification for 1970 is presented in Table 5-11.

In the same time span, the total number of CPAs has nearly quadrupled. It has been noted that the "CPA trend is considerably more accelerated than the other leading professions." AICPA membership has increased to more than six times that in 1950. AICPA practicing

---

[12] Parker, Computer Abuse, pp. 26, 78.

[13] John W. Buckley and Marlene H. Buckley, The Accounting Profession (Los Angeles, CA: Melville Publishing Company, 1974), pp. 23-25.

TABLE 5-11

DISTRIBUTION OF ACCOUNTANTS AND AUDITORS
BY INDUSTRY CLASSIFICATION, 1970

Industry	Number
Public accounting and professional services	189,665
Agriculture, forestry, and fisheries	1,915
Mining	9,510
Construction	16,800
Manufacturing	166,339
Transportation, communications, electric, gas, and sanitary services	41,068
Wholesale and retail trade	66,993
Finance, insurance, and real estate	68,790
Services (and all other not included elsewhere)	56,367
Government	96,673
Total	714,120

SOURCE: John W. Buckley and Marlene H. Buckley, The Accounting Profession (Los Angeles, CA: Melville Publishing Company, 1974), adapted from Exhibit 10, p. 26.

CPAs have consistently averaged about 60% of the total membership. The number of practice units in which AICPA CPAs are involved increased from 11,415 in 1960 to 14,975 in 1970 (see Table 5-12).[14]

Information concerning a CPA firm's clients, billings, and types of engagements appear to constitute an infrequently broached frontier.

[14] Buckley and Buckley, pp. 26-29.

TABLE 5-12

ACCOUNTANTS AND AUDITORS

Year	Total CPAs	AICPA Member CPAs	AICPA Practicing CPAs
1950	39,000	16,061	
1960	70,250	38,397	26,422
1967	101,100	61,254	38,835
1968	107,000	65,587	41,385
1969	112,000	70,005	44,033
1970	119,000	75,381	46,184

SOURCE: American Institute of Certified Public Accountants, Report of Council, 1968, 1969, 1970, 1971; and The Accounting Profession Annual Report, 1972-73.

John W. Buckley and Marlene H. Buckley, The Accounting Profession (Los Angeles, CA: Melville Publishing Company, 1974).

Very little has appeared in print or, at the least, been released to the general public. However, the barriers are being impinged if not broken.

Virtually the first study "on the nature and scope of activities of U.S. public accounting firms" available to the accounting profession at large was accomplished by Stephen A. Zeff and Robert L. Fossum. They used 1964 data consisting of "sales, asset, and (net) income figures . . . rearranged according to the public accounting firms whose opinions are contained in the annual reports of companies . . . ." Results were summarized into sector exhibits for "industrials, merchandising,

transportation, and utilities," with supporting exhibits detailing the data under 38 industry categories.[15]

A subsequent study by John Grant Rohde, Gary M. Whitsell, and Richard L. Kelsey used "1971 sales, asset, and (net) income figures" and was "patterned after the Zeff and Fossum investigation . . . [as] a replication and updated extension of their earlier work." However, sectors were identified as "industrials, retailing, transporation, and utilities" with no further detailed breakouts. They noted also that an additional "four separate studies analyzed industrial concentrations for audit firms in England, New Zealand, Australia, and Canada" and that "two recent attempts to present a rank-ordering of revenues from domestic operations of the Big Eight firms were reported in Fortune and Business Week."[16]

The practice of a CPA firm may be divided into three broad areas: Auditing, management advisory services, and tax. The three "practice" areas differ in importance as a source of revenue for CPA firms. In a major CPA firm it is estimated that billings for auditing (attest function) are about 60-70% of total revenue. In contrast, the local firm gains about "two-thirds of the income . . ." while a CPA proprietorship "more than 80% of income . . . from write-up (bookkeeping),

---

[15]Stephen A. Zeff and Robert L. Fossum, "An Analysis of Large Audit Clients," Accounting Review, April 1967, pp. 298-320.

[16]John Grant Rohde, Gary M. Whitsell, and Richard L. Kelsey, "An Analysis of Client-Industry Concentrations for Large Public Accounting Firms," Accounting Review, October 1974, pp. 772-787.

unaudited financial statements, and tax services." The Buckleys draw the conclusion that the "attest (audit) function is largely absent in local practice."[17]

From the above tables in this chapter, it is possible to identify data for several parameters--namely, numbers of computers, of terminals, of employees in direct computer occupations, of business firms, and of computer fraud (abuse) cases in the several "industry divisions"--that are pertinent to computations of percentages and/or averages which illustrate some relationships within or among several classifications of environments. Among these relationships are the following:

Percent of firms having computers
Probability that any given firm had a computer
Probability that any given firm had one entry or access point (terminal or computer)
Average number of terminals per computer
Average number of entry points or risk units per computer installation
Average number of computer employees per computer or entry point

It seems clear that the number of computers installed and the number of terminals attached are relevant parameters that establish the number of opportunities for access to computer systems. Any access may be, in general, of any duration unless interrogative and timing controls are utilized. Clearly the number of persons--through employment or otherwise--who have the capability and knowledge to gain access

---

[17] Buckley and Buckley, p. 33; see also Rohde, Whitsell, and Kelsey, Ibid., and "Accounting: A Crisis Over Fuller Disclosure," Business Week, April 22, 1972, pp. 54-60.

to a computer system constitutes another parameter. The interplay of these parameters rests upon the same sociological factors that are present in any other case of fraud.

The parameters in the above tables and the list of cited relationships provide a basis for a conceptual, if not a mathematical, model for determination of an index of a CPA's exposure to computer fraud. In order to complete the creation of a mathematical model it would be necessary to have a count of CPAs and a count of CPA clients for each of the Bureau of Labor Statistics industry classifications.

Refinement of the number of CPA entities would be necessary also. According to the Internal Revenue Service's Statistics of Income, 1970 Business Income Tax Returns, there were 29,546 CPA firms--partnerships and proprietorships--that filed. For each CPA firm, the number of clients having computers and/or terminals would be an important factor in determining a computer fraud exposure index.

The refinement should include only CPA firms conducting audit engagements of clients having computerized accounting systems. As indicated above, these "counts" are not readily available. However, some generalizations are known. About 20 percent of practicing CPAs are in one-man firms. More than 45 percent are in firms having 10 or more members. Slightly more than 38 percent work in the 25 largest firms. The Buckleys also note that "major firms perform 90% of the audit and related services of the 2500 publicly held corporations in

the United States."[18] Another source says "about 80 percent of all companies filing with the SEC employ one of eight large accounting firms."[19]

Since the publicly held firms are the ones that must comply with SEC's requirement for annual financial statements, these no doubt would become predominant in the "count" of client firms for which audits of computerized accounting systems would need to be conducted by a CPA. There are some differences in the estimates of the number of publicly held companies. While the reference noted above cites 2,500 as the applicable figures, a recent Wall Street Journal article states that "independent accountants now must review only annual financial statements, about 10,000 publicly held companies file with the SEC, to ensure that they comply with generally accepted accounting principles."[20] A more recent actual count of the published lists of the New York Stock Exchange and the American Stock Exchange showed that there were slightly more than 5,000 publicly held companies included.

---

[18]Buckley and Buckley, pp. 28-29. See also Bruce S. Berlin and Francis J. Walsh, Jr., Corporations and Their Outside Auditors (New York, NY: The Conference Board, 1972), pp. 15-16, in which they note "more than 9 out of 10 participating companies employ one of the Big Eight firms as their outside auditors . . . [in] auditing engagements."

[19]Thomas F. Russell, "Critique of the Whitman and Flynn Papers," Corporate Financial Reporting: Conflicts and Challenges, edited by John C. Burton and published by American Insitute of Certified Public Accountants, 1969, p. 184.

[20]Wall Street Journal, March 18, 1975, p. 36.

On the basis of the above information, it could be reasonably estimated that, if there are 10,000 publicly held firms, 8,500 such companies are audited by 25 CPA firms. That leaves 1,500 publicly held companies to be audited by the remaining 29,500 CPA firms. If the 280,000 large firms previously noted are subject to audit and if the same ratios apply, 238,000 companies will be audited by 25 CPA firms. That leaves 42,000 companies to be audited by the remaining 29,500 CPA firms. Thus, on the premise that companies subject to audit under the "publicly-held" and "large firm" categories would be most apt to have computers and/or terminals, a range of CPA firm exposure may be established. On the one hand, if only publicly-held firms are considered, it is estimated that 1,525 CPA firms encounter the risk of computer fraud within their clients' activities. On the other hand, if large firms are considered, it is estimated that as many as 20,325 CPA firms could encounter the risk of computer fraud within their clients' activities.

On the basis of the factors presented in the tables and narrative as integral to the proposed mathematical model, it can be determined that there were for 1970 in total about 305,000 access or entry points to computer systems and about five and one-half million persons that could have used those entry points. Thus, on the average 18 persons utilized each of the entry points. We know that the number of firms involved was not less than 10,000 and probably not much greater than 280,000. Therefore, it seems likely that about 145,000 firms had one or more access points into a computer system. Since for a ten-year

span (1964-1973), there were only 96 reported cases of computer abuse, the probability is virtually zero that a CPA firm would have a client in whose firm computer fraud was discovered.

Refinement of the proposed mathematical model is considered absolutely necessary. A reporting system must be so designed and constructed that all pertinent data will be captured and collected.

CHAPTER 6

COMPUTER FRAUD: SEARCH FOR A CPA'S RESPONSIBILITY

In the first chapter of this study, the evolutionary process that brought accounting and computers to the present state of the art was described. It now seems fitting to set the stage for this chapter by describing the eras of auditing evolution. By examining and comparing the eras or milestones of one or both evolutionary processes, pertinent cause-and-effect relationships for computer fraud and a CPA's responsibility should be disclosed and/or highlighted. As a minimum it seems necessary to trace the development of auditing standards, auditing procedures, and auditing tools and techniques and their applicability to fraud in a computer environment.

At a 1972 Symposium on Auditing Problems, one of the discussion subjects concerned the auditing evolution. The classification of auditing history by eras establishes the boundaries useful in comparing and/or correlating critical or milestone events. The framework established by the discussion at the Symposium is appropriate for the purposes of this study. The eras were described "in terms of the major periods of professional change or growth" as follows:

> Emergence: Late 19th century to 1920
> The birth and early development of the auditing profession in the United States
>
> Consolidation: 1929 to early 1940s
> The move toward combination, uniformity and strength

> Technology: 1950s
> The interest in and sometimes preoccupation with audit tools and techniques, especially the so-called "scientific" tools
>
> Professionalism: 1960s
> The assumption of responsibility for shaping the destiny of the profession rather than responding to outside pressures for change; organizing and bonding together for influence
>
> Conflict and Uncertainty: 1970s
> Serious questions about the nature and scope of audit content and responsibility create internal conflict within the profession.[1]

Although it was quite apparent that the primary participants in the auditing evolution discussion emphasized different landmark events as crucial or important in the profession's development, no one challenged the era classifications or the time phases.[2] While perhaps not universally known and accepted, these eras provide a convenient and pertinent framework for the purposes of this study.

Fraud seems to have always been with us and to continually change in method of perpetration as it is adapted to the environment. The potential for computer fraud was born when the technology era

---

[1] R. Gene Brown and Roger H. Salquist, "Some Historical Auditing Milestones: An Epistemology of an Inexact Art," Auditing Looks Ahead, Proceedings of the 1972 Touche Ross/University of Kansas Symposium on Auditing Problems, edited by Howard F. Stettler (Lawrence: University of Kansas, School of Business, May 11 and 12, 1972), pp. 1-11. (Contents were not copyrighted and permission was granted to reproduce or quote from material included therein in whole or part provided full and proper credit given.)

[2] See also Horace G. Barden, "Discussant's Response to Some Historical Auditing Milestones: An Epistemology of an Inexact Art," Auditing Looks Ahead, Ibid., pp. 12-22.

produced the computer. Today, in the midst of the Conflict and Uncertainty era, a question remains as "the judicial concepts of legal liability expand and the auditor's responsibility for fraud and deception becomes cloudy."[3] What is the CPA's responsibility for the prevention and detection of computer fraud?

The introduction of the computer in the 1950s Technology era ultimately led to a recognition that auditing procedures and techniques would be impacted. The AICPA's first official pronouncement concerning the CPA and the computer took the form of recommendations in the Common Body of Knowledge (CBOK) study. Initiated in 1963 and published in 1967, the study considered "the computer to be a permanent and growing element in the world of the CPA." The authors noted:

> Our concern with the CPA's obligation to review the system of internal control, with his need to modify his auditing methods to conform to computerized systems, and with his increasing activity in management services prompts us to make the following recommendations for inclusion in the common body of knowledge:
>
> 1. The beginning CPA should have basic knowledge of at least one computer system. This implies a knowledge of the functions of the component parts, of the general capabilities of the system, and of the more universal terms associated with the computer.
>
> 2. He should be able to chart or diagram an information system of modest complexity. This means that he should be able to comprehend the procedural steps in a system and utilize basic diagram symbols that describe the system clearly and precisely.
>
> 3. He should have a working knowledge of at least one computer language. We recommend no specific language,

---

[3]Brown and Salquist, Ibid, p. 6.

> but there are several relatively universal languages that would serve better than those with more limited applicability. With an understanding of a programming language together with his overall knowledge of information systems, the beginning CPA should be in a position to design a simple information system, program it, and proceed to debugging and testing.[4]

Shortly after the CBOK study became available, another major work pertinent to the subject of this dissertation was published in 1968. A book, which was the result of efforts of an Auditing EDP Task Force appointed in 1966, had an avowed purpose (among others) of guiding "CPAs in auditing business enterprises which use computers for record keeping." Strangely enough the AICPA seemed to disavow its usefulness in certain professional aspects. The Technical Services Division Director noted in the Preface that:

> This book is not intended to represent the establishment of auditing standards and procedures for EDP. Since it has not been considered and acted upon by the Council of the Institute, it does not represent an official position of the Institute . . . .

Since 1969 this author has used the book as a teaching tool and reference in an annual CPA examination preparation review program. Though some material spread across the chapters is redundant--actually redundancy is often absolutely necessary and generally desirable in a learning situation--Auditing and EDP is considered by this author as an excellent coverage of the fundamentals for a CPA who is assigned to an engagement involving the audit of a computerized accounting system.

---

[4] Robert H. Roy and James H. MacNeill, Horizons for a Profession (New York, NY: American Institute of Certified Public Accountants, 1967), pp. 212-13.

In spite of the AICPA's initial view of the Task Force's effort, it seems that the book has served, to some degree, as a subsantive authoritative reference source. It has been used since its publication as the primary reference for all computer-related auditing questions appearing on the semi-annual CPA exams.

The Task Force noted that "this report is directed solely at . . . [CPA] function as independent auditor of organizations with computer-based data processing systems." The authors had the following to say:

> The auditor should understand EDP for two reasons: (1) so that he can prepare a reliable evaluation of internal control in a computer-based data processing system and (2) so that he can utilize the computer in auditing if the characteristics of the system and the relative cost of the application make this procedure advisable . . . .
>
> . . . the relevant body of knowledge for CPAs having field work or immediate supervisory responsibility in audits involving a computer . . . [is comprised] as follows:
>
> The auditor should have a general understanding of computer equipment. He should be familiar with the uses and capabilities of the central processor and the peripheral equipment, but need not be concerned with details such as internal circuit design.
>
> The auditor should have a broad knowledge of file organization, process flow and system design. He should also understand the various methods for safeguarding computer files and the problems of including management or audit trails. He should have the ability to analyze and design an information system of modest complexity.
>
> Though the auditor need not be a programmer, he should understand what programming entails. Elementary training in programming is often helpful in this respect and also provides an awareness of the capabilities of the computer. The auditor should have the ability to prepare specifications for and supervise preparation of a computer program.
>
> The auditor should understand the use of software in the operation of the computer. Though he does not generally

> operate the computer himself, he should understand the operator's role and should be able to supervise the running of computer audit programs.
>
> Typical duties and different patterns of organization, supervision and division of duties should be understood by the auditor. He should also understand the application of management principles to the data processing function.
>
> A knowledge of good documentation practices is necessary. The auditor should be able to follow system flowcharts, record layouts and error listings. Though he generally does not need to be able to decipher detailed symbolic coding or assembly printouts, he should understand their use in documentation.
>
> The auditor should be familiar with the controls used in EDP systems (data conversion controls, input controls, hardware controls, processing controls, output controls, operating controls, file and program controls, etc.). He should know the types of errors usually encountered and the methods for detecting, handling and correcting them.
>
> The auditor must understand fully the audit procedures that do not make use of the computer and must know how to obtain the records necessary for implementing these procedures.
>
> The auditor should be able to recognize situations in which the computer can be used effectively for conducting the audit. He should be able to plan and supervise the development and use of techniques such as test data, controlled processing and audit computer programs.[5]

By again referring to the first chapter of this study, the reader will recall that the momentum of technological advances in the computer field resulted in a third generation of EDP equipment and what some authors, in 1970, dubbed the "3½ generation." These developments were having "a significant effect on the skills required to meet generally accepted auditing standards."

---

[5]Gordon B. Davis, Auditing and EDP (New York, NY: American Institute of Certified Public Accountants, 1968), Preface, pp. 231, 233-35.

In recognition of the problems associated with the dynamism of EDP technology and the anticipated growth of communications tie-ins and the wide array of computer audit situations encountered, members of the (then) AICPA Auditing EDP Systems Committee and Institute staff proposed an approach to "providing the audit staff with the types of competence required." In a 1971 article, these authors suggested "three different proficiency levels for persons assigned to [computer] audits are appropriate: (1) the general audit staff member, (2) the computer audit specialist and (3) the data processing professional." Their delineation of the responsibilies for the respective proficiency levels are cited in part below.

> General Audit Staff Member . . . may be the accountant-in-charge of an engagement, or he may be supervised by an accountant-in-charge. The staff member performs normal audit work and is technically qualified to carry out audit responsibilites on a company whose accounting records are processed by a computer. The computer system may be either "in-house" within the client's own facility or may be at an outside service center. . . . it is clear that the general staff member should:
>
> A. Understand basic computer concepts . . . .
>
> B. Understand and be able to analyze the concentration of controls in an EDP environment . . . .
>
> C. Understand systems flowcharts and descriptions of computerized systems . . . .
>
> D. Have general familiarity with at least one computer programing [or programming] language . . . .
>
> E. Understand in a general way the use of computer auditing software . . . .
>
> F. Understand concepts of file processing . . . .
>
> G. Know when to call for the assistance of a computer audit specialist . . . .

> Computer Audit Specialist . . . is basically an auditor and not a data processing specialist. . . . will be required from time to time in the audit of accounting records processed by the EDP systems . . . because it is not practical for every accountant-in-charge of the audit of computerized clients to have all of the skills of the computer audit specialist. . . . The computer audit specialist's abilities should include:
>
> A. Proficiency as an auditor . . . .
>
> B. Ability to review and evaluate EDP internal control, and recommend the extent of audit procedures required . . . .
>
> C. Understand EDP systems design and operation . . . .
>
> D. Knowledge of programing [or programming] languages and techniques . . . .
>
> E. General familiarity with computer operating systems and software . . . .
>
> F. Ability to identify and reconcile problems with client data file format and structure . . . .
>
> G. Ability to bridge the communication gap between the auditor and the data processor . . . .
>
> H. Know when to call for the assistance of a data processing professional . . . .
>
> Data Processing Professional . . . resolve specialized processing problems . . . [but] it is not possible to categorize all of the proficiency requirements . . . as they embody all of the unique skills within the data processing field.[6]

It seems apparent that the several study groups have recognized a growing degree of complexity and comprehensiveness in the art of computer auditing. The proficiency specifications cited above merely

---

[6]Richard W. Cutting, Richard J. Guiltinan, Fred L. Lilly, Jr., and John Mullarkey, "Technical Proficiency for Auditing Computer Processed Accounting Records," Journal of Accountancy (Accounting and Auditing Problems), October 1971, pp. 74, 76, 78, 80, 82.

mark "snapshot" lists in the transitional process as the auditing profession, at least in part, attempts to "stay current" in the field of EDP auditing. Clearly, however, the criteria delineated above in the several studies relating proficiency requirements to computer auditing would not constitute definitive auditing standards or auditing procedures. The AICPA makes a distinction between standards and procedures in a statement of generally accepted auditing standards.

> Auditing standards differ from auditing procedures in that "procedures" relate to acts to be performed, whereas "standards" deal with measures of the quality of the performance of those acts and the objectives to be attained by the use of the procedures undertaken. Auditing standards as distinct from auditing procedures concern themselves not only with the auditor's professional qualities but also with the judgment exercised by him in the performance of his examination and in his report.[7]

For the purposes of this study, the following generally accepted auditing standards appear to be relevant:

> General Standards
>
> 1. The examination is to be performed by a person or persons having adequate technical training and proficiency as an auditor.
>
> 2. In all matters relating to the assignment, an independence in mental attitude is to be maintained by the auditor or auditors.
>
> 3. Due professional care is to be exercised in the performance of the examination and the preparation of the report.
>
> Standards of Field Work
>
> 1. The work is to be adequately planned and assistants,

---

[7]Committee on Auditing Procedure, Statement on Auditing Standards No. 1 (Codification of Auditing Standards and Procedures) (New York, NY: American Institute of Certified Public Accountants, 1973), p. 4.

> if any, are to be properly supervised.
>
> 2. There is to be a proper study and evaluation of the existing internal control as a basis for reliance thereon and for the determination of the resultant extent of the tests to which auditing procedures are to be restricted.
>
> 3. Sufficient competent evidential matter is to be obtained through inspection, observation, inquiries, and confirmations to afford a reasonable basis for an opinion regarding the financial statements under examination.[8]

It should be noted that the set of standards applicable to a case involving prevention of computer fraud would not necessarily be identical with the set of standards applicable to a case involving detection of computer fraud--even though both cases might well exist within the same or an identical computer environment. The standards must be applied to fit the situation.

The American Accounting Association has taken a slightly different approach in developing criteria to be used as guidelines in measuring the performance of an auditor. The qualities necessary for an auditor are described. Applicable material is quoted:

> Complexity of the subject matter and the audit process indicate the requirement of competence on the part of the auditor. Competence is a product of education and experience as well as continued development of the individual and his profession . . . .
>
> To be judged competent, the auditor must possess the common body of knowledge with in-depth understanding of the subject matter from which the information is drawn, of the process by which the information is developed, and of the audit process. In addition, the auditor must have acceptable experience at an appropriate level of work in the application of relevant knowledge to real-life situations. His

---

[8] Ibid., pp. 4-5.

> competence, of course, improves with continued study and experience.
>
> Fulfillment of auditing's role in society requires that the auditor be competent. Users are dependent upon the auditor to be so qualified in the service he renders since users generally are unable to evaluate an auditor's competency. Consequently, he is obligated morally, professionally, and legally to maintain continually high standards of competence.
>
> Since the auditor serves people, he must possess attributes that instill confidence in his work. His high moral character, integrity, and natural aptitudes are required attributes. To instill confidence, the auditor must perform his tasks with due care. . . . Consequently, moral resposibility is undoubedly higher than legal or professional responsibility, because the auditor is morally responsible if he does not perform his duties properly in a manner that conforms to the best practices of his profession . . . .[9]

Auditing standards, though not given that title immediately, came into existence via formal documentation prior to World War I. The development of an officially declared set of auditing standards was an evolutionary process covering more than three decades. A chronology of six decades of development and improvement is summarized as follows:

1912 Memorandum on Balance Sheet Audits (by Price Waterhouse & Co.)

1917 Uniform Accounting: A Tentative Proposal Submitted by the Federal Reserve Board (w/d in 1918)

1918 Approved Methods for the Preparation of Balance Sheet Statements (w/d in 1929)

---

[9]Committee on Basic Auditing Concepts, A Statement of Basic Auditing Concepts, Studies in Accounting Research #6 (Sarasota, FLA: American Accounting Association, 1973), p. 17.

1929 Verification of Financial Statements (w/d in 1936)

1932 Began Correspondence with New York Stock Exchange (to 1934)

1936 Examination of Financial Statements by Independent Public Accountants (w/d in 1949)

1939 Began Statements on Auditing Procedure (1-24 to 1951)

1947 Tentative Statement of Auditing Standards--Their Generally Accepted Significance and Scope (w/d 1954)

1949 Internal Control (replaced by 1951 Codification)

1950 Audits by Certified Public Accountants--Their Nature and Significance (Also 1960 reprint)

1951 The CPA's Opinion; and, Codification of Statements on Auditing Procedure (w/d in 1963)

1954 Generally Accepted Auditing Standards (w/d in 1963)

1956 40 Questions and Answers About Audit Reports

1963 Statement on Auditing Procedure No. 33: Auditing Standards and Procedures Codification of SAP 25-32 (33-54 to 1973)

1967 The Auditor's Report . . . Its Meaning and Significance

1973 Statement on Auditing Standards No. 1

1974 SAS No. 3--The Effects of EDP on the Auditor's Study and Evaluation of Internal Control

The first guidelines--actually a combination of objectives, standards and procedures--were published in 1917 and subsequently revised in 1918, 1929 and 1936. In 1939, The American Institute of Accountants (AIA) appointed a committee, which became known as the Committee on Auditing Procedure with the objective "to examine into auditing procedure and other related questions." This committee issued 24

Statements on Auditing Procedure between the years of 1939 and 1949.[10] In 1947, the committee issued Tentative Statement of Auditing Standards--Their Generally Accepted Significance and Scope, which was later revised, retitled, and reissued in 1954.[11] Both editions emphasized the importance of the review of internal control while virtually eliminating the requirement for detailed fraud investigation as a part of every audit. In 1949, the committee issued a special report on internal control which assigned "responsibility for safeguarding the assets of concerns and preventing and detecting errors and fraud" to management. The CPA was charged with the review of the system of internal control as a basis for setting the scope of his audit examination.[12]

In 1951, the committee consolidated the more valuable and useful features of the earlier statements by publication of a codification summary. Although many audit techniques actually in use during this period were designed primarily to detect fraud, the Institute declared "the ordinary examination incident to the issuance of an opinion respecting financial statements is not designed and cannot be relied upon to

---

[10]Thomas W. Hill, Jr., "Accountants' Legal Liability," Independent Auditing Standards, A Book of Readings, edited by J. C. Ray (New York, NY: Holt, Rinehart and Winston, Inc., 1964), pp. 95-129. Reprint from The New York Certified Public Accountant, March 1959, pp. 177-88; October 1959, pp. 707-723.

[11]Committee on Auditing Procedure, Generally Accepted Auditing Standards, Their Significance and Scope (New York, NY: American Institute of Certified Public Accountants, 1954), pp. 5-10, 31-35.

[12]Committee on Auditing Procedure, Internal Control (New York, NY: American Institute of Accountants, 1949), pp. 5-6, 11-12.

disclose defalcations and other similar irregularities, although their discovery frequently results."[13]

Once more the earlier pronouncements were consolidated and published (in 1963) with substantially the same language being used in regard to the auditor's responsibility for the detection of fraud. These guidelines stated that "reliance for prevention and detection of fraud should be placed principally upon an adequate accounting system with appropriate internal control."[14]

The 1973 Statement of Auditing Standards is the more recent codification of, and supersedes, Statements on Auditing Procedure Nos. 33 through 54 previously issued by the Committee on Auditing Procedure. The detection of fraud is treated under the major heading concerning responsiblities and functions of the independent auditor. The official AICPA position is quoted verbatim below.

> In making the ordinary examination, the independent auditor is aware of the possiblity that fraud may exist. Financial statements may be misstated as the result of defalcations and similar irregularities, or deliberate misrepresentation by management, or both. The auditor recognizes that fraud, if sufficiently material, may affect his opinion on the financial statements and his examination, made in accordance with generally accepted auditing standards, gives consideration to this possibility. However, the ordinary examination directed to

---

[13]Committee on Auditing Procedure, Codification of Statements on Auditing Procedure (New York, NY: American Institute of Accountants, 1951), pp. 5-8, 11-12.

[14]Committee on Auditing Procedure, Statements on Auditing Procedure No. 33, Auditing Standards and Procedures (New York, NY: American Institute of Certified Public Accountants, 1963), pp. 10-12, 27-33.

the expression of an opinion on financial statements is not primarily or specifically designed, and cannot be relied upon, to disclose defalcations and other similar irregularities, although their discovery may result. Similarly, although the discovery of deliberate misrepresentation by management is usually more closely associated with the objective of the ordinary examination, such examination cannot be relied upon to assure its discovery. The responsibility of the independent auditor for failure to detect fraud (which responsibility differs as to clients and others) arises only when such failure clearly results from failure to comply with generally accepted auditing standards.

Reliance for the prevention and detection of fraud should be placed principally upon an adequate accounting system with appropriate internal control. The well-established practice of the independent auditor of evaluating the adequacy and effectiveness of the system of internal control by testing the accounting records and related data and by relying on such evaluation for the selection and timing of his other auditing procedures has generally proved sufficient for making an adequate examination. If an objective of independent auditor's examination were the discovery of all fraud, he would have to extend his work to a point where its cost would be prohibitive. Even then he could not give assurance that all types of fraud had been detected, or that none existed, because items such as unrecorded transactions, forgeries, and collusive fraud would not necessarily be uncovered. Accordingly, it is generally recognized that good internal control and fidelity bonds provide protection more economically and effectively. In the case of fidelity bonds, protection is afforded not only by the indemnification for discovered defalcations but also by the possible deterrent effect upon employees; the presence of fidelity bonds, however, should not affect the scope of the auditor's examination.

When an independent auditor's examination leading to an opinion on financial statements discloses specific circumstances that make him suspect that fraud may exist, he should decide whether the fraud, if in fact it should exist, might be of such magnitude as to affect his opinion on the financial statements. If the independent auditor believes that fraud so material as to affect his opinion may have occurred, he should reach an understanding with the proper representatives of the client as to whether the auditor or the client, subject to the auditor's review, is to make the investigation necessary to determine whether fraud has in fact occurred, and, if

> so, the amount thereof. If, on the other hand, the independent auditor concludes that any such fraud could not be so material as to affect his opinion, he should refer the matter to the proper representatives of the client with the recommendation that it be pursued to a conclusion. For example, frauds involving "lapping" accounts receivable collections, or frauds involving overstatements of inventory, could be material, while those involving peculations from a small imprest fund would normally be of little significance because the operation and size of the fund tend to establish a limitation.
>
> The subsequent discovery that fraud existed during the period covered by the independent auditor's examination does not of itself indicate negligence on his part. He is not an insurer or guarantor; if his examination was made with due professional skill and care in accordance with generally accepted auditing standards, he has fulfilled all of the obligations implicit in his undertaking.[15]

Strict adherence to this position concerning the CPA's degree of responsibility for detecting fraud may well be an important factor in the previously noted surge in the number of court cases involving CPAs. In a recent study of claims against public accountants, Dr. Bakay reviewed 96 files relating to litigation against local practitioners and found that one-third of these cases alleged undiscovered defalcations.[16]

Although the summarized chronological listing presented earlier in this chapter gives the appearance of a fairly neat and clean-cut

---

[15]Committee on Auditing Procedure, Statement of Auditing Standards No. 1, Codification of Auditing Standards and Procedures (New York, NY: American Institute of Certified Public Accountants, 1973), pp. 2-4.

[16]Virginia Hicks Bakay, "A Review of Selected Claims Against CPAs," The Journal of Accountancy, May 1970, pp. 54-58.

progression from one document to another, such is not really the case when the contents of the documents are examined more closely. For example, "internal check" was referenced in the 1917 memorandum and was carried through the 1929 revision. It was further emphasized in the 1932-1934 correspondence with the New York Stock Exchange. In 1936, the term "internal check and control" was utilized and carried over into the 1939 extension of auditing procedure. By 1949, "internal control" replaced "internal check."

Internal check is generally described as encompassing those characteristics and/or procedures of an accounting system that serve to establish the accuracy and efficiency of the results through some set of "cross-checks" and/or "checks and balances." Prior to the 1940s internal check was viewed as having reasonably broad coverage but by the mid-1950s the meaning had been narrowed considerably. Internal control connotes a wider scope of coverage than internal check ever did. With the advent of the computer, significant changes in the system of internal control are often required. Such changes nearly always demand changes in auditing procedures.

The changes in the use of terms and their meanings, as noted in the preceding paragraphs, may be contrasted to the auditing standards that have remained unchanged from the original language. However, it is quite interesting to note the changes in interpretation that have been presented by various authorities and practitioners.

In 1965, Wayne S. Boutell sought to examine "the environment within which business data-processing systems function" as well as "to

explore possible solutions to the problems which the auditor faces in reviewing these systems." In examining auditing in a changing environment, he comments upon internal control in a manner that seems to reflect a difference in understanding between practitioners and theorists.

> . . . . The problem of internal check was not mentioned prior to 1900, but by 1958 internal control had become of paramount importance in the conduct of an examination . . . .
>
> It is not clear, however, that all accountants are in agreement as to exactly what constitutes a system of internal control or what is meant by the efficiency of the system. . . . But it is not certain that the definition means the same thing to each practitioner . . . .
>
> In order to place the idea of a system of internal control in appropriate perspective from the standpoint of the public accounting practitioner, it may be viewed as a subclassification of the accounting system, which in turn is a part of the information system of the business firm. Conceived in this way, internal control can be said to have three principal objectives: (1) to safeguard the assets of the firm; (2) to prevent intentional or unintentional mistakes; and (3) to insure adherence to management policies . . . .
>
> A new question has arisen in the light of recent technological developments: What changes, if any, might--or should--now be made in these auditing standards? . . . . Since 1954 there has been a decided shift of emphasis; it now appears that study and evaluation of internal control has achieved top status as the basis of efficient and satisfactory examination . . . .
>
> . . . . Along with the current change in emphasis on auditing standards, substantial changes in the underlying auditing procedures have already taken place, too, and it is almost certain that additional substantial changes will take place in the future.
>
> The impact of electronic data-processing equipment on auditing procedures clearly involves the auditor's review

of the system of internal control . . . .[17]

As the accounting environment has changed so was it expected that the internal control system would be changed. Actually, the internal control systems have changed whether computers were introduced or not. Other factors, such as employee turnover, worker resistance, and other human-originated biases have impacted internal control systems so that they tend to be dynamic--and perhaps even in a state of flux--rather than stabilized.

Even before computers were "popular" in the accounting environment, Cardwell noted inherent weaknesses of internal control. He believed that:

> First, it is always a practical compromise between effectiveness and cost; hence the protection is never complete. Second, internal controls deteriorate easily. Small changes in procedure that apparently are unimportant and innocuous will often destroy or impair internal controls. Third, internal controls can usually be circumvented by collusion. . . . Fourth, effective internal controls of all operations cannot be installed in many organizations without excessive costs. For this reason the medium-sized and the smaller units in our economy have always largely depended on surveillance by public accountants rather than on perfected internal controls.[18]

Others have noted the vulnerability of internal controls in information systems. An East Coast consultant wrote:

> There is no such thing as a fraud proof or embezzlement proof information system. This was confirmed by a

---

[17]Wayne S. Boutell, Auditing with the Computer (Berkeley, CA: University of California Press, 1965), pp. vii, 52.

[18]Harvey Cardwell, The Principles of Audit Surveillance (Princeton, NJ: D. Van Nostrand Company, Inc., 1960), pp. 19, 261.

> statement in the 14 June 1971 Security Letter by Marshall Armstrong, president of the American Institute of Certified Public Accountants. He said, "No accountant in the history of our profession has been able to establish fool-proof controls against fraud and embezzlement . . . creating fool-proof controls is impossible." Because people (emphasis added) design and use an information system, it is plainly impossible for someone to design a system that someone else cannot compromise or manipulate. This is equally true with computerized information systems.[19]

The transition from manual, hand-actuated, power-actuated and unit record accounting systems to those that are computer based has not been easy for either accountants or auditors. As Cardwell and Boutell point out, the auditing environment was undergoing change even without the switch to computers. With computers oftentimes there was no audit trail and the internal control system was barely discernible. The lack of training and knowledge on the part of auditors in regard to computer hardware and software, as the technology quickly moved to the third generation level in a decade's time, caused consternation in most local and regional CPA firms.

In the history of auditing, the detection of fraud has played an important part. However, as R. Gene Brown and others have pointed out, there has been a transition in audit objectives as well as in auditing standards and procedures. From ancient times to about 1905, the detection of fraud was a primary audit objective. After the turn of the twentieth century, American auditors began to stress determination

---

[19]Belden Menkus, "Computerized Information Systems Are Vulnerable to Fraud and Embezzlement," Menkus on Management (Bergenfield, NJ: Belden Menkus, 1972), pp. 1-4.

of fairness of the reported financial position while the detection of fraud and errors was relegated to secondary importance. The Securities Acts of 1933 and 1934 and the McKesson Robbins case of 1939 heightened the swing toward the "fairness" objective.[20]

Audit techniques actually in use during any period may be deduced to some degree by review of the textbooks of the era. Whereas Brown indicates the detection of fraud had been eliminated as a stated audit objective by 1940, only a minor amount of research is required to find evidence that tends to refute that statement. Bell and Johns, authors of an auditing text that was extremely popular for more than a quarter century, included in their 1941 and 1952 editions as numbers 5, 6, and 7--the last three items--in their list of "purposes for which accounts and records are audited" the following:

> To detect fraud
> To determine the extent of fraud already detected
> To prevent fraud by the moral effect upon the client's staff[21]

As late as 1957, Holmes--one of the textbook authors found to be popular in the 1971 survey mentioned previously--notes the "objectives of an independent external audit" as:

> To judge management's representations
> To report independently upon financial condition and operating results

---

[20]R. Gene Brown, "Changing Audit Objectives and Techniques," Perspectives in Auditing, Readings and Analysis Situations, by D. R. Carmichael and John J. Willingham (New York, NY: McGraw-Hill Book Company, 1971), pp. 2-13. Reprint from The Accounting Review, October 1962, pp. 696-703.

[21]William H. Bell and Ralph S. Johns, Auditing, 2d and 3d eds. (New York, NY: Prentice-Hall, Inc., 1941, 1952), p. 2.

To correct errors and to detect fraud[22]

In 1961, a study of the philosophy of auditing was an attempt to find some theoretical foundations for auditing. In that process, the study examined the profession's acceptance of responsibility and in particular its stated position about the prevention and detection of fraud. The researchers utilized the then current Rules of Professional Conduct, Generally Accepted Auditing Standards, and the Codification of Statements on Auditing Procedure. Although they expressed only minor complaints about the first two documents, the comments on the 1951 Codification document were more zealous. Their arguments might well be appropriate against similar or corresponding passages of Statements on Auditing Procedure No. 33 (1963) and of Statement on Auditing Standards No. 1 (1973). The researchers' comments were, in part, as follows:

> We are not in . . . agreement with the position taken on the . . . responsibility for the detection of fraud and irregularities.
>
> . . . . One must question, first, whether independent auditors can absolve themselves of responsibility for the detection of irregularities by a simple declaration to that effect when there is ample evidence in professional literature that at one time they considered this an important part of their duties; second, whether some useful search for irregularities might not be effected without incurring prohibitive cost; third, whether internal control and surety bonds actually do provide a satisfactory degree of protection; fourth, whether the extent of the auditor's responsibility for extension of his work when suspicion is aroused might not be more

---

[22]Arthur W. Holmes, Basic Auditing Principles (Homewood, ILL: Richard D. Irwin, Inc., 1957), p. 1.

> usefully stated; fifth, whether the over-all attitude toward acceptance of professional responsibility implicit in such a statement is appropriate to the growth and development of a profession.[23]

Whether or not the auditing profession questions the CPA's role in connection with the prevention or detection of fraud, other interested persons do seem to be of another mind. In a survey performed on a completely independent basis, the Opinion Research Corporation undertook to assess, among other things, the role of the independent auditor. Shareholders and key publics were questioned about the "responsibility for the detection of fraud." The results showed that:

> 66% of the investing public believe that the audit is conducted primarily to uncover fraud.
>
> Analysts/brokers and the business press also tend to agree that detection of fraud is the audit's most important function.
>
> On the other hand, 79% of corporate executives and similarly high majorities of the other key publics disagree.[24]

In the performance of the management advisory service--which for the purposes of this study is deemed to include write-up (bookkeeping) work and preparation of unaudited financial statements--and the tax function, the CPA's responsibility is similar to that of any

---

[23]R. K. Mautz and Hussein A. Sharaf, The Philosophy of Auditing, Monograph No. 6 (Evanston, ILL: American Accounting Association, 1961), pp. 112-115-16.

[24]Opinion Research Corporation, Public Accounting in Transition (Chicago, ILL: Arthur Andersen & Co., 1974), p. 48, 208-213. See also, "The CPAs Get Mixed Reviews," Business Week. September 14, 1974, p. 31.

member of a learned profession. This has been clearly established for a considerable length of time and is generally supported by a reference to Cooley on Torts as the primary authority on the subject.

> In all those employments where peculiar skill is requisite, if one offers his services, he is understood as holding himself out to the public as possessing the degree of skill commonly possessed by others in the same employment, and if his pretensions are unfounded, he commits a species of fraud upon every man who employs him in reliance on his public profession. But no man, whether skilled or unskilled, undertakes that the task he assumes shall be performed successfully, and without fault or error; he undertakes for good faith and integrity, but not for infallibility, and he is liable to his employer for negligence, bad faith, or dishonesty, but not for losses consequent upon mere errors of judgment.

In the performance of the audit (attest) function, however, the CPA not only has a professional responsibility--also supported by the Cooley on Torts reference--to the client but becomes responsible to third parties who rely upon the auditor's opinion rendered for the client firm. Such third party users of information and financial statements to which the audit report relates may include investors, creditors, potential investors, potential creditors, governmental agencies, the general public, client firm employees, unions, and client firm management.

Clearly the above observations can be used only to create a generalized approach to the problem of relating computer fraud and a CPA's responsibility. However, this is sufficient for the purpose of

---

[25]Saul Levy, Accountants' Legal Responsibility (New York, NY: American Institute of Accountants, 1954), p. 3.

establishing a workable structure or classification of a CPA's responsibility. In a recent, comprehensive work covering duties and liabilities of CPAs, Denzil Y. Causey Jr., lists three sources that generate the determinants of a CPA's responsibility:

1. Specific contractual obligations undertaken,
2. Statutes and the common law governing the conduct and responsibility of public accountants, and
3. Requirements of voluntary professional organizations.

An objective of his book is met admirably as Causey develops "emerging patterns of civil and criminal liability of public accountants" and "a discussion of relevant auditing standards and procedures." One of his motivating factors was that "since the early 1960s there has been a great increase in litigation concerning the legal responsibility of professional persons, particularly public accountants."

In developing his approach, Causey splits "legal responsibility" into several types of liability, which seems pertinent to this study on computer fraud and the CPA. Depending upon the circumstances involved in any given case or incident, litigation action may be initiated that would require determination of a CPA's:

Liability to clients
Liability to third parties at common law
Civil liability under federal securities law, or
Criminal liability

He states that the "auditor can no longer achieve a comfortable sense of security by proclaiming that an annual audit is not designed or intended to detect fraud." Causey chooses to deal with the "auditor's duty to discover fraud when making an audit" under the classification

of Liability to Clients. Though he uses extensive footnotes for reference to court cases and presents a number of "briefs" in a part of the book, none could be found that actually pertain to the use of a computer to perpetrate fraud. Here, in part, is what he had to say:

> . . . . Some of the AICPA statements on auditing procedure originated within the auditing profession and some without. These procedures are constantly changing because the environment is changing and expectations of performance are rising . . . .
>
> An auditor is not a guarantor, and an audit cannot be relied upon to discover fraud, especially where it does not materially affect financial position. But if the auditor's negligence prevents his discovery of fraud and results in losses which could, by the discovery, have been prevented, the auditor may be liable. Even if such further losses cannot be shown, it has been held that the client can recover the fee paid for the negligent audit.
>
> The lack of due care or negligence can be based on failure to adhere to a specific or implied duty as to auditing procedures which would have disclosed either the fraudulent practice or the consequential misrepresentation in financial condition. An engagement to do an audit implies duties to . . . generally adhere to accepted professional standards.[26]

Further substantiation of the CPA's obligation for adherence to professional standards is available from authoritative law references.

> Although an accountant may be held liable to his client for either fraud or negligence in the preparation of financial statements, as well as for breach of contract, a distinction is generally made, in suits by relying third parties, between actions for negligence and for fraud . . . .

---

[26]Denzil Y. Causey, Jr., Duties and Liabilities of the CPA (Studies in Accounting No. 5) (Austin: University of Texas, Bureau of Business Research, 1973), pp. xv, xvii, 4, 14, 17.

> In the area of accountants' third-party liability, it appears that three basic issues remain unresolved: (1) whether an accountant generally may be held liable to a relying party, absent privity of contract, for negligence in the preparation of financial statements; (2) if so, within what limits of foreseeability; and (3) what relationship exists between gross negligence and fraud in the preparation of accountants' reports.
>
> In the light of these arguments, it is submitted that public policy would best be served by imposing on accountants liability in negligence to reliant third parties, but limiting the bounds of liability to a group more restricted than that of all persons foreseeably injured. The most appropriate element of actionable negligence with which to achieve this aim seems to be that of duty.[27]

As described earlier, auditing, since the turn of the century, has progressed through several eras and has generated a number of landmark/milestone activities and events that were either transitional or evolutionary in building generally accepted sets of auditing standards and auditing procedures. These have all served to help establish auditing as truly professional in nature, even though there is not universal recognition and acceptance of the auditing objectives, standards, and procedures.

In a typical engagement a CPA's responsibility rests upon the contract provisions, common and public law, and professional standards. Causey and others summarize the CPA's professional, legal and moral responsibility quite well--accomplish the engagement as any prudent, reasonable, typically competent and qualified auditor would--with primary regard to competence and to avoiding negligence. What is true

---

[27] Jack W. Shaw, Jr., "Liability of Public Accountant to Third Parties," ALR Digests (Annotation), 46 ALR 3d 979.

for an engagement in general would seem true also for an engagement involving an audit of a computerized accounting system.

A problem remains, however, in that the auditing profession's view and the public's view of the responsibility for the prevention and detection of fraud do not necessarily coincide. This question was considered at a 1974 symposium on auditing problems. Selected comments therefrom reflect the trend of thinking in the current Conflict and Uncertainty era as well as summarizing the view considered in this chapter.

George R. Catlett of Arthur Andersen & Company discussed the nature of fraud, responsibilities of management, auditing standards, internal control, representations by clients, and selected pertinent questions. In part, Catlett had this to say:

> The accounting profession is facing a wide diversity of difficult challenges. One of the current problems facing CPAs in public practice is how to achieve a proper understanding on the part of the public and others of (1) the relationship of auditing standards to the detection of fraud, and (2) the responsibilities of auditors for the detection of fraud . . . .
>
> Legal liability of independent auditors for alleged negligence and other deficiencies in their work has many ramifications. . . . The number of court cases involving the question of whether and under what circumstances an auditor may have legal liability is still somewhat limited; but more such cases will probably go to trial in the next few years, and the guidelines may become clearer than they are at the present time . . . .
>
> . . . . Are the present standards satisfactory? Have we learned as much as we should have from our experiences? Have the fraud situations gone undetected by auditors because of ineffective work or inadequate auditing standards; or has the cause been fraudulent concealment by management or other actions not detectable by normally appropriate auditing procedures? . . .

> The greater use of electronic computers and all sorts of sophisticated equipment for accounting and related purposes also represents new challenges in developing audit techniques. Some of the basic concepts of auditing may be changed. However, the standards of auditing should not be thwarted by equipment. People, not machines, commit fraud (emphasis added) . . . .
>
> Most of the significant fraud cases publicized in the financial press are the result of a breakdown in internal control as a result of management direction, collusion of officers and/or employees, deterioration of internal control from neglect, or a combination of these and similar factors. . . .
>
> Auditors do have responsibilities in the conduct of an audit, but these responsibilities do not include infallibility or clairvoyance. . . . An auditor should not be held responsible when he follows customary auditing procedures, those procedures do not disclose the deception, and no apparent reason exists to expand the customary audit procedures . . . .[28]

---

[28]George R. Catlett, "Relationship of Auditing Standards to Detection of Fraud," Contemporary Auditing Problems (Proceedings of the 1974 Arthur Andersen/University of Kansas Symposium on Auditing Problems), edited by Howard F. Stettler (Lawrence: University of Kansas, May 9 and 10, 1974), pp. 47-65. (Contents were not copyrighted and permission was granted to reproduce or quote from material included therein in whole or part provided full and proper credit given.)

CHAPTER 7

COMPUTER FRAUD: SEARCH FOR A SOLUTION

The primary objectives of this research effort were as follows: to determine the extent of computer fraud; to ascertain the reasons for its occurrence and how it was discovered in each case; to study each case in an effort to uncover weaknesses in auditing procedures; to examine the characteristics of a computer environment and computer fraud in relation to auditing procedures and generally accepted auditing standards; and, to re-assess the question of the auditor's degree of responsibility for the prevention and detection of fraud in a computer environment.

Emphasis was placed on trying to determine the risk of computer fraud exposure for the CPA in his audit (attest) function and on evaluating the auditing profession's acknowledgement of the computer in terms of auditing standards and accepted responsibility. However, the original, and still the chief, hypothesis of this study is that the CPA has a greater degree of responsibility for the prevention and detection of computer fraud than the auditing profession currently accepts in its expression of auditing standards relating to the subject of fraud.

Persons both inside and outside the auditing profession have presented questions similar to the central hypothesis of this study. The frequency of all fraud--not just computer fraud--has caused concern in many sectors. Business Week noted the AICPA's creation of a

seven-member commission "to study the gap between what the public expects from auditors and what CPAs can accomplish." In the reporter's words the AICPA was "smarting over growing public criticism of auditors' performance in detecting fraudulent corporate practices." The same may well be said of computer fraud if nothing is done to overcome the frightening potential in cases where the CPA does not detect such fraud when it exists. Accordingly, the task of the commission to "consider whether auditors should assume responsibility for all public financial information and whether existing procedures for setting audit standards are adequate"[1] is pertinent to the central hypothesis of this study.

In a May 1975 Journal article, a more definitive list of the major issues is presented as well as a more official description of the commission's charge. The latter is defined as being "to study the independent auditor's role, to identify the needs and expectations of users of financial statements and to recommend any changes necessary to assure that the auditors discharge their responsibilities."

The major issues that have "been identified by the seven-member, blue-ribbon study group" are as follows:

> The role of the independent auditor in the American economy
> The gap between the performance of independent auditors and the needs and expectations of users of audited financial statements

---

[1] Business Week, October 12, 1974, p. 35. The membership of the commission is presented in The CPA Letter, October 14, 1974, p. 2, and in other media. The Commission is chaired by Manuel F. Cohen and includes Walter S. Holmes, Jr., CPA; LeRoy Layton, CPA; William C. Norby; Prof. Lee J. Seidler, CPA; Kenneth Stringer, CPA, and John J. van Benten, CPA.

The auditor's responsibility in judging the "fair presentation" of financial statements and the role of "generally accepted accounting principles" in that judgment process

The responsibility of the auditor for detecting fraud

The auditor's role in evaluating the effect on financial statements, including the adequacy of disclosure, of uncertainties concerning the outcome of future events

The possibility of extending the auditor's role in reporting on new forms of information, such as interim information (including the auditor of record concept), and in reporting on other activities and characteristics, such as the efficiency of operations or the adequacy of internal control systems.

The responsibility of the auditor to detect adverse management behavior and disclose known adverse behavior to interested parties

The role of the auditor's report in communicating with users of financial information and possibilities for improving communication

The effectiveness of auditing methods and techniques and possibilities for improving effectiveness

The effectiveness of the present process for establishing auditing standards and possible ways of making that process more effective or efficient

The relationship of the independent auditor to investors, creditors, the board of directors and its audit committee, management and other interested parties, and the nature and extent of the auditor's responsibilities to those various parties

The effectiveness of present policies and procedures for maintaining the quality of audit practice, and the desirability of increasing information available to the public concerning a firm's quality review practices and other information that might bear on public confidence

The effectiveness of the present organizational structure of the auditing profession for regulating the practice of auditing and the possibilities for improving that structure

The effectiveness of the present process for establishing and administering procedures for recognizing individuals as qualified to practice as independent auditors, including the educational process, and the possibilities for improving that process

The effect of nonauditing services, such as management services or tax practice, on the audit function and the possible need for restrictions on those services

The effect of the present process for litigating claims against auditors and the possibility and desirability of changes in that process.

Although all of the issues are pertinent to this study, the issue concerning "the responsibility of the auditor for detecting fraud"[2] is of primary importance.

In the determination of the extent of computer fraud, there are some loopholes and something less than complete agreement. Computer fraud was no doubt perpetrated shortly after the first inventory and payroll applications were computerized but there was no organized research until 1971, when studies relating to computer abuse began. This author's research effort utilizes the 150 computer abuse cases uncovered by Donn B. Parker of the Stanford Research Institute. Such cases occurred over the 1964-1973 period but only 96 were reported as being within the business sector. It should be noted that in mid-1974, Parker had assembled in excess of 200 computer abuse cases and was adding a new case about every two weeks.

Whereas Parker reported six financial fraud computer cases for 1970 among a total of twelve abuse cases in which the total loss was $10,920,000, estimates by the Chamber of Commerce now reach $100 million annually for computer crime. The latter agency noted that dollar loss per incident of computer-related crime reached as high as $5 million. Numerous authorities, including Parker, admit that at least 20 percent of the cases are not detected and as many as 85 percent of the cases go unreported.

Although this author's research uncovered six agencies that

---

[2] Journal of Accountancy, May 1975, p. 26.

had established reporting systems for the collection and dissemination of information about fraud cases, none had the declared objective of being in support of the CPA or any of his professional organizations. Accordingly, the only reasonable and economical avenue open was to use case material from Stanford Research Institute even though that research effort was directed toward "computer abuse" incidents rather than "computer fraud" cases. Although crime statistics for several classes of fraud are available in the FBI's annual Uniform Crime Report and in the U.S. Department of Justice publication, Criminal Justice Statistics, they do not serve as useful measures for the purpose of this study.

The literature on computer fraud seems scarce, or spotty at best, among all that has been written separately about auditing and EDP. The term "computer fraud" seems to have been first coined in 1969 when several articles by different authors were published. Since 1971 there has been an increasing stream of articles and books that include computer fraud as a topic under the more general heading computer security. The AICPA has seemed to lag in bringing such literature to the attention of the CPA profession. Cardwell and others have commented on the dearth of published material available through AICPA resources.

The extent of computer fraud cannot be determined with even a fair degree of accuracy. The records maintained by interested persons or agencies are fragmentary and generally reflect special interests or segments. The news media seem to have a tendency to

report only the sensational cases. Article and book publications also seem to focus on the cases that have already received much attention in the news media. There are only a few--probably less than a dozen--active researchers working in the computer fraud area. In large part, the deficiencies in the knowledge about the extent of computer fraud result from the fact that there is no central respected, trustworthy entity engaged in the collection, coordination, and dissemination of computer fraud information on a "need to know" basis.

In ascertaining the reasons for computer fraud occurrence and how it was discovered in each case, it was necessary to rely upon the results of Parker's research on computer abuse.

> Perpetrators are white-collar amateurs rather than emotional or professional criminals. Few women have been encountered . . . . Most perpetrators are 18 to 30 years old . . . . Just the challenge of penetrating systems is attractive to many programmers . . . . Most perpetrators have rationalized part or all of their acts . . . [and] often tend to deviate in only small ways from the accepted and common practices of their associates . . . . Another commonly found rationalization is the Robin Hood argument. Perpetrators tend to differentiate between doing harm to individual people, which is immoral, and doing harm to organizations, which they believe is not immoral in certain circumstances . . . . Among traditional motivating forces in crime, the challenge aspect seems to be much stronger in computer-related acts. . . . It appears that perpetrators strongly fear unanticipated detection and exposure. This makes detection as a means of protection at least as important as deterrence and prevention.[3]

Parker also noted that "few among the discovered and reported cases were those detected by persons directly responsible for detection,

---

[3]Donn B. Parker et al., Computer Abuse (Menlo Park, CA: Stanford Research Institute, 1973), pp. 49-51.

such as security officers or EDP auditors." In fact, he observed that "discovery was usually accidental and resulted from the curiosity of programming, marketing, or operations staff about unusual activities."[4] Numerous other authors, as indicated in evidential discussion presented earlier in this study, have also commented on the fact that nearly all cases have been discovered by accident. Of equal concern is the frequent observation in print on the lack of auditor involvement in the detection. There appears to be a generally recognized need for some entity to accept a role for the prevention, detection, and investigation of computer fraud.

It was not possible to study each computer fraud case in an effort to uncover weaknesses in auditing procedures. The questionnaire used by Parker was not designed so as to gather any information about auditor involvement in any way. As a consequence, the following information items that had been contemplated as necessary in fulfilling the objectives of this author's research were not captured in connection with the computer fraud cases:

Amount of recovery via fidelity bond insurance

Professional liability insurance claims awarded

Court-awarded damage or recovery claims

Role of the CPA (if any) in connection with the case

Weaknesses in auditing procedures

Weaknesses in internal control

---

[4]Parker, p. 53.

All of the above information items would seem to be of vital importance in drawing the complete picture and circumstances of any computer fraud case. Certainly any CPA would be deficient if he did not recognize weaknesses in internal control in circumstances in which computer fraud existed. The CPA could be open to a charge of negligence if he permitted weaknesses in auditing procedures in any audit engagement which immediately preceded the discovery of computer fraud in his clients' facilities.

In the examination of the characteristics of a computer environment and computer fraud in relation to auditing procedures and generally accepted auditing standards, the diversity of the subject matter and coverage required that the several facets be examined separately. Accordingly, the development of accounting systems, data processing, computer and communications technology, and auditing adaptations to these changes in the business environment was traced in earlier discussions in this study. Briefly, it was determined that auditing procedures were altered as a matter of practical necessity when a computer was introduced. Legal definitions as well as technical methods of computer fraud were developed in the earlier discussions. Generally accepted auditing standards seem to have stood the test of time. Rather, however, these standards relate to skills, knowledge and performance; thus as the environment and technology change the interpretation of the appropriate level or standard for possessing these attributes changes.

As reported in an earlier chapter, the Equity Funding case of

computer fraud was reported in early 1973. Shortly thereafter, the AICPA appointed a special committee which "understood its charge to require appraisal not only of the ten standards, but more particularly of the auditing procedures by means of which auditing standards are implemented."

Even though much discussion could be engendered in connection with related aspects of this author's research, only a few points need to be reiterated here. The committee found that, "except for certain observations relating to confirmation of insurance in force and auditing related party transactions, generally accepted auditing standards are adequate and that no changes are called for in the procedures commonly used by auditors." The committee also reported that in its opinion:

> A knowledge of computer audit techniques was not essential to the detection of the Equity Funding fraud. Manual application of customary auditing procedures would have provided a reasonable degree of assurance that the fraud would be uncovered.
>
> The fraud did not contain any elements that involved new or unique computer applications. Thus no recommendations are made for any new auditing standards or procedures in regard to computer maintained financial records.
>
> . . . the auditor has an obligation to discover material (emphasis added) frauds that are discoverable through application of customary auditing procedures applied in accordance with generally accepted auditing standards. The auditing profession should, on an on-going basis, continue to improve the efficiency of customary audit procedures to the end that probability of discovery of material (emphasis added) frauds continues to increase within the limits of practicability.

The committee generally limited its review to the events of 1971 and 1972 even though it appears that the fraud began as early as 1964 and did extend into 1973. It also spent some time in considering

degrees of the term "massive" but concluded that "there is no definable degree of massiveness as to which such an audit can invariably be relied upon for such detection." On the one hand the review seems to avoid the question of why fraud went undetected for nine years--even through changes of auditors. On the other hand, its concern with the term "massive" seems to be more in response to the use of that term by news media than an objective analysis in regard to a CPA's responsibility for the detection of fraud.[5]

It seems fairly clear that computer auditing procedures have not had a chance to stabilize primarily due to the rapidly advancing computer technology, which has been described elsewhere in this study. The continuous pressure for more sophisticated computer systems has caused an almost complete disarray in the understanding of, and in implementing, internal control systems. Thus, from the CPA viewpoint, there is little standardization, and compliance testing of internal control in a computer system requires the creative genius of a systems designer and the expertise of a high qualified statistician, if the requirements of Statement on Auditing Standards No. 1 are to be properly met.

Although the eras of auditing evolution can be extended back to at least the 19th century, the concept of internal control actually

---

[5] Report of the Special Committee on Equity Funding (New York, NY: American Institute of Certified Public Accountants, 1975), pp. 6-7, 9, 27, 34, 38-39.

dates officially from 1949 when the AICPA issued a pronouncement in the form of a bulletin devoted only to that subject matter. Cardwell, Boutell and other authors writing in the interim have called attention to weaknesses in internal control systems and their application. The deficiencies have not been overcome as is evident by Robert K. Mautz's observation that "both intellectually and practically it is one of the most intractable problems I know." He declares that "we must learn how to analyze and evaluate the strengths and weaknesses of the internal control systems of all the various kinds of enterprises and organizations with which auditors must deal" and that "we must establish standards of performance for the review and testing of internal control that can be applied effectively under the conditions in which audits must be performed, conditions which call for time and cost constraints."[6]

With the introduction of the computer into the auditing environment and the adoption of the "audit around" approach it soon became apparent that this resulted in less than full reliance on the internal control system. Much data were invisible and as a consequence many files were not sampled or tested in any way. This led to the "audit through" the computer approach. However, again shortcomings were soon noted. The major difficulty was that this "test deck" approach tended to contaminate files yet did not provide the capability to

---

[6]Robert K. Mautz, "The Case for Professional Education in Accounting," Schools of Accountancy: A Look at the Issues (Proceedings of a Symposium), edited by Allen H. Bizzell and Kermit D. Larson and published by American Institute of Certified Public Accountants, 1975, p. 32.

perform all necessary audit tests. The "audit with" the computer approach was aimed at giving the auditor a tool or technique that could be utilized with minimum data processing skill or knowledge. As noted in Chapter 1, the search for a solution resulted in the development of generalized computer audit programs.

The "pure" generalized computer audit programs are few in number. A survey was made to determine the extent of their availability.[7] Most of the initial programs in this category appear to have been created and developed by CPA firms. There are probably less than a dozen software companies that could qualify as specialists in generalized computer audit programs. The most widely reported computer audit programs (or program packages) are listed in Table 7-1.

The outlook may improve as more software firms become aware of the demand for generalized computer audit programs by the typical, traditional CPA who wishes to make the transition to the computer. Also, edging into this market are generalized packages for file management systems, information retrieval systems, edit program generators, and report program generators, all of which are incorporating capabilities that could satisfy certain audit functions.

The typical and traditional CPA faces some serious problems in trying to cope with EDP systems. The CPA is not a computer expert. There is still a great deal of secrecy and a lack of communication in

---

[7]See Appendix C for summaries of selected computer programs for auditors and Appendix D for the details concerning recipients and responses for the survey related to generalized audit programs.

TABLE 7-1

GENERALIZED COMPUTER AUDIT PROGRAMS/PACKAGES

Name	Company	Approximate Date of First Use
ASK 360	Murray and McLintock (UK)	1968
AUDASSIST	Alexander Grant and Co.	1965
AUDEX	Arthur Andersen and Co.	1969
AUDIT ANALYZER	Program Products, Inc.	1973
AUDITAPE	Haskins & Sells	1965
AUDITPAK	Lybrand, Ross Bros, & Montgomery	1968
AUDITRONIC	Ernst & Ernst	1968
AUDIT-SOURCE CODE COMPARE	IBM	1975
AUDIT-THRU	Computer Resources Corp.	1968
AYAMS	Arthur Young & Co.	1968
CARS	Computer Audit Systems	1967
COMPUTER FILE ANALYZER	Price Waterhouse & Co.	1970
DYL-250	Dylakor Computer Systems, Inc.	1970
DYL-260	Dylakor Computer Systems, Inc.	1972
EASYTRIEVE	Pansophic Systems, Inc.	1974
EDP AUDITOR	Cullinane Corporation	1970
FIND	International Computers (UK)	1966
GRS	Program Products, Inc.	1968
HEWCAS	Dept. of Health, Education, and Welfare	1972
MARGEN	Randolph Computer Corporation	1968
MARK IV FILE MANAGEMENT SYSTEM	Informatics, Inc.	1968
MIRACL	Republic Software Products	1968
NITA	National Computer Centre (UK)	1967
PANVALET	Pansophic Systems, Inc.	1974
PW CALL	Price Waterhouse & Co.	1968
RSVP	National Computing Industries	1968
SCORE	Programming Methods, Inc.	1968
STRATA	Touche Ross & Co.	1968
SYSTEM 2170	Peat, Marwick, Mitchell & Co.	1968
TRAP	Touche Ross & Co.	1968

NOTE: Approximate date of first use is either estimated or deduced from documentary evidence that was available from the various sources.

SOURCE: Auditing by Computer Study Group, Proceedings of Symposium on Computer Audit Packages, Saddlers' Hall, London, England, April 9, 1970, Institute of Chartered Accountants in England and Wales; Charles R. Wagner, A CPA's Search for a Generalized

the auditing field in relation to EDP techniques and programs--due, in part, to the "independence" standard; in part, to the constraints on advertising; and, in part, to the desire to retain proprietary benefits.

In the search for a solution to computer fraud and the CPA's responsibility, the AICPA's position on education, qualifications to enter the profession, and standards related to EDP systems is of utmost importance. Recently Guy Trump, AICPA Vice President, re-affirmed the Institute's position by noting that the "AICPA's present position was established in 1969 by the Committee on Education and Experience Requirements for CPAs (the Beamer Committee.)" He stated further that "Horizons for a Profession is an authoritative description of the common body of knowledge for beginning CPAs."[8]

As noted in an earlier chapter, auditing texts seem to neglect or minimize the EDP coverage. This has been reiterated and re-emphasized by both the AICPA and the American Accounting Association. A task force of educators from each of these organizations developed

---

SOURCE (continued): Audit Program, unpublished research project, 1971; Donald L. Adams and John F. Mullarkey, "A Survey of Audit Software," Journal of Accountancy, September 1972, pp. 39-66; Footnote, Department of Health, Education, and Welfare, May 1975 issue devoted entirely to articles on HEWCAS; letter from Program Products, Inc., April 1974; "Auditability," Data Processor, June 1975, pp. 13-14; Donald L. Adams, "Audit Software-DYL-250 and DYL-260," EDPACS, July 1974, pp. 7-11; Jan Snyders, "Runs for Your Money," Computer Decisions (Software for Sale), August 1975, pp. 16-17.

[8]Guy Trump, "Attributes of a New (Public) Accountant," Accounting Education: Problems and Prospects, edited by James Don Edwards and published by American Accounting Association, 1974, pp. 60-66.

an article which was published initially in the Accounting Review.[9] It noted that "three leading textbooks devote only 44 pages, 18 pages and 17 pages to EDP auditing" and in addition to this limited coverage the subject is not integrated or related to the many topics covered in the auditing curriculum.

The authors recognize the need for students to become knowledgeable about computers in all facets of auditing. Their "article describes how EDP auditing topics can be introduced as part of the discussion of such classic subjects as auditor's technical proficiency, auditing standards, review of internal control and the audit of balance sheet and income and expense accounts." The task force delineated five topics which should be included as a minimum. These were as follows:

1. EDP technical proficiency requirements for the staff auditor
2. The review, evalution and study of internal control in an EDP environment
3. Auditing a computer system without using a computer
4. Using the computer to perform compliance and substantive tests of the records produced by a computer system
5. Auditing data processing records produced by a computer service center

The reader may well note that these topics are similar to those advocated in the Common Body of Knowledge (CBOK) study and in the Beamer recommendations. The fact that five and more years later the

---

[9]This author was asked to review and comment on the proposed article.

situation in regard to the auditor's preparedness for computer auditing seems little changed could be a major reason for the frequency of occurrence of computer fraud (abuse) cases. As observed in the article "education in the classroom should reflect the changes in the profession."[10]

Since it has been the practice to limit the number of practicing CPAs trained in the art of EDP auditing, the profession must be presuming that the beginning CPAs will have that breadth of knowledge. If beginning CPAs do not meet the CBOK requirements, and that seems to be the only logical conclusion that can be reasonably drawn, then the auditing profession must feel the pressure of increasing risk of computer fraud exposure. After all, numbers of computers and terminals are increasing but numbers of CPAs that can "cope with" the changed environment and controls are not keeping pace.

AICPA's EDP Task Force, headed by Everett C. Johnson, has prepared "a preliminary paper on matters that should be considered in designing and developing advanced EDP systems to ensure that they meet management's needs and audit requirements for both large and small companies." The position taken by that task force is supportive of the views presented or suggested in this study. Thus, the search for a solution to computer fraud and a CPA's responsibility continues even though the pertinent parameters may not be defined completely.

---

[10]"Inclusion of EDP in an Undergraduate Auditing Curriculum," Journal of Accountancy (Education), December 1974, pp. 118-21.

The task force has predicted that the audit (attest) function will be impacted for the following reasons:

> As computers are applied to more and more functions, internal control techniques may be inadequate. Guidelines and standards must be developed.
>
> Traditional documents and magnetic data that now comprise the audit trail may not be present in advanced systems. Alternative approaches will be required.
>
> The auditor must be sure that the system subject to the audit test is actually the same one that is used to produce financial statements.
>
> Auditors will have to anticipate the impact of new computer hardware and software developments on accounting records and will have to modify their audit techniques accordingly.
>
> Despite the complexity of advanced systems, the audit must be performed at a reasonable cost.[11]

Few authors have attempted any analysis in regard to risk and/or exposure ratings connected with computer fraud. Several mention the need to estimate theft, fidelity, and fire insurance coverage. Two works described in narrative form the concept and some factors to consider in making such a cost/benefit/risk analysis covering computer security.[12]

James Martin devoted an entire chapter to the subject of "security exposure." In his coverage, Martin warns that "the

---

[11] The CPA Letter, November 11, 1974, p. 2.

[12] See Security Standards for Data Processing by Susan Wooldridge, Colin Corder and Claude Johnson (New York, NY: John Wiley & Sons, 1973), pp. 9-17; and, Security for Computer Systems by M. A. L. Farr, B. Chadwick, and K. K. Wong (Manchester, England: NCC Publications, 1972), pp. 23-31.

probability can be estimated only very approximately" and that "the cost can be estimated only vaguely in many cases," and presents two mathematical models that determine the exposure in terms of a "quantitative rating . . . that corresponds to the probable average damage per year."

According to Martin, protection is needed to cover: "acts of God, hardware and program failure, human carelessness, malicious damage, crime, and invasion of privacy." These factors are aligned in column and row matrix form in combination with the results that are possible: "loss of single records, modifications of records, loss of an entire file, loss of ability to process a file, and unauthorized reading or copying of records."

A probability rating is then assigned, where applicable, at the intersections in accordance with the following code and event frequencies:

0: Virtually impossible
1: Might happen once in 400 years
2: Might happen once in 40 years
3: Might happen in 4 years (1000 working days)
4: Might happen once in 100 working days
5: Might happen once in 10 working days
6: Might happen once a day
7: Might happen 10 times a day

The damage assessment is in terms of "lost business, cost of correcting the data, and other costs" and is determined from the following code and dollar values:

0: Negligible (about $1)
1: On the order of $10
2: On the order of $100
3: On the order of $1,000
4: On the order of $10,000

5: On the order of $100,000
6: On the order of $1,000,000
7: On the order of $10,000,000

Using appropriate probability and damage rating inputs in the formulas, which was given as $E = 10^{(P+D-3)} \div 4$, gives dollars per year. Martin's other formula is given as Estimate ($) = Damage an event causes ($) ÷ Mean time between events occurring (years).[13]

Perhaps an adaptation of the formula suggested and used by the Surety Association of America would also be useful in determining a CPA's computer fraud exposure index. The referenced formula, Dishonesty Exposure Index, is explained by Pratt and apparently is of long standing. The Index is calculated by applying specified percentages to Current Assets less Goods on Hand, to Goods on Hand, and to Annual Gross Sales or Income and deriving a total thereof.[14] However, in order to accomplish this, such data would have to be captured for those firms having computers and/or terminals.

The risk of a computer fraud incident being perpetrated in any given computer installation--regardless of the system's simplicity or complexity--is determined by several factors which can be reduced to essentially two variables. One of these is a computer fraud exposure index: a relationship between the number of people having the

---

[13]James Martin, Security, Accuracy, and Privacy in Computer Systems (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1973), pp. 11-16.

[14]Lester A. Pratt, Embezzlement Controls for Business Enterprises (Baltimore, MD: Fidelity and Deposit Company, 1952), pp. 29-31.

requisite knowledge and access to a computer and the number of entry points into that computer system. The other is what might be called vulnerability: the degree of controls and/or security within the computer system.

The CPA's computer fraud exposure index as conceived in Chapter 5 is similar to that described above except that the number of business firms becomes a factor. The CPA becomes "vulnerable" to the extent that he reviews the controls and/or security within the computer system and does not find computer fraud when in actual fact it exists.

With only 96 computer abuse cases having been reported for all business sectors over the period from 1964 to 1973, the probability of a CPA having encountered computer fraud on any given audit engagement seems practically negligible. However, that does not mean that further work on the conceptual and mathematical models for determination of an index of a CPA's exposure to computer fraud should be terminated. Rather, as noted in Chapter 5, refinement of the definition of the parameters should be accomplished. Perhaps equally important would be the development of a respected, trustworthy entity that could centralize collection, coordination, and dissemination of computer fraud information on a "need to know" basis.

The Institute of Internal Auditors has joined in the search for a solution to computer fraud and the determination of auditing responsibility by recognizing the need to improve EDP audit effectiveness. William E. Perry, Director of Research, observed that "the controls and documentation not built into computer applications during

the 1960s and early 1970s are starting to pose problems for organizations." In referring to problems not being caught by existing controls, Perry notes the increase in the number of incidents and calls "equally alarming . . . the associated problem that cases involving fraud and invasion of privacy are not being caught by existing controls. Those incidents being uncovered are normally exposed by third parties." Over 40 IIA chapters have established EDP Auditing Committees[15] in recognition of the fact that this is a multifaceted and very complicated problem.[16]

Perry has been instrumental in initiating research studies also aimed at improving EDP audit effectiveness. One of these is a 1974 Survey of Internal Auditing from which a report covering (among other areas) EDP techniques will be issued. Another involves a project entitled "Foozles and Frauds" to be undertaken by Harold F. Russell.

The latter "project report will offer guidance on how to handle suspected cases of fraud, discuss the legal implications of fraud, provide guidance on how to interrogate an individual suspected of fraud, discuss the internal auditor's responsibility in regard to fraud, review several major frauds or foozles as a means of illustrating why and where controls break down, and recommend ways to strengthen controls."[17]

---

[15]This author was appointed to the newly created EDP Auditing Commitee of the Omaha Chapter in December 1974 and has been reappointed to that same committee for the 1975-1976 year.

[16]Auditing News, February 1975, p. 6.

[17]Auditing News, October 1974, p. 3.

Another tremendously important research study has been launched and will be funded by a $500,000 grant from the International Business Machines Corporation. A contract has been signed with the Stanford Research Institute to do extensive field research to bring together the best-known control and audit techniques for organizations using computers. The objective is "to survey the state of the art in the areas of auditing and control of computer-based systems and computer related applications to develop practical, solution-oriented guidelines, approaches and techniques for use by management, data processing and internal auditing personnel."[18]

Since the discussion in this chapter has centered on the search for a solution to computer fraud and the determination of the CPA's responsibility for its prevention and detection, it is appropriate to summarize the conclusions reached prior to making recommendations for a way out of the present dilemma. The evidence accumulated in fulfilling the research objectives supports the following views:

1. No organized reporting system adequately covers all sectors of the business environment; therefore, computer fraud data is fragmentary.

2. Frequency and scope of occurrences of computer fraud within computer systems of CPA clients are not known.

3. The incidence of employee dishonesty--including computer crime and other white-collar crime--appears to be rising in frequency and dollar amounts.

---

[18] Auditing News, April 1975, pp. 1, 3. See also, Journal of Systems Management, May 1975, p. 6; and Auditing News, October 1975, p. 2.

4. Internal control systems encompassing EDP facilities do not provide preventive barriers to computer fraud perpetrators.

5. The lack of auditor involvement in computer fraud detection conflicts with the public's view of audit objectives.

6. The accountant/auditor who has been the acknowledged accounting (information system) specialist for nearly five centuries may be in danger of losing that recognition.

Although it is recognized that the above views constitute arguments of a negative nature, they no less fully support the chief hypothesis of this study. It seems clear that the CPA is not fulfilling his obligation to society as an accountant/auditor professional. Accordingly, in positive form then, the CPA has a greater degree of responsibility for the prevention and detection of computer fraud than the auditing profession currently accepts in its expression of auditing standards relating to the subject of fraud.

Since there is no easy route to the enlargement of the CPA's responsibility, it should be approached cautiously. This research did not incorporate an analysis or study of changes that could be made in the actual enlargement of the CPA's responsibility for the prevention and detection of computer fraud. Rather, even though two recommendations surface easily as a result of research findings, they are intended as steps or measures in making changes to accomplish the transition to different levels of a CPA's responsibility.

First, a study should be initiated to determine the feasibility of establishing a computerized information retrieval system for

computer fraud cases. It would appear that the accounting profession already has the expertise to accomplish this since the National Automated Accounting Research System (NAARS)[19] has been recently implemented. The data collection and retrieval system might well employ a network consisting of the state boards of accountancy and/or state societies of CPAs as local input and data bank monitors. Such a system should provide confidentiality while preserving privacy rights yet offer the opportunity for a complete, comprehensive data bank on the computer fraud cases.

Second, a study should be initiated to determine the feasibility of expanding the scope of services offered by CPA firms to include computer fraud detection. Just as management advisory services and tax work are now kept separate from the audit (attest) function so might computer fraud detection service be marketed to client firms. The chief premise here is that it should be much easier to convince the appropriate "publics" that computer fraud detection service is available separately at a certain fee than it is to convince the same "publics" that "the ordinary examination directed to the expression of an opinion on financial statements is not primarily or specifically designed, and cannot be relied upon, to disclose defalcations and other similar irregularities

---

[19] NAARS is a full text system which permits multiple-term coordinate search capabilities in a real-time, interactive mode of operation. See NAARS brochure available from AICPA; also, "NAARS, Computerized Accounting and Auditing Research," by Willis Leonhardi in Arthur Andersen's The People, June 1975, pp. 46-49.

. . . [such as computer fraud], although their discovery may result."[20]

---

[20]See quotation referenced by footnote 15 in Chapter 6.

SELECTED BIBLIOGRAPHY

SELECTED BIBLIOGRAPHY*

AICPA PRONOUNCEMENTS/PUBLICATIONS

Accounting and the Computer. New York, NY: American Institute of Certified Public Accountants, 1966.

Accounting Objectives Study Group. Objectives of Financial Statements New York, NY: American Institute of Certified Public Accountants, October, 1973.

Auditing Standards Executive Committee. The Effects of EDP on the Auditor's Study and Evaluation of Internal Control. Statement on Auditing Standards 3. New York, NY: American Institute of Certified Public Accountants, Inc., December, 1974.

Bizzell, Allen H. and Kermit D. Larson (eds.). Schools of Accountancy: A Look at the Issues. Proceedings of a Symposium. New York, NY: American Institute of Certified Public Accountants, 1975.

Burton, John C. (ed.). Corporate Financial Reporting: Conflicts and Challenges. New York, NY: American Institute of Certified Public Accountants, 1969.

Burton, John C. (ed.). Corporate Financial Reporting: Ethical and Other Problems. New York, NY: American Institute of Certified Public Accountants, Inc., 1972.

Carey, John L. The CPA Plans for the Future. New York, NY: American Institute of Certified Public Accountants, Inc., 1965.

Carey, John L. The Rise of the Accounting Profession, From Technician to Professional, 1896-1936. New York, NY: American Institute of Certified Public Accountants, Inc., 1969.

Carey, John L. The Rise of the Accounting Profession, To Responsibility and Authority, 1937-1969. New York, NY: American Institute of Certified Public Accountants, Inc., 1970.

Committee on Auditing Procedure. Internal Control. New York, NY: American Institute of Accountants, 1949.

Committee on Auditing Procedure. Codification of Statements on Auditing Procedure. New York, NY: American Institute of Accountants, 1951.

---

*Entries for articles and books included in Tables 3-2, 3-3 and 3-4 in the textual material are not repeated in this bibliography.

Committee on Auditing Procedure. Generally Accepted Auditing Standards, Their Significance and Scope. New York, NY: American Institute of Certified Public Accountants, 1954.

Committee on Auditing Procedure. Statements on Auditing Procedure No. 33, Auditing Standards and Procedures. New York, NY: American Institute of Certified Public Accountants, 1963.

Committee on Auditing Procedure. Statement on Auditing Standards No. 1 (Codification of Auditing Standards and Procedures). New York, NY: American Institute of Certified Public Accountants, 1973.

Committee on Terminology. Accounting Terminology Bulletins, Number 1, Review and Resume. New York, NY: American Institute of Accountants, 1953.

Cramer, Joe J. Jr., and George H. Sarter (eds). Objectives of Financial Statements. Vol 2. Selected Papers. New York, NY: American Institute of Certified Public Accountants, 1974.

Designers of Order, The Story of Accountancy Briefly Told New York, NY: American Institute of Certified Public Accountants, 1970.

Kane, Robert L., Jr. (ed.). Duties of Junior and Senior Accountants. Supplement to the CPA Handbook. New York, NY: American Institute of Accountants, 1953.

Report of the Special Committee on Equity Funding, The Adequacy of Auditing Standards and Procedures Currently Applied in the Examination of Financial Statements. New York, NY: American Institute of Certified Public Accountants, Inc., 1975.

Rich, Wiley Daniel. Legal Responsibilities and Rights of Public Accountants. New York, NY: American Institute Publishing Company, Inc., 1935.

Roy, Robert H. and James H. MacNeill. Horizons for a Profession, The Common Body of Knowledge for Certified Public Accountants. New York, NY: American Institute of Certified Public Accountants, 1967.

ARTICLES

Adams, Donald L. "EDP Auditors vs EDP Personnel Survey." EDPACS, January 1974, pp. 13-14.

Alexander, Tom. "Waiting for the Great Computer Rip-Off." Fortune, July 1974, pp. 143-150.

"Audit Commission Lists Issues Under Study." Journal of Accountancy (Professional). May 1975, p. 26.

Bakay, Virginia Hicks. "A Review of Selected Claims Against CPAs." Journal of Accountancy, May 1970, pp. 54-58.

Barden, Horace G. "Discussants' Response to Some Historical Auditing Milestones; An Epistemology of an Inexact Art." Auditing Looks Ahead. Proceedings of the 1972 Touche Ross/University of Kansas Symposium on Auditing Problems. Edited by Howard F. Stettler, May 11 and 12, 1972, School of Business, University of Kansas, pp. 12-22.

Brown, R. Gene. "Changing Audit Objectives and Techniques." Accounting Review, October 1962, pp. 696-703. Reprinted in Perspectives in Auditing, Readings and Analysis Situations, by D. R. Carmichael and John J. Willingham. New York, NY: McGraw-Hill Book Company, 1971, pp. 2-13.

Brown, R. Gene and Roger H. Salquist. "Some Historical Auditing Milestones; An Epistemology of an Inexact Art." Auditing Looks Ahead. Proceedings of the 1972 Touche Ross/University of Kansas Symposium on Auditing Problems. Edited by Howard F. Stettler, May 11 and 12, 1972, School of Business, University of Kansas, pp. 1-11.

Burton, John C. "The SEC and the World of Accounting in 1974." Journal of Accountancy (statement in quotes), July 1974, pp. 59-60.

Catlett, George R. "Relationship of Auditing Standards to Detection of Fraud." Contemporary Auditing Problems. Proceedings of the 1974 Arthur Andersen/University of Kansas Symposium on Auditing Problems. Edited by Howard F. Stettler, May 9 and 10, 1974, School of Business, University of Kansas, pp. 47-56.

"Computer Fraud and Embezzlement." EDP Analyzer, September 1973, pp. 1-14.

Cutting, Richard E., Richard J. Guiltinan, Fred L. Lilly, Jr., and John F. Mullarkey. "Technical Proficiency for Auditing Computer Processed Accounting Records." Journal of Accountancy (Accounting and Auditing Problems), October 1971, pp. 74, 76, 78, 80, 82.

"Datacomm to Jump Fivefold in Decade." The Data Communications User (Datacomm Developments), May 1975, pp. 25-26.

"Data Communications Growing at 22.5% a Year." Data Communications (Newsfront), May/June 1975, p. 16.

"EDP Almanac 1642-1971." Data Management, January 1972, pp. 26-32.

Farmer, Jerome. "Auditing and the Computer--A Suggested Program." Journal of Accountancy, July 1970, pp. 53-56.

Fusco, G. P. "IBM Unifies Structure for Teleprocessing." The Data Communications User, December 1974, pp. 24-25.

Gilson, Milo. "Computer Assisted Fraud--Who Gets the Axe?" Data Management, April 1975, pp. 22-23.

Hill, Thomas W., Jr. "Accountants' Legal Liability." Independent Auditing Standards, A Book of Readings, edited by J. C. Ray. New York, NY: Holt, Rinehart and Winston, Inc., 1964. See also New York Certified Public Accountant, March 1959, pp. 177-88, and October 1959, pp. 707-723.

Horwitz, Geoffrey B. "EDP Auditing--The Coming of Age." Journal of Accountancy, August 1970, pp. 48-56.

"Inclusion of EDP in an Undergraduate Auditing Curriculum." Journal of Accountancy (Education), December 1974, pp. 118-21.

Johnson, James R. "The Changing DP Organization." Datamation, January 1975, pp. 81, 83.

Kadin, Morris B. and Robert Green. "Computerization in the Medium-Sized CPA Firm." Journal of Accountancy, February 1971, pp. 44-49.

Kuehn, Richard A. "Systems Planning and Control." The Data Communications User (Tutorial Handbook edition), December 1974, pp. 15-16, 18.

Leonhardi, Willis. "NAARS, Computerized Accounting and Auditing Research." The People (Arthur Andersen and Company), June 1975, pp. 46-49.

Mautz, Robert K. "The Case for Professional Education in Accounting." Schools of Accountancy: A Look at the Issues. Proceedings of a Symposium, edited by Allen H. Bizzell and Kermit D. Larson. New York, NY: American Institute of Certified Public Accountants, 1975.

Menkus, Belden. "Computerized Information Systems Are Vulnerable to Fraud and Embezzlement." Menkus on Management. Bergenfield, NJ: Belden Menkus, 1972, pp. 1-4.

"Microcomputers--Mind-Boggling Potential." Infosystems, June 1975, p. 54.

Milecke, Helen. "DPMA's 1973 Computer Sciences Man of the Year." Data Management, June 1973, pp. 14-20.

Neville, Haig. "Computer 'Capers' Herald New Crime Wave of Embezzlement." The National Underwriter (Property & Casualty Insurance Edition), August 20, 1971, pp. 1-2, 13.

Olson, Bruce P. "Controls and the Audit Trail." Data Processing, Volume VII. Proceedings of the 1964 International Data Processing Conference, June 23-26, 1964, New Orleans, LA. Data Processing Management Association, 1964.

Rohde, John Grant, Gary M. Whitsell, and Richard L. Kelsey. "An Analysis of Client-Industry Concentrations for Large Public Accounting Firms." Accounting Review, October 1974, pp. 772-787.

Roy, Robert H. and James H. MacNeill. "Study of the Common Body of Knowledge for CPAs." Journal of Accountancy, December 1963, pp. 56-57.

Ruskin, Vernon. W. "Comparing Computer Operations." Journal of Systems Management, December 1973, pp. 34-38.

Russell, Thomas F. "Critique of the Whitman and Flynn Papers." Corporate Financial Reporting: Conflicts and Challenges, edited by John C. Burton. New York, NY: American Institute of Certified Public Accountants, 1969, pp. 184-88.

Shaw, Jack W., Jr. "Liability of Public Accountant to Third Parties." ALR Digests (Annotation), 46 ALR ed 979.

Trump, Guy. "Attributes of a New (Public) Accountant." Accounting Education: Problems and Prospects, edited by James Don Edwards. Sarasota, Florida: American Accounting Association, 1974, pp. 60-66.

"Using Computers to Steal--Latest Twist in Crime." U.S. News & World Report, June 18, 1973, pp. 39-40, 42.

Voris, J. Walker. "The Computer and You, How the Computer Can Be Used to Commit Fraud." Practical Accountant, March/April 1975, pp. 63-64.

Wagner, Charles R. "Availability of Fraud Literature." Internal Auditor (Education), November/December 1973, pp. 79-85.

Webb, Richard. "Audassist." Journal of Accountancy, November 1970, pp. 53-58.

Weiss, Harold. "The Danger of Total Corporate Amnesia." Financial Executive, June 1969, pp. 63-64, 67-68.

Weissman, Clark. "Trade-Off Considerations in Security System Design." Computers and Management, 2d ed. by Donald H. Sanders. New York, NY: McGraw-Hill Book Company, 1974, pp. 470-81.

Wilkins, Barbara. "Sequel: How Jerry Schneider Took on Ma Bell, Won for a While, Then Lost and Wound Up Rich Anyhow." People, July 28, 1975, pp. 62-63.

Withington, Frederick G. "Beyond 1984: A Technology Forecast." Datamation, January 1975, pp. 54-57, 61, 63, 65, 67, 71, 73.

Zeff, Stephen A. and Robert L. Fossum. "An Analysis of Large Audit Clients." Accounting Review, April 1967, pp. 298-320.

Ziegler, John H. "Current Trends in the Teaching of Auditing." Accounting Review (Academic Notes), January 1972, pp. 169-70.

AUDITING (ACCOUNTING)

Baker, Roy E. Cases in Auditing with Supplemental Readings. Englewood Cliffs, NY: Prentice-Hall, Inc., 1969.

Bell, William H. and Ralph S. Johns. Auditing. 2d ed. New York, NY: Prentice-Hall, Inc., 1941.

Bell, William H. and Ralph S. Johns. Auditing. 3d ed. New York, NY: Prentice-Hall, Inc., 1952.

Bennett, George E. Fraud, Its Control Through Accounts. New York, NY: The Century Company, 1930.

Berlin, Bruce S. and Francis J. Walsh, Jr. Corporations and Their Outside Auditors. New York, NY: The Conference Board, 1972.

Boutell, Wayne S. Contemporary Auditing. Belmont, CA: Dickenson Publishing Company, Inc., 1970.

Briloff, Abraham J. Unaccountable Accounting. New York, NY: Harper and Row, Publishers, 1972.

Brink, Victor Z. and James A. Cashin. Internal Auditing. 2d ed. New York, NY: Ronald Press Company, 1958.

Brink, Victor Z., James A. Cashin, and Herbert Witt. Modern Internal Auditing: An Operational Approach. 3d ed. New York, NY: The Ronald Press Company, 1973.

Buckley, John W. and Marlene H. Buckley. The Accounting Profession. Los Angeles, CA: Melville Publishing Company, 1974.

Cadmus, Bradford. Operational Auditing Handbook. Orlando, Florida: The Institute of Internal Auditors, 1964.

Carmichael, D. R. and John J. Willingham. Perspectives in Auditing. New York, NY: McGraw-Hill Book Company, 1971.

Cashin, James A. Handbook for Auditors. New York, NY: McGraw-Hill Book Company, 1971.

Cashin, J. A. and G. C. Owens. Auditing. 2d ed. New York, NY: Ronald Press Company, 1963.

Causey, Denzil Y., Jr. Duties and Liabilities of the CPA (Studies in Accounting No. 5). Austin, Texas: Bureau of Business Research, The University of Texas at Ausin, 1973.

Chatfield, Michael. Contemporary Studies in the Evolution of Accounting Thought. Encino, CA: Dickenson Publishing Company, 1968.

Committee On Basic Auditing Concepts. A Statement of Basic Auditing Concepts, Studies in Accounting Research #6. Sarasota, FLA: American Accounting Association, 1973.

Edwards, James Don (ed.). Accounting Education: Problems and Prospects. American Accounting Association, 1974.

Grinaker, Robert L. and Ben B. Barr. Auditing, The Examination of Financial Statements. Homewood, IL: Richard D. Irwin, Inc., 1965.

Holmes, Arthur W. Auditing Principles and Procedure. New York, NY: Business Publications, Inc., 1939.

Holmes, Arthur W. Auditing Principles and Procedure. 5th ed. Homewood, IL: Richard D. Irwin, Inc., 1959.

Holmes, Arthur W. Basic Auditing Principles. Homewood, IL: Richard D. Irwin, Inc., 1957.

Holmes, Arthur W. and Wayne S. Overmeyer. Auditing Principles and Procedure. 7th ed. Homewood, IL: Richard D. Irwin, Inc., 1971.

Holmes, Arthur W. and Wayne S. Overmeyer. Basic Auditing Principles. 4th ed. Homewood, IL: Richard D. Irwin, Inc., 1972.

Kamp, Walter H. and James A. Cashin. Internal Control Standards and Related Auditing Procedures. Boston, MA: Herman Publishing, 1947.

Lindberg, Roy A. and Theodore Cohn. Operations Auditing. New York, NY: American Management Association, Inc., 1972.

Mautz, Robert K. Fundamentals of Auditing. 2d ed. New York, NY: John Wiley & Sons, Inc., 1964.

Mautz, R. K. and Hussein A. Sharaf. The Philosophy of Auditing, Monograph No. 6. Evanston, IL: American Accounting Association, 1961.

Meigs, Walter B. and John E. Larsen. Principles of Auditing. 3d ed. Homewood, IL: Richard D. Irwin, Inc., 1969.

Meigs, Walter B. and John E. Larsen. Principles of Auditing. 5th ed. Homewood, IL: Richard D. Irwin, Inc., 1973.

Montgomery, Robert H. Montgomery's Auditing. 8th ed. Lenhart, N. J. & Defliese, P. L. (eds.). New York, NY: Ronald Press Company, 1957.

Murphy, Mary E. Advanced Public Accounting Practice. Homewood, IL: Richard D. Irwin, Inc., 1966.

Opinion Research Corporation. Public Accounting in Transition, American Shareowners and Key Publics View the Role of Independent Accountants and the Corporate Reporting Controversy (Survey and Report for Arthur Andersen & Company). Chicago: Arthur Andersen & Company, 1974.

Porter, W. Thomas, Jr. and John C. Burton. Auditing: A Conceptual Approach. Belmont, CA: Wadsworth Publishing Company, Inc., 1971.

Prentice-Hall Editorial Staff. Encyclopedia of Auditing Techniques. 2 vols. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1966.

Ray, J. C. Independent Auditing Standards, A Book of Readings. New York, NY: Rinehart and Winston, Inc., 1964.

Sawyer, Lawrence B. The Practice of Modern Internal Auditing: Appraising Operations for Management. Orlanda, FLA: The Institute of Internal Auditors, Inc., 1973.

Stettler, Howard F. Auditing Principles. 2d ed. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1961.

Stettler, Howard F. Auditing Principles. 3d ed. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1970.

Stettler, Howard F. Systems Based Independent Audits. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1967.

Stettler, Howard F. Systems Based Independent Audits. 2d ed. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1974.

Stettler, Howard F. (ed.). Auditing Looks Ahead (Proceedings of the 1972 Touche Ross/University of Kansas Symposium on Auditing Problems, May 11 and 12, 1972). Lawrence Kansas: School of Business, University of Kansas, 1972.

Stettler, Howard F. Contemporary Auditing Problems (Proceedings of the 1974 Arthur Andersen/University of Kansas Symposium on Auditing Problems, May 9-10, 1974). Lawrence, Kansas: School of Business, University of Kansas, 1974.

Willingham, John J. and D. R. Carmichael. Auditing Concepts and Methods. New York, NY: McGraw-Hill Book Company, 1971.

Woods, Richard S. (ed.). Audit Decisions in Accounting Practice. New York, NY: The Ronald Press Company, 1973.

BIBLIOGRAPHIES

American Data Processing, Inc. Computer Yearbook and Directory. Vol 2, 2d ed. Detroit, MI: American Data Processing, Inc., 1969. (Bibliographical Index to Periodical Articles 1962 through 1968 and Bibliography of Books 1957 through 1968 in the Data Processing Field.)

Applied Computer Research, Inc. Quarterly Bibliography of Computers and Data Processing, 1968-69 Cumulation. Phoenix, Arizona: Applied Computer Research, Inc., 1972.

Applied Computer Research, Inc. Quarterly Bibliography of Computers and Data Processing, 1970-71 Cumulation. Phoenix, Arizona: Applied Computer Research, Inc., 1972.

Applied Computer Research, Inc. Quarterly Bibliography of Computers and Data Processing, 1972 Cumulation. Phoenix, Arizona: Applied Computer Research, Inc., 1973.

Applied Computer Research, Inc. Quarterly Bibliography of Computers and Data Processing, 1973 Cumulation. Phoenix, Arizona: Applied Computer Research, 1974.

Bergart, Jeffrey G, Marvin Denicoff and David K. Hsiao. An Annotated and Cross-Referenced Bibliography on Computer Security and Access Control in Computer Systems. Technical Report Series OSU-CISRC-TR-72-12. (Work performed under Contract N 14-72-C-391 Office of Naval Research.) Columbus: The Ohio State University, November, 1972.

Canning Publications, Inc. Bibliography and Sources of Information: Computer Fraud and Embezzlement. Vista, Calif: Canning Publications, Inc., 1973. (List published separately but in support of a September 1973 article in EDP Analyzer.)

Carter, Ciel. Guide to Reference Sources in the Computer Sciences. New York, NY: Macmillan Publishing Company, Inc., 1973.

Cleaver, Goodrich F. "Annotated Selective Bibliography--Auditing and Electronic Data Processing." Journal of Accountancy, November 1958, pp. 48-54.

Couger, J., Daniel (ed.). "Books Useful in Teaching Business Applications of the Computer." Computing Newsletter. 7th annual bibliography. Colorado Springs, CO: School of Business Administration, University of Colorado, January 1974.

Duggan, Michael A. Law and the Computer: A KWIC Bibliography. New York, NY: Macmillan Information (a division of Macmillan Publishing Company, Inc.), 1973

French, L. L. Management Information Systems: A Bibliography, Part I: System Design and Development. Redondo Beach, CA: TRW Systems Group, 1971.

French, L. L. Management Information Systems: A Bibliography, Part II: Applications. Redonda Beach, CA: TRW Systems Group, 1971.

Gotterer, Malcolm H. KWIC Index: A Bibliography of Computer Management. New York, NY: Petrocelli Books, 1970.

Gregory, Robert H. "Computers and Accounting Systems; A Bibliography." Accounting Review, April 1956, pp. 278-85.

Institute of Internal Auditors. Bibliography of Internal Auditing: Supplement 1950-1965. New York, NY: The Institute of Internal Auditors, 1967.

Institute of Internal Auditors. Bibliography of Internal Auditing: Supplement 1966-1968. New York, NY: The Institute of Internal Auditors, Inc., 1969.

Knutson, Peter H. (ed.). Topical Guide to Accounting Readings. New York, NY: Haskins and Sells, 1973.

Kuong, Javier F. Computer Security, Auditing and Controls--A Bibliography, 1964-1973. Wellesley Hills, MASS: Management Advisory Publications, 1973.

Kuong, J. F. (ed.). Computer Security, Auditing and Controls--Semi-Annual Review, Vol. 1, No. 1, July 1973-January 1974. Wellesley Hills, MASS: Management Advisory Publications, 1974.

Kuong, J. F. (ed.). Computer Security, Auditing and Controls--Semi-Annual Review, Vol. 1, No. 2, January 1974-July 1974. Wellesley Hills, MASS: Management Advisory Publications, 1974.

Library Committee. Books and Publications Suggested for an Accountant's Library. New York, NY: American Institute of Certified Public Accountants, 1970. Also published in Journal of Accountancy, December 1971, pp. 78-82.

Management Information Service. EDP Auditing: Concepts and Techniques. New York, NY: American Management Associations, September 1973.

Management Information Service. Managing the Security of Data Processing. New York, NY: American Management Associations, February 1974.

National Association of Accountants. Your Reference Library. New York, NY: Technical Service Department, National Association of Accountants, 1973.

National Computing Centre, Ltd. International Computer Bibliography, A Guide to Books on the Use, Application and Effect of Computers in Scientific, Commercial, Industrial and Social Environments, 2 vols. New York, NY: International Publications Service, 1971.

Pritchard, Alan. A Guide to Computer Literature: An Introductory Survey of the Sources of Information. 2d ed. Hamden, CT: Shoe String Press, Inc., 1972.

Rand Corporation. A Bibliography of Selected Rand Publications: Privacy in the Computer Age. Santa Monica, CA: Rand Corporation, February 1974.

Rittersbach, George H. "Data Processing Security: A Selected Bibliography." Management Adviser, September-October 1973.

Rittersbach, George H. Computer Security Bibliography. Unpublished paper, not dated.

Rothman, John (dir.). The New York Times Information Book. New York, NY: Information Services, The New York Times, 1973. (Subscription service to computerized storage and retrieval system.)

R. R. Bowker Company. Subject Guide to Books in Print, 1974. New York, NY: R. R. Bowker Company, 1974.

University of Florida. Annotated Bibliography of Electronic Data Processing. Accounting Series No. 2. Gainesville, FLA: Accounting Department, College of Business Administration, University of Florida, 1968.

U. S. Department of Commerce. NTI Search. Springfield, VA: National Technical Information Service, U. S. Department of Commerce, 1973. (Computer printouts from automated on-line access to technical report titles of U. S. Government research.)

U. S. Department of Justice. Document Retrieval Index. Washington, D. C.: Law Enforcement Assistance Administration, National Criminal Reference Service, U. S. Department of Justice, September 1973.

U. S. Department of Justice. Document Retrieval Index. Washington, D. C.: Law Enforcement Assistance Administration, National Criminal Reference Service, U. S. Department of Justice, January 1974.

U. S. Department of Justice. Document Retrieval Index. Washington, D. C.: National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, National Criminal Justice Reference Service, U. S. Department of Justice, September 1974.

U. S. Department of Justice. Document Retrieval Index (DRI). Supplement. Washington, D. C.: National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, Nationl Criminal Justice Reference Service, U. S. Department of Justice, March 1975.

U. S. Department of Justice. Selective Notification of Information. Washington, D. C.: Law Enforcement Assistance Administration, National Criminal Justice Reference Service, U. S. Department of Justice. (Monthly service of abstracts of documents.)

Witzer, Harold (ed.). Computer Security Bibliography. 2d rev., January 1971. Wilmington, MASS: Avco Computer Service, Avco Corporation, 1970.

A World List of Computer Periodicals. New York, NY: International Publications Service, 1971.

Xerox. A Bibliography of Doctoral Research on Crime and Law Envorcement. (1938-1970) Ann Arbor, MI: University Microfilms, Xerox Corporation, not dated.

Youden, W. W. Computer Literature Bibliography, 1946-1967. New York, NY: Arno Press, 1970. (Reprint of 1967 ed.)

COMPUTERS AND AUDITING (ACCOUNTING)

Canadian Institute of Chartered Accountants. Control Guidelines. Toronto: Study Group on Computer Control and Audit Guidelines, Canadian Institute of Chartered Accountants, 1970.

Clifton, H. D. and T. Lucey. Accounting and Comptuter Systems. New York, NY: Petrocelli Books, div. of Mason and Lipscomb Publishers, Inc., 1973.

Cook, Gregory A. Computer Accounting Methods. New York, NY: Petrocelli Books, 1974.

Hein, Leonard W. Contemporary Accounting and the Computer. Encino, CA: Dickenson Publishing Company, 1969.

Institute of Internal Auditors. Internal Auditing of Electronic Data Processing Systems. New York, NY: The Institute of Internal Auditors, Inc., 1967.

International Research Committee. Auditing Computer Centers. Orlando, FLA: The Institute of Internal Auditors, Inc., 1974.

International EDP Auditing Committee. Establishing the Internal Audit Function in EDP, Job Descriptions. Orlando, FLA: The Institute of Internal Auditors, Inc., 1974.

International Research Committee. Auditing Fast Response Systems. Orlando, FLA: The Institute of Internal Auditors, Inc., 1974.

Jancura, Elise. Computing and Auditing. New York, NY: Mason and Lipscomb Publishers, 1973.

Jancura, Elise G. Audit and Control of Computer Systems. New York, NY: Mason/Charter Publishers, Inc., 1974.

Jancura, Elise G., and Arnold H. Berger (eds.). Computers: Auditing and Control. Philadelphia, PA: Auerbach Publishers, Inc., 1973.

Kaufman, Felix. Electronic Data Processing and Auditing. New York, NY: Ronald Press, Inc., 1961.

Kuong, Javier F. Computer Security, Auditing and Controls, Text and Readings. Wellesley Hills, MASS: Management Advisory Publications, 1974.

Kuong, J. F. (ed.). Computer Auditing and Security Manual, Checklists and Guidelines for Evaluating Computer Security and Installations. Wellesley Hills, MASS: Management Advisory Publications, 1975.

Li, David H. Accounting--Computers--Management Information Systems. New York, NY: McGraw-Hill Book Company, 1968.

Lybrand, Ross Bros. and Montgomery. The Control and Audit of Electronic Data Processing Systems. New York, NY: Lybrand, Ross Bros. and Montgomery, 1965.

McRae, T. W. The Impact of Computers on Accounting. London, UK: John Wiley and Sons, 1964.

Pescow, J. and J. Horn (eds.). Accountant's and Manager's Guide to Computer Techniques. (Successful Data Processing Applications Series). Englewood Cliffs, NJ: Prentice-Hall, Inc., 1971.

Porter, W. Thomas, Jr. Auditing Electronic Systems. Belmont, CA: Wadsworth Publishing Company, 1966.

Sweeney, Robert P. Use of Computers in Accounting. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1971.

Tyran, Michael. Computerized Accounting Methods and Controls. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1972.

U. S. General Accounting Office. Review Guide for Evaluating Internal Controls in Automatic Data Processing Systems. U. S. General Accounting Office, 1968 (with 1970 revisions).

Washbrook, Harry. Management Control, Auditing and the Computer. New York, NY: Crane-Russak and Company, Inc., 1971.

COMPUTERS AND CRIME

Barlay, Stephen. The Secrets Business. New York, NY: Thomas Y. Crowell Company, 1973.

Best, Harry. Crime and the Criminal Law in the United States. New York, NY: Macmillan Company, 1930.

Chamber of Commerce of the United States. A Handbook on White Collar Crime: Everyone's Problem, Everyone's Loss. Washington, D. C.: Chamber of Commerce of the United States, 1974.

Clarke, Thurston and John J. Tigue, Jr. Dirty Money. New York, NY: Simon and Schuster, 1975.

Curtis, S. J. Modern Retail Security. Springfield, ILL: Charles C. Thomas Publisher, 1960.

Farr, Robert. The Electronic Criminals. New York, NY: McGraw-Hill Book Company, 1975.

Geis, Gilbert (ed.). White-Collar Criminal: The Offender in Business and the Professions. New York, NY: Atherton Press, 1968.

Gorrill, B. E. How to Prevent Losses and Improve Profits with Effective Personnel Security Procedures. Homewood, ILL: Dow Jones-Irwin, Inc., 1974.

Jaspan, Norman. Mind Your Own Business. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1974.

Jaspan, Norman, and Hillel Black. The Thief in the White Collar. Philadelphia, PA: J. B. Lippincott, Company, 1960.

McKnight, Gerald. Computer Crime. New York, NY: Walker and Company, 1973.

Nettler, Gwynn. Explaining Crime. New York, NY: McGraw-Hill Book Company, 1974.

Pace, Denny F. and Jimmie C. Styles. Organized Crime: Concepts and Control. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1975.

Seymour, Whitney North Jr. Fighting White Collar Crime: A Handbook on How to Combat Crime in the Business World. New York, NY: Office of the United States Attorney for the Southern District of New York, 1972.

Sutherland, Edwin H. White Collar Crime. New York, NY: The Dryden Press, 1949.

U. S. Department of Commerce. The Cost of Crimes Against Business. Bureau of Domestic Commerce, Domestic and International Business Administration, U. S. Department of Commerce, Washington, D.C.: Government Printing Office, November 1974.

COMPUTERS, LAW AND SECURITY

AFIPS System Review Manual on Security. Montvale, NJ: AFIPS Press, 1974.

Bigelow, Robert P. (ed.). Computer Law Service. 7 Vols. Chicago, IL: Callaghan and Company, 1972.

Brown, William F. AMR's Guide to Computer and Software Security. New York, NY: AMR International, Inc., 1971.

Computer Science and Engineering Board. National Academy of Sciences. Databanks in a Free Society: Computers Record-Keeping and Privacy. New York, NY: Quadrangle/The New York Times Book Company, 1972.

Computer Security Research Group. Computer Security Handbook. New York, NY: Macmillan Information (A division of Macmillan Publishing Company, Inc.), 1973.

Del Mar, D. The Security of Industrial Information: A Guide and Reference for Managers and Engineers. New Hope, PA: The Chestnut Hill Press, 1974.

Farr, M. A. L., B. Chadwick and K. K. Wong. Security for Computer Systems. Manchester, Eng.: National Computing Centre Limited, 1972.

Freed, Roy N. Computers and Law: A Reference Work. 4th ed. Boston, MASS: By the Author, c/o Peabody Brown, Rowley and Storey, One Boston Place, 1974.

Lundell, E. Drake Jr. and Edward J. Bride. Computer Use: An Executive's Guide. Boston, MASS: Allyn and Bacon, Inc., 1973.

National Bureau of Standards. Guidelines for Automatic Data Processing Physical Security and Risk Management (Federal Information Processing Standards, Publication 31), U. S. Department of Commerce. Washington, D. C.: Government Printing Office, 1974.

National Computing Centre, Ltd. (ed.). Insuring a Computer System (Computerguide Series No. 7). New York, NY: International Publications Service, 1973.

Parker, Donn B. Threats to Computer Systems. Livermore, CA: Lawrence Livermore Laboratory, 1973. (Prepared for U. S. Atomic Energy Commission under contract No. W-7405- Eng-48.)

Parker, Donn B., Susan Nycum and S. Stephen Oura. Computer Abuse. Menlo Park, CA: Stanford Research Institute, 1973. (Prepared for the National Science Foundation, RANN NSF/RA/S-73-017.)

Renninger, Clark R. (ed.). Approaches to Privacy and Security in Computer Systems. Proceedings of a Conference held at the National Bureau of Standards, March 4-5, 1974. Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D. C. 20234, September 1974.

Renninger, Clark R. and Dennis K. Branstad (eds.). Government Looks at Privacy and Security in Computer Systems (NBS Technical Note 809). A Summary of a Conference held at the National Bureau of Standards, Gaithersburg, Maryland, November 19-20, 1973. Institute for Computer Sciences and Technology, National Bureau of Standards, U. S. Department of Commerce. Washington, D. C.: Government Printing Office, 1974.

Sanders, Donald H. Computers and Management in a Changing Society. 2d ed. New York, NY: McGraw-Hill Book Company, 1974.

Tapper, Colin. Computers and the Law. Hackensack, NJ: Fred B. Rothman and Company, 1973.

Westin, Alan F. and Michael A. Baker. Databanks in a Free Society. New York, NY: Quadrangle/The New York Times Book Company, 1972.

Wooldridge, Susan, Colin R. Corder, and Claude R. Johnson. Security Standards for Data Processing. New York, NY: John Wiley and Sons (Halsted Press), 1973.

PERIODICALS

Auditing News, October 1974, p. 3.

Auditing News, February, 1975, p. 6.

Auditing News, April 1975, pp. 1, 3.

Auditing News, October 1975, p. 2.

Business Week, April 22, 1972, pp. 54-60.

Business Week, April 14, 1973, p. 71.

Business Week, September 14, 1974, p. 31.

Business Week, October 12, 1974, p. 35.

Business Week, September 8, 1975, p. 30.

Computerworld, April 25, 1973, pp. 1, 4.

The CPA Letter, October 14, 1974, p. 2.

The CPA Letter, November 11, 1974, p. 2.

EDPACS (Abstracts and Commentaries), May 1974, pp. 17-18.

Journal of Systems Management (Data Matter), May 1975, pp. 5-6.

Newsweek, April 23, 1973, pp. 90, 93.

Wall Street Journal, April 9, 1973, p. 3.

Wall Street Journal, April 24, 1973, pp. 1, 37.

Wall Street Journal, May 4, 1973, pp. 1, 8.

Wall Street Journal, March 18, 1975, p. 36.

Wall Street Journal, May 22, 1975, p. 9.

SOURCES FOR INITIAL RESEARCH EFFORTS

American Data Processing, Inc. Management Information Systems Index (Articles through 1961, books 1961-62). American Data Processing, Inc., 1962.

American Institute of Certified Public Accountants. Accounting Firms and Practitioners 1971. New York, NY: AICPA, 1972.

American Institute of Certified Public Accountants. Alphabetical Listing of Attendees. Seventh Annual Conference on Computers and Information Systems, Boston, Massachusetts, May 24-26, 1971.

Bentley, Harry C. and Ruth S. Leonard. Bibliography of Works on Accounting by American Authors, 2 vols. (1796-1900, 1901-1934). Boston, MA: Harry C. Bentley, 1934, 1935. (See also reprint by Augusta M. Kelley, Publishers.)

Blough, Carmen G. (ed.). "Selected Accounting Research Bibliography; Publications of the Principal Accounting Organizations in the U.S." Journal of Accountancy (Accounting and Auditing Problems), February 1963, pp. 73-78.

Bradford, Ernest S. Bradford's Directory of Marketing Research Agencies and Management Consultants in the United States and the World. Fairfax, VA: Bradford's Directory of Marketing Research Agencies, 1971.

Demarest, Rosemary R. (ed.). Accounting, A Guide to Information Sources (Management Information Guide 18). Detroit, MI: Gale Research Company, 1970.

Dissertation Abstracts International, Retrospective Index. Ann Arbor, MI: University Microfilms, Xerox Corporation, 1970.

"Doctoral Dissertations Accepted" (1968-1971). Journal of Business, January issues of 1970, 1971, 1972, 1973.

Edwards, James Don. History of Public Accounting in the United States (MSU Business Studies. Bureau of Business and Economic Research, Graduate School of Business Administration. East Lansing, MI: Michigan State University, 1960.

Federal Government Accountants Association. Bibliography on Federal Accounting, Auditing, Budgeting, and Reporting. Arlington, VA: Federal Government Accountants Association, 1971.

Ferguson, Elizabeth (ed.). Sources of Insurance Statistics. New York, NY: Special Libraries Association, 1965.

Fisk, Margaret (ed.). Encyclopedia of Associations (Vol. 1, National Organizations of the U.S.). 7th ed. Detroit, MI: Gale Research Company, 1972.

Hewer, Verlyn. Address list for selected organizations furnished via telephone by Mrs. Hewer, National Referral Center, Library of Congress, Washington, D. C., August 10, 1973.

Krause, Roy H. (ed.). Moody's Industrial Manual. 2 vols. New York, NY: Moody's Investor Service, Inc., 1972.

Kruzas, Anthony T. Encyclopedia of Information Systems and Services. Ann Arbor, MI: Edwards Brothers, 1971.

Littleton, A. C. Accounting Evolution to 1900. New York, NY: American Institute Publishing Company, Inc., 1933.

Littleton, A. C. and B. S. Yamey. Studies in the History of Accounting. Homewood, IL: Richard D. Irwin, Inc., 1956.

Magnuson, Arnold. Address list for state societies of certified public accountants, furnished by Executive Director, Nebraska Society of Certified Public Accountants, Lincoln, Nebraska, July 5, 1973.

Magnuson, Arnold. Address list for state boards of public accountancy, Furnished by Executive Director, Nebraska Society of Certified Public Accountants, Lincoln, Nebraska, July 5, 1973.

Morrill, Chester, Jr. (ed.). Systems and Procedures Including Office Management Information Sources (Management Information Series, No. 12). Detroit, MI: Gale Research, Inc., 1969.

Morrill, Chester, Jr. (ed.). Computers and Data Processing Information Sources (Management Information Guide 15). Detroit, MI: Gale Research Company, 1969.

Office of Federal Register. United States Government Organization Manual 1972/73 (National Archives and Records Service, General Services Administration). Washington, D. C.: Government Printing Office, 1973.

"Research in Accounting" (1969-1972). Accounting Review, January issues of 1970, 1971, 1972, 1973.

R. R. Bowker Company. Subject Guide to Books in Print, 1972.. New York, NY: R. R. Bowker Company, 1972.

Smith, Mildred J. (ed.). The Insurance Almanac: Who, What, When and Where--In Insurance. New York, NY: The Underwriter Printing and Publishing Company, 1967.

Statistical Department. 1967 Argus F. C. & S. Chart. Cincinnati, OH: The National Underwriter Company, 1967.

The Spectator. Desk Directory of Insurance 1966 Edition. Philadelphia, PA: Chilton Company, 1966.

Sterling, Robert R. (ed.). Research Methodology in Accounting. Lawrence, Kansas: Scholars Book Company, 1972.

Thomas, Roy E. (ed.). Insurance Information Sources (Management Information Guide 24). Detroit, MI: Gale Research Company, 1971.

SOURCES NOT CLASSIFIED ABOVE

American Institute of Certified Public Accountants Tenth Annual Conference on Computers and Information Systems, Chicago, Illinois, May 6-8, 1974.

AFIPS. Data on Computer Related Occupations Extracted from the 1970 Census. Montvale, NJ: American Federation of Information Processing Societies, Inc., October 1974.

AFIPS/Time. A National Survey of the Public's Attitudes Toward Computers. A joint project of Time Magazine and American Federation of Information Processing Societies, Inc., 1971.

Bouvier, John. Bouvier's Law Dictionary and Concise Encyclopedia, 2 vols. 3d rev. (being the 8th ed.) by Francis Rawle. St Paul, MI: West Publishing Company, 1914.

Brochure on membership promotion from Institute of Internal Auditors, Orlando, Florida (not dated).

Bridgewater, William and Elizabeth J. Sherwood (eds.), The Columbia Encyclopedia, 2d ed. Morningside Heights, NY: Columbia University Press, 1950.

Bureau of Labor Statistics. Computer Manpower Outlook (Bulletin 1826). Washington, D. C.: Government Printing Office, 1974.

Computer printout from DATRIX, University Microfilms, Ann Arbor, MI., October 10, 1973.

Data Processing, Volume VIII. Proceedings of the 1964 International Data Processing Conference, June 23-26. New Orleans, LA: Data Processing Management Association, 1964.

Editorial Staff. Black's Law Dictionary. 4th ed. St Paul, MINN: West Publishing Company, 1957.

Editorial Staff. Black's Law Dictionary. Rev. 4th ed. St Paul, MINN: West Publishing Company, 1968.

Editorial Staff. The New Encyclopaedia Britannica Micropaedia, Volume IV, Ready Reference and Index. Chicago, IL: Encyclopaedia Britannica, Inc., 1974.

Editorial Staff. The New Encyclopaedia Britannica Macropaedia, Volume 5. Chicago, IL: Encyclopaedia Britannica, Inc., 1974.

Fund and Wagnalls Company. Standard Dictionary of the English Language, International Edition. Chicago, IL: Encyclopaedia Britannica, Inc., 1958.

Gove, Philip Babcock (ed.). Webster's Third New International Dictionary of the English Language Unabridged. Springfield, MASS: G & C Merriam Company, 1961.

Hindelang, Michael J., Christopher S. Dunn, L. Paul Sutton, and Alison L. Aumick. Sourcebook of Criminal Justice Statistics, 1973. (Prepared under research grant 72-SS--99-6006 to the Criminal Justice Research Center, Albany, New York.) U. S. Department of Justice, Law Enforcement Assistance Administration, National Criminal Justice Information and Statistics Service. Washington, D. C.: Superintendent of Documents, U. S. Government Printing Office, August 1973.

Letter from Brandt R. Allen, Associate Professor of Business Administration, Graduate School of Business Administration, University of Virginia, Charlottesville, VA., July 30, 1973.

Letter from John C. Burton, Chief Accountant, Securities and Exchange Commission, Washinton, D. C., July 30, 1973.

Letter from Leonard Landsman, Director of Inquiries Department, Legal and Compliance Division, American Stock Exchange, Inc., New York, NY., July 23, 1973.

Letter from Ken Pollock, Assistant Director, Division of Financial and General Management Studies, United States General Accounting Office, Washington, D. C., August 13, 1973.

Letter from Jerome Priest, Computer Resources Corporation, Darien, CONN., July 30, 1973.

Letter from John Rothman, Director, Information Services, The New York Times, New York, NY., September 5, 1973.

Letter from Mary Jane Ruhl, NTIS Program Manager, National Technical Information Service, U. S. Department of Commerce, Springfield, VA., August 21, 1973.

Letter from James K. Steen, Deputy Director, Financial-Regulatory Branch, Department of Insurance, State of Illinois, Springfield, August 27, 1973.

Letter from Marvin Stone, President, American Institute of Certified Public Accountants, New York, NY., April 1, 1968.

Letter from Harold Weiss, Director, Automation Training Center, Reston, VA., August 14, 1973.

Letter from M. B. Woodbury, Deputy Comptroller for Audit Policy, Office of the Assistant Secretary of Defense, Washington, D. C., August 16, 1973.

Manpower Report of the President. Washington, D. C.: Government Printing Office, 1975.

McNamara, M. Frances. 2,000 Famous Legal Quotations. Rochester, NY: Aqueduct Books, 1967.

Microdata Corporation. The Communications Handbook. Irvine, CA: Microdata Corporation, 1973.

NBC News. The White-Collar Rip-Off. Special Documentary TV Special produced by Eliot Frankel and reported by Edwin Newman on NBC TV, 9:00 CDT, June 1, 1975.

New York Times Company. The New York Times Information Bank. New York, NY: Information Services, The New York Times, 1972. (Brochure describing subscription service to computerized storage and retrieval system.)

Questionnaire response from Alan R. Kaplan, Editor, Modern Data, Framingham, MA., July 18, 1973.

Questionnaire response from Michael S. Keplinger, Staff Assistant, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D. C., August 7, 1973.

Questionnaire response from Donn B. Parker, Senior Information Processing Specialist, Stanford Research Institute, Menlo Park, CA., July 23, 1973.

Questionnaire reponse from J. J. Wasserman, President, Computer Audit Systems, East Orange, NJ., July 23, 1973.

Strong, James. The Exhaustive Concordance of the Bible. New York, NY: Abingdon Press, 1890.

United States Senate Select Committee on Small Business. The U.S.A. Business Community: Its Composition and Changing Nature, with Special Reference to Small Business. Senate Report 93-1168, 93d Congress, 2d Session. Washington, D. C.: Government Printing Office, 1974.

Weber, Richard E. and Bruce Gilchrist. Data on Computer Related Occupations Extracted from the 1970 Census. (A report prepared under the auspices of the AFIPS Statistical Research Program.) Montvale, NJ: American Federation of Information Processing Societies, Inc., 1974.

Weber, Richard E. and Bruce Gilchrist. Numerical Bias in the 1970 U.S. Census Data on Computer Occupations. (A study performed under the auspices of the AFIPS Statistical Research Program.) Montvale, NJ: American Federation of Information Processing Societies, Inc., 1974.

APPENDIX A

Summaries of Computer Abuse Cases

APPENDIX A

SUMMARIES OF COMPUTER ABUSE CASES

6421Y*
Hancock vs Texas, Texas--Program Theft.

A programmer stole $5 million worth of programs he was maintaining for his employer and attempted to sell them to a customer of his employer. He was convicted of grand theft and lost two appeals based on programs not being property as defined by theft laws. He served five years in prison.

6431N
MICR Deposit Slips Fraud, New York City--Fraud.

A depositor put a large sum of money in his account and asked for 1,000 MICRO-coded deposit slips. He placed them on counters in the bank and accumulated money in his account from other depositors.

6432N
Boston MICR Deposit Slips Fraud, Boston--Fraud.

Same method used as in case 6431 . . .

6433N
Washington MICR Deposit Slips Fraud, Washington, D.C.--Fraud.

A depositer exhanged blank deposit slips on the counter in the bank with his own MICR-coded slips. He accumulated $250,000 in four days from other people's deposits. He then withdrew $100,000, disappeared and has never been caught.

6531N
Embezzlement by Collusion in London--Embezzlement.

As reported in the London Sunday Times by way of Adrian Norman. The chief programmer, buyer, and sales manager allegedly embezzled $125,000. Dismissed.

6631Y
Bennett vs U.S.A., Minneapolis--Altering Bank Records.

A programmer altered his demand-deposit accounting program to ignore overdrafts in his checking account for about six months. He

---

*Y means the case is verified. N means the case is not verified.

accumulated overdrafts of $1357 before he was caught by manual accounting when the computer failed. He made restitution and received a suspended sentence.

6741N
Equipment Use, Chicago--Fraud.

According to Datamation, 12/67, p. 78, five employees including the director of the computer bureau used equipment without authorization.

6811N
1401 Shooting Vandalism, Washington State--Vandalism.

An unknown assailant fired two shots from a pistol at an IBM 1401 computer at a state unemployment office. He did minor damage.

6821N
Airline Software Theft, England--Theft.

Sections of an airline seat reservation software system were taken and used by another firm to contract for a publicly funded real-time system.

6831Y
Mansfield Embezzlement, California--Embezzlement.

A chief accountant embezzled $1 million from his employer over six years. He used a computer for financial modeling of his company to gauge appropriate changes in accounts receivable and payable to remain undetected. He was convicted and given a ten-year prison term.

6832N
Credit Cards Duplication Fraud, New York--Fraud.

Blank credit cards and authentic names and account numbers were used to produce duplicate cards and to avoid computer rejections of false accounts. The alleged perpetrator was murdered.

6833N
Securities Brokerage Fraud, Texas--Mail Fraud.

Three former employees of a securities brokerage are alleged to have changed securities transactions statements; they claimed the changes were computer errors. $500,000 was taken.

6834N
Youth Corps Payroll Fraud, New York--Embezzlement.

A data center employee printed Youth Corps payroll checks for nine months at 100 checks per month for a total loss of $2,750,000.

6911Y
Sir George Williams University Vandalism, Montreal.

Computer center destroyed.

6912Y
Boston University Vandalism, Boston.

IBM 360/40 central processor was damaged by wire cutting and acid.

6931N
University Extortion, Massachusetts.

Students took over the computer center and threatened to keep it out of operation until their demands were met by the administration.

6921N
Programmed Bigotry, New York.

A programmer was accused of bigotry because he programmed a computer to eliminate black people in screening and selecting new employees.

6922N
Wang Computer Theft, Illinois.

A student summer employee stole a Wang Computer worth $2,500. He took it with him when he returned to his university.

6923N
University victim--Theft, conviction.

A student stole a PDP8 computer in Boston.

6924Y
Commercial time-sharing staff--Fraud.

A systems programmer gained legitimate LOGON to his employer's competitor's service and tested possible privileged system commands. He discovered enough weaknesses to penetrate privileged mode where he could obtain confidential data.

6952N
Fictitious Credit Notes Embezzlement, London.

Programmer altered a program to cause a computer to print fictitious credit notes for cigarette coupons and sent to his address. He was discovered as a result of outside information, convicted, and served 9 months in prison.

6931Y
Payroll Embezzlement Conspiracy and Forgery, California

City employees produced payroll checks for fictitious employees. Perpetrators are still fugitives.

7011Y
Chemical Company Vandalism, Michigan.

Beaver 55 antiwar group destroyed data processing media. It is alleged that magnets were used. The cost to reconstruct data was $100,000.

7012Y
University of Wisconsin Vandalism, Wisconsin.

An Army data center was bombed by political dissidents. A researcher was killed. $1.5 million damage was sustained, and 20 years of important data were lost.

7013Y
University of Kansas Vandalism, Kansas.

The university data center was bombed. Magnetic tape racks were damaged.

7014Y
New York University Vandalism, New York.

Students held the Atomic Energy Commission computer for $100,000 ransom. Incendiary devices were defused before damage was caused. Two people were indicted on bomb conspiracy charges.

7015Y
Fresno State Vandalism, California.

A student led a riot in which a CDC 3300 computer was fire bombed, doing $1 million in damages.

7016N
Pharmaceutical Company Vandalism, New Jersey.

An employee destroyed on-line data files after being given notice of termination.

7017N
Army Purchasing Data Vandalism, Washington, D. C.

A disgruntled Army officer awaiting retirement erased purchasing data from magnetic tape.

7021N
Publishers Mailing List Theft, Chicago.

Three million customer addresses were stolen by three night shift computer operators.

7022N
Lost Subscription List, Negligent Accident, New York City.

Computer operators of a consulting firm rendered useless the subscription list of a magazine.

7023Y
Honeywell vs Lithonia Breach of Contract, Georgia.

Lithonia stopped lease payments to Honeywell for an installed computer because it was claimed that software did not function properly. The case was decided in favor of Honeywell.

7024N
Population Registry Data Theft Fraud, Sweden.

Two employees borrowed tapes of population registry and copied them, using another computer. They sold the copies at reduced prices to their employer's customers. Both employees were convicted and given six-mon jail sentences.

7025N
Unaut Use Fraud, Georgia.

A Defense Department public relations executive bribed a Pentagon EDP employee to make a computer run to compile results of 1,000 questionnaires for a Canadian National Exhibition in Toronto.

7031N
CPA Firm Fraud, San Francisco.

The perpetrator manipulated input data to affect totals and stole cash receipts of $20,000.

7032N
Midwest Bank Fraud.

Two employees forged and balanced control totals of demand deposit accounts. They were caught after stealing $30,000.

7033N
New Jersey Bank Embezzlement, New Jersey.

The computer systems vice president, senior computer operator,

and three nonemployees of a bank were charged with transferring money from infrequently used savings accounts to newly opened accounts. They were detected when conversion to a new computer disrupted work.

7034N
Los Angeles Welfare Embezzlement Theft, Los Angeles.

Eleven County Department of Social Service employees used terminated state welfare numbers, changing names and addresses, to issue checks to themselves.

7035N
New York Two-Bank Float Embezzlement, New York-Jamaica, Queens.

A bank vice president and four others deposited checks designated as cash deposits, which are recorded for immediate credit. Checks drawn on the account were good until the deposit checks were found not to be covered by another bank. The act was discovered when a bank messenger failed to deliver $440,000 worth of checks to the clearing house. The scheme worked for four years, with a total theft of $900,000.

7036N
IRS Tax Credit Embezzlement, Washington, D.C.

An IRS adjustment clerk transferred unclaimed tax credits from one account through a chain of other accounts and finally to a relative's account. The act was discovered when auditors traced a complaint of no refund of a $1,500 tax credit.

7041N
Dating Bureau Fraud, Los Angeles.

A computer dating bureau was charged by the State Attorney with making false claims that a computer was being used to evaluate data and match clients.

7042Y
Time-Sharing Use Fraud, Louisville-Cincinnati.

A former employee of a time-sharing service is alleged to have made unauthorized access to extract confidential data over a long distance circuit from Cincinnati. The indictment was dropped.

7043Y
TWA vs Burroughs Breach of Contract, New York.

TWA claimed that Burroughs failed to install a workable reservation system.

7044N
Minnesota Dating Bureau Fraud, Minneapolis.

A dating bureau was accused by the State Attorney General of falsely advertising that clients would be matched with compatible dates by computer (same firm as in the Los Angeles fraud case, 7041).

7045Y
Computer Service Theft, Detroit.

Two engineers accidentally used a password one digit different than theirs. It belonged to the president of the time-sharing firm and allowed access to privileged customer and accounting data. Thus it allowed the engineers to use unlimited amounts of computer time and obtain customer information and proprietary program listing. Discovery was made by computer operators who noticed use of the password at unusual times. The engineers were fired, no other action was taken.

7111N
Tape Reels Label Removal Vandalism, New York.

A discharged employee removed labels from 1,500 reels of tape.

7112Y
Life Insurance Company, Paper Tape Failure Vandalism, New York.

Three on-strike computer maintenance technicians activated a field office data collection system by prerecorded computer messages via telephone. The instructions were not to rewind paper tape, causing the next read command to read blank tape endlessly. Perpetrators were discharged and indicted under an obscene telephone call law.

7113N
Program Change, Vandalism, France.

A programmer changed his employer's program to destroy all records on January 1, 1970.

7114N
Toulouse Computer Center Destruction, Vandalism, Toulouse, France.

Left-wing extremists vandalized a computer center.

7115N
West Coast Electronics Firm, Vandalism.

An angry employee destroyed all files and programs.

7116
Computation Center Vandalism, California.

A student tried to erase every table of contents on each disk pack. He succeeded in erasing only one, using a readily available IBM utility program. Malicious mischief was charged and proven before a judicial council. Use of that utility now requires a password.

7121
Ward v. California, California.

A programmer was accused of stealing a copy of a program from the computer of his employer's competitor through telephone circuits from a remote job entry terminal. Criminal charges of theft of a trade secret and a civil suit resulted in conviction and a judgment for $300,000 payment of damages to the plaintiff.

7122N
Railroad Theft, New York.

A suspected organized crime attempt to manipulate input to a computerized inventory system to steal rolling stock.

7123N
Time-Sharing Theft, Unethical Act.

A person claims that he was discharged by his time-sharing service employer for obtaining confidential passwords.

7124N
Insurance Fraud Civil Suit, Denmark.

Plaintiff's policy lapsed before an accident occurred. He claimed he did not receive renewal notices. The company claimed such notices are sent automatically by computer, but no record is kept. The plaintiff lost the suit for other reasons.

7125Y
Program Extortion, Theft, Los Angeles.

A programmer is alleged to have taken all his employer's programs to hold for extortion. The case was dropped for lack of evidence.

7126Y
Software Theft, Civil Suit, New York.

A software firm with a contract to do program development for a time-sharing company is alleged to have taken the time-sharing system and sold it to another firm.

7127Y
Registered Voters List Civil Suit, Los Angeles.

A computer service used a registered voters' address list for commercial purposes. A suit was filed by the state. It was settled out of court when the defendant paid $22,000.

7128Y
Denver Time-Sharing Dispute, Civil Suit, Denver.

Three defendants were accused of taking the time-sharing system of their employer and going to work for a competitor. A suit was filed but was settled out of court. The complainant stated that "the judge threw it out because it was too technical for a court to understand."

7129N
NCIC Information Theft, Chicago.

A policeman is alleged to have obtained from the FBI National Crime Information Center (NCIC) the dossier of a man involved in a transaction with the policeman's brother-in-law.

71210Y
Belmont Pawsey, Civil Suit, San Francisco.

The State Personnel Board disciplined two psychiatrist case workers for refusing to submit welfare data because they claimed the computer system lacked security and confidentiality. Judgment was made in the state's favor, but the case has been appealed.

71211N
Bank Data Extortion, Theft, Los Angeles.

Two suspects are alleged to have stolen cancelled checks and magnetic tapes at the airport and held them for ransom. The bank, owner of the property, was not suffering a great loss because it had copies of the tapes and records of the checks. The suspects were arrested.

71212N
Customer List, Theft, White Plains, New York.

The suspect is alleged to have tried to sell listings of new customers. He was caught when a potential buyer reported the offer to the police. The list was estimated to be worth $37,000 in the address list market. The case was dropped for lack of evidence.

71213N
Payroll Information Theft, Toronto.

Several programmers stole information from a payroll system and sold it to an insurance company agent.

71214Y
Computer Theft, Massachusetts.

An employee removed a minicomputer from the manufacturing plant a piece at a time and assembled it a home. He was fired.

71215N
Data theft

Two employees of a U.S. economic data collection firm extracted and sold data. After they were fired, they tried to get others to do the same thing.

71216N
Espionage, West Germany.

A secret agent is alleged to have copied confidential data of 3,000 West German firms onto tape and gave them to E. Germany, for whom he was working.

7131Y
Bank Embezzlement.

An assistant vice president and a computer operator at a bank were caught in an embezzlement. The method was not known. Reported in the U.S. Defalcation Report, 1971.

7132Y
Bank Misapplication of Funds

A former systems analyst misapplied funds. Restitution of $10,150 was made to the bank. Reported in the U.S. Defalcation Report, 1971.

7133N
French Round Down, Embezzlement, France.

An employee was authorized to round salaries to two decimal places. He accrued the rounded-down amounts to his own salary.

7134N
German Family Allowance Fraud, Germany.

Clerks in a government department diverted family allowances for children whose death notices they received.

7135N
Doctor's Claim, Fraud, Canada.

A manager of claims of a government medical aid service introduced false doctor's claims into a computer system and directed payments to a fictitious doctor's office.

7136N
Catering Service, England.

An account clerk at a catering service had a grocery store owner accomplice. He submitted to a computer system false account numbers and invoices for undelivered food. Thefts amounted to $120,000 over eight years. Both conspirators were convicted.

7137N
Collection Agency Fraud, Texas.

A computerized collection agency sent new bills to people who had paid the bills the previous year. They relied on the discouragement of people fighting computerized systems.

7138Y
Department Store Fraud, Embezzlement, Canada.

A systems analyst ordered expensive appliances at his employer's store and coded them as special pricing orders at $6. Discovery was made by systems consultants reviewing the adequacy of EDP controls.

7139N
Bookkeeper Embezzlement, California.

A woman bookkeeper embezzled $600 through a computer system.

71310N
Payroll Theft, Solingen, Germany.

Reiner von sur Muhlen in Wirtschaft and Politik reported that an insurer lost 280,000DM in a payroll theft. The victim was an industrial company. The employee was forced to make restitution after he changed punch card input to change employee salaries soon after conversion to the computer. Management noticed the high salaries and a suprise audit resulted in apprehension.

71311N
Pension theft, West Germany.

An EDP employee in a chemical firm altered deceased employee's data to have the deceased's pension paid into his own bank account.

71312N
Pension theft, Canada.

An employee in an insurance company changed several deceased insured persons' account number to his own to collect their pensions. He was caught when a staple in a punch card forced manual handling which revealed several cards with the same number.

71313N
Pension theft, West Germany.

An employee was caught leaving deceased pensioners' accounts in the system, but changing recipients' bank account numbers. Auditors noticed unusual activity in March when pensioners must verify their existence.

71314N
Payroll theft, West Germany.

An EDP operator pressed the "repeat" button on the printer to print 200 extra copies of his check. He was caught when he cashed 37 checks all at the same bank.

71315N
Bank Embezzlement.

A vice president and employee of a discount chain credited incoming checks in the computer system, but not the old parallel ledger system during the changeover to the computer. $6.8 million was embezzled. The bank vice president was promoted to a new job and had to erase evidence and was caught. This was reported by the Administrator of National Banks, Office of the Controller of Currency, U.S. Treasury.

71316N
Embezzlement, England.

Programmer transferred 17,000 Pounds to a special error write-off account in a British firm. The British Association for Resocialization of Ex-convicts indicated that he was convicted and served two years in prison.

71317N
Bank Credit Embezzlement.

An accounting programmer changed a limit check from $2000 to $200,000 to claim a higher amount of credit than was allowed.

71318N
Bank Embezzlement, Hamburg Germany.

A programmer collected round-downs from a large number of accounts in a favored account in a Hamburg bank. The bank lost 480,000DM.

71319N
Sales Commission Embezzlement, England.

A programmer in a mail order company created a sales commission account in the name of Zwana to be the last in order. He collected round downs in the last account. It was discovered after three years when Marketing chose the first and last accounts for a public relations project.

7141N
Data Service Fraud, Civil Suit, Atlanta,

A data service is alleged to have failed to provide a range of services to a consumer credit reporting company.

7142N
Unauthorized Time-Share Use, Unethical Act.

An employee claimed he was using his company's time-sharing service without detection.

7143N
Dating Bureau, Chicago--Fraud.

A dating service claimed use of computer. The Cook County Grand Jury claimed they had no computer and did not provide dates.

7144N
Computer Training, Akron, Ohio--Fraud.

A computer training institute terminated its classes in mid-course. It lacked equipment, class schedules, and teaching quality.

7145N
Computer Training School, New York--False Advertising.

A computer training correspondence school advertised false employment opportunities and aptitude requirements. A $2,000 fine was paid.

7146N
Computer Use, Cambridge, England--Fraud.

An employee committed fraud using his employer's computer, taking $750. He claimed the reason was "it was a horrible, impersonal machine." He was found guilty, fined, and order to make restitution.

7211Y
Computer Training Institute, Fullerton, California--Vandalism.

Flares were thrown through broken windows. Two tape transports were damaged.

7212Y
Insurance Vandalism, Denver, Colorado--Vandalism

According to Computerworld, a computer operator employee inserted a metal object causing a short circuit in a disk file drive 56 times in two years. $500,000 was spent attempting to correct the problem. As a last resort sabotage was suspected and a TV monitor was used to catch the suspect. He is quoted as saying his reason was an overpowering urge to shut the computer down.

7213N
Computer Shooting, Johannesburg--Vandalism.

As reported by Reuters in the San Francisco Chronicle, 9/13/72, a person fired four shots through a window at the computer. It was dented but continued working. It is believed the person may have received an exorbitant account.

7214N
Tapes and Disks, California--Vandalism.

Employee of a Berkeley or San Francisco messenger service carrying tapes and disks between computer sites claims he used a magnet to destroy information. Presumed to be a case of malicious mischief.

7215Y
University Computing Center--Vandalism.

A student gained privileged access to the time-sharing system and caused frequent crashes: a case of malicious mischief.

7216Y
Insurance Company--Vandalism.

A tape librarian, disgruntled because she was fired, replaced all of the magnetic tapes in the vault with new, blank tapes during her 30-day notice period. The loss was estimated at $10 million.

7221Y
Telephone Company Order Systems, Los Angeles--Theft.

The president of a telephone equipment distributor used a phone to enter orders for equipment, then picked the equipment up in a truck disguised as a telephone company truck. His company sold the equipment for several years before he was caught and convicted. He served two months in jail and now operates a computer security consulting firm.

7222Y
Insurance, Kansas--Liability, Civil Suit.

An insurance company lost a suit filed by a customer and appealed on the basis that it was not liable because a computer's print out of a renewal had the wrong data and time. The appeal was denied.

7233N
Horse Racing, Los Angeles--Fraud.

The manager of EDP and part of his staff were using the computer to analyze race horse handicaps making several thousand dollars each week.

7224N
Insurance Firm, Knoxville, Tennessee--Liability, Civil Suit.

A customer received a policy cancellation notice. The insurance company computer sent an invoice, after which the customer had an accident. The company claimed the policy was still cancelled and a computer error sent the invoice. The customer won the suit. The company is appealing.

7225N
Mailing List, Orange County, California--Unauthorized Use, Civil Suit.

An employee association claimed a political candidate requisitioned a mailing list of civil service employees to use for political campaigning.

7226N
Data Preparation Fraud, Lansing, Michigan--Unauthorized Act.

According to Computerworld, five keypunch operators were discarding traffic tickets issued to their own and fellow workers' cars. A meter-maid became suspicious after ticketing one car several days in a row. A three-part ticket with one copy to the supervisor as a control has been instituted.

7227N
Board of Elections, New York--Vote Fraud.

According to Computerworld, 10/11/71, an administrative assistant was charged by the FBI to have conspired with others to defraud the United States of its rights to have votes registered lawfully and correctly. 100 punch cards with names of unregistered voters were inserted into the voter registration list.

7228Y
University Computation Center, California--Information Theft.

A student copied 5000 passwords from the system file by using a text editor. The password file is now kept in scrambled form; sanctions were privately imposed on the student.

7229N
Public Safety, Iowa--Invasion of Privacy

According to Computerworld, 9/27/72, the State Commissioner of Public Safety is the defendant in a case where the plaintiff is represented by the Iowa Civil Liberties Union. The plaintiff claims a file on him was sent to the FBI claiming he is a known criminal, whereas although he had seven arrests, he had no convictions.

72210N
Credit Data Company--Fraud.

A former employee obtained credit reports by using the identification number of a legitimate subscriber. The number was changed; the former employee was not found. (Reported in Westin and Baker, Data Banks in a Free Society.)

72211N
Credit Data Company, Los Angeles--Fraud.

An employee tried to change information about himself. A keypunch operator discovered him when she thought it unusual that an employee would submit forms changing his own record. The employee was fired. (Reported in Westin and Baker, Data Banks in a Free Society.)

72212Y
Software Leasing Company--Thefts of Programs.

A blind man, president of the firm, and another man convinced programmers to take software from their employers and sell it to the leasing company, which then marketed the software.

72213Y
Aerospace Company--Theft of Patentable Processes.

Two employees scheduled for layoff took program listings describing secret processes to be patented. One employee was fired; one died of a heart attack.

72214Y
Data Bank, England--Theft of Dossiers.

An employee was selling dossiers for 5 Pounds on the London black market. He obtained them from an on-line B6700 data bank. He was caught by a program change that trapped on a preassigned name in the file.

72215Y
Industrial Espionage, Boston--Theft.

A programmer obtained confidential information, one record at a time, through his terminal. It was detected in an audit. A notice falsely stating a termination of deferred printer output logging was placed near his office. He immediately requested deferred output of the entire file. An undercover agent offered to pay him $80,000 for delivery of the output. Employee was fired and prosecuted.

7231Y
MICR, Reno--Counterfeiting Fraud.

Phony airline payroll checks with counterfeited MICR codes passed

successfully through a check reader, but were noticed in manual handling. No suspects have been identified.

7232N
Payroll, Brooklyn, New York--Fraud, Theft.

Suspects are alleged to have retained former employees' records in the payroll system. Addresses were changed for check mailing. $40,000 was taken.

7233N
Accounts Receivable, Lexington, Kentucky--Fraud.

In a medical center $61,800 in checks from insurance companies were diverted and computer records were changed to "uncollectable."

7234N
Property Taxes, Woonsocket, Rhode Island--Base Error.

A keypunch error caused the property rate to be based $7,000,950 too high, causing reduced tax revenues. There were five points at which the error could have been corrected.

7235N
Bank Service Bureau, San Francisco, California--Check Forgery.

According to Computerworld, 9/27/72, a check passer made photostat copies of a payroll check with payee and date changed. The MICR code failed to be read because the code did not use magnetic ink. The service bureau replaced the check with a correct substitute and let it pass because the bank had accepted the check.

7236N
Health Insurances, Oakland, California--Fraud.

An employee perpetrated a fraud on the insurance company.

7237Y
Painting Contractor--Embezzlement.

The controller embezzled by setting up dummy vendors in accounts payable. His actions were discovered when an analyst for the computer manufacturer was converting to a new system. The controller was fired.

7238N
Bank Computer, England--Embezzlement.

According to the London Times, several members of the bank's staff defaced MICR characters on their checks after crediting to payee's accounts. When the checks were rejected in reader, they destroyed them, stopping the debiting to their own accounts. About $3,000 was embezzled, the employees were convicted.

7239N
State Department of Welfare, California--Fraud.

In Los Angeles County, welfare grants are paid from vouchers based on punch cards. Someone put extra cards in computer to produce unauthorized grants. No suspects were identified.

7231ON
Bank, England--Embezzlement.

The six perpetrators mutilated their own checks. When rejected by the check reader, they were returned to the department run by the perpetrators for handling, where they were destroyed and never debited. The perpetrators were convicted of embezzling $8,300 but given suspended sentences of six months to one year.

7241N
Computer Time Sales, a county in New York--Theft.

The head programmer and several keypunch operators sold 250 hours of IBM 360/20 computer time without authorization. The programmer was convicted and fined $500.

7242N
Computer Training Institutes, Washington, D.C.--Deceptive Trade Practices.

Three large computer training institutes were indicted for alleged false advertising of the number of jobs and salaries available.

7243Y
Computer Time, Denver--Theft.

The perpetrator used Sigma 5 computer time at a state college for a personal, outside contract.

7244Y
Computer Service, Texas--Theft.

A high school student found a privileged password of the services analyst on a listing in a waste basket. He also obtained detailed specifications of the system. He used large amounts of computer time, played computer games, and obtained other customers' data. He was discovered when a computer operator noticed scratch tapes being read before being written. Restitution was made.

7245N
University Data Processing Center, Yugoslavia--Sedition and Hostility to the State

According to Computerworld, five students were suspected of

replacing business output data with antigovernment slogans. They were arrested.

7246N
City of Honolulu--Fraud.

According to Computerworld an ex-analyst in the Department of Information Systems claimed the mayor used $100,000 worth of city computer services for his reelection campaign.

7247Y
University Computation Center, California--Time Theft.

High school students were allowed to use free terminal services on one project. The employee involved left. Students continued to use the services, using new passwords they found. They used $3,000 worth of services before being caught. Now a "poaching bit" is set to alert operators to suspected account activity. Sanctions were imposed privately.

7248N
Telephone Service, England--Improper Use.

Engineers perpetrated "fiddles" for five years: they wired exchange equipment to accept certain numbers for access to outgoing trunk lines.

7311Y
University Computer Center, New Hampshire--Vandalism.

A student at a college with low-level privilege used a Trojan Horse technique within a file maintenance program he wrote. When an operator ran it at privileged level, the program took over the executive and invoked another resident privileged program that removed all evidence of penetration. Systems programmers discovered the extra privileged program in a core dump. Logical matching of privilege and ID of each program set for a maximum privilege solved the problem. No action was taken against the student.

7312Y
Aerospace Company--Vandalism

Employees returning from a strike sabotaged the on-line parts inventory and ordering system.

7313Y
University Computer Center, Indiana--System Crash Vandalism.

A "crash program" resulted in a large loss of time and money.

7321N
IBM and Telex, Texas--Industrial Sabotage.

IBM and Telex engaged in civil suits claiming industrial espionage and monopoly domination of the peripherals market.

7322Y
State of Illinois--Theft.

A computer operator was bribed for $10,000 to steal a tape reel of driver registration addresses normally sold by the Driver Registration for $70,000.

7323Y
Campus Computer Usage, Indiana--Theft and Unauthorized Use.

There was theft and improper usage of a CRT display unit and acoustic compiler.

7324N
Vote Fraud, California--Vote Count Fraud.

The county vote counting system produced identical vote counts in several precincts. Up to four precincts had identical vote counts. Fraud was suspected but no suspect found.

7325N
Homes in Chicago--Burglary.

$1 million in negotiable securities was stolen from burglarized homes. A raid on the suspects' residence produced a computer output listing of affluent supermarket owners.

7326N
A U.S. Security Agency--Espionage.

Hidden wireless transmitters found inside a CPU at a security agency were capable of transmitting to a truck with electronic receiving equipment.

7327Y
Equity Funding Insurance Company Class Action Civil Suit.

The suit claims IBM failed to inform its customers about the vulnerability of its products to fraud and failed to provide sufficient security in its products.

7331Y
1-1/2 million Union Dime Savings Bank Embezzlement, New York--Embezzlement.

The suspect manipulated hundreds of accounts through his teller

terminal in the computer system. He was caught when a raid on a bookie showed large bets placed by the suspect. He was prosecuted for embezzling $1.5 million by the Manhattan District Attorney's Office.

7332Y
Equity Funding Life Insurance, Los Angeles--Alleged Fraud.

Equity created 56,000 fake insurance policies and sold them to re-insurers. Insurance Commissioners in at least three states are investigating. The estimated loss is $2,000 million.

7333
Saving and Loan Embezzlement, California--Alleged Embezzlement.

A programmer used a terminal to program the transfer of $100 from sequential accounts, A-D, into his wife's account. His wife withdrew $500 each time in a different disguise, totaling $4,000; $3120 was recovered. The theft was discovered when a customer complained and exception reports showed unusual no-book transfers. A Federal indictment was expected.

7334N
Commodity Option Sales, California--Possible Fraud or Vandalism.

The State Department of Corporations claims the firm should be barred from selling commodity options. The firm claimed lightning struck the computer causing destruction of the master files and inability to recover, in turn causing millions of dollars of errors.

7335
Dividend Payments--Embezzlement.

A clerk caused the computer to issue dividend checks to former shareholders, but addressed to an accomplice, and then to erase records of the checks. The clerk was convicted for embezzling $33,000.

7341N
Insurance Company, Michigan--Fraud.

According to Computerworld, an agent used computer analysis of life insurance to confuse policy holders, saying the computer recommended his policy over theirs. About 100 policy holders were victims. The State Commerce Department's Insurance Bureau prosecuted.

7342Y
University Computer Center, Indiana--Theft of Services.

Theft of account password and use of computer services led to a conviction for obtaining services under false pretenses.

7343Y
University Computer Center, Massachusetts--Theft of Services.

A student wrote a program that obtained the account number when a user attempted to log in, and then declared the system was unavailable. The student then used terminal-time credit on the account for his own purposes.

7344N
Time Sharing Service, California--Theft. Investigation charges dropped.

Three weeks of unauthorized use of a demonstration account number, for three to eight hours at a time, was discovered as a result of irregularities observed in computer operation. The sheriff's investigation was dropped.

SOURCE: Donn B. Parker, Susan Nycum, and S. Stephen Oura, Computer Abuse, Prepared for the National Science Foundation RANN NSF/RA/S-73-017, under Grant No. GI-37226 (Menlo Park, CA: Stanford Research Institute, 1973), pp. 91-112. (Quoted verbatim with permission.)

APPENDIX B

Details of Survey of Information Resources

APPENDIX B

DETAILS OF SURVEY OF INFORMATION RESOURCES

Purpose of Survey

The survey was designed with the objective of developing the widest possible network of information resources for computer fraud cases. The intent was to locate, identify and describe pertinent facts of all reported cases.

Selection of Survey Recipients

Selection of survey recipients was made on a judgmental basis since there was no way of determining the appropriate universe from which to draw a statistical sample. Individuals, organizations and agencies believed to be most likely to have information or knowledge about computer-assisted fraud cases were selected. In many instances, library references were used to develop the mailing lists. However, some survey recipients were selected by virtue of referral by others or by this author having read or heard about them such that it was believed they would at least have considerable interest in the project. The following sources were thought to offer the best potential for computer fraud case information:

A. Selected accounting firms
B. Selected consultants, educators and researchers
C. State boards of public accountacy
D. State societies of certified public accountants
E. Selected business and EDP periodicals
F. Selected information centers and regulatory agencies
G. Selected business, commercial, industry, professional, and trade organizations/associations
H. Selected computer vendors

I. Selected insurance companies
J. State officials having supervision of insurance activities.

The names of all questionnaire recipients are shown in Exhibit B-6.

National and regional public accounting firms were selected to include the "Big Eight" and others based on personal recognition. In addition, the leading accounting firms in one state were surveyed. Management consulting firms were selected from a reference resource primarily on this author's recognition as being a leader in the field. Educators were selected chiefly on the basis of their published works or by another's recommendation. Periodical resources were selected by reference to library or this author's subscription copies. All other categories of survey recipients were selected on a judgmental basis from library reference resources.

A questionnaire with an accompanying letter was mailed to all survey participants (see Exhibits B-2, B-3, B-4, and B-5). Several mailings were made with the first being sent on July 12, 1973 and the last letter on August 30, 1973. The first response was received July 16, 1973 and the last on November 19, 1973. The bulk of the responses was received within the period from July 16, 1973 through August 23, 1973.

Responses

A count of the results showed that 132 responses were received from the 371 "good" survey recipients for a 35% rate. Thirty-two of the respondents had been referred by other respondents. Five survey questionnaires were returned with each envelope indicating the addressee

had moved and left no forwarding address. One questionnaire was returned by a parent organization with the notation that the activity to whom the survey had been addressed had been terminated. Eleven addressees were determined to be duplicates, i.e., different names or titles but obviously the same activity at the same address or the same activity but different addresses.

Statistics for the results of the questions asked are presented in Exhibit B-1. It should be noted that in some cases the survey recipients responded via individual letter, or memorandum or telephone and thus did not return the questionnaire. In each of these cases, however, sufficient information was given either implicitly or explicitly so that some of the survey questions could be included in the response tallies. One recipient in each of the A, B, C, D, and E categories returned the qeustionnaire and also sent an accompanying letter.

Exhibit B-1

RESULTS OF SURVEY FOR COMPUTER FRAUD CASES

Questionnaire Item	TOTALS	Category of Recipients A	B	C	D	E	F	G	H	I	J
Survey questionnaires returned	97	19	8	18	17	6	7	5	2	3	12
Substitute letters received	32		6	3	1	2	10	7			3
Substitute telecon's	2					1	1				
Substitute memo received	1					1					
Total responses	132	19	14	21	18	10	18	12	2	3	15
Questionnaires sent	371	31	25	54	53	27	46	57	9	14	55
Response rate (nearest %)	35	61	56	36	34	40	40	20	20	20	30
% of respondents having no CAF files (line 1f total responses)	70	69	30	100	100	50	56	67	50	unk	80
1. In reference to computer-assisted fraud, we maintain files of:											
a. First-hand (raw) data	7	1	4			1				1	
b. Published cases	17	2	4			4	3	2		1	1
c. Other resouces	9	1	2			1		3		1	1
d. News media reports	23	5	5			5	5			1	2
e. Library material	9	1	1				2	3	1	1	
f. No such cases	93	13	4	21	18	5	10	8	1	1	12
2. From the files/resources maintained, a researcher can determine for subject computer-assisted fraud (CAF) cases:											
a. Type of industry and/or business in which CAF occurred	12	4	2			3	1		1		1
b. Amount of direct CAF dollar loss	8		2			3	1				2

Exhibit B-1 (continued)

Questionnaire Item	TOTALS	Category of Recipients A	B	C	D	E	F	G	H	I	J
2. (continued)											
c. Amount of recovery via fidelity bond insurance	2										2
d. Professional liability insurance claims awarded	0										
e. Court-awarded damage or recovery claims	3		1			1	1				
f. Method of discovery of the CAF	11	3	2			2			1	1	2
g. Role of the CPA (if any) in connection with the cases	8	3	1			2					2
h. The weaknesses in auditing procedures	9	3	2			2			1		1
i. The weaknesses in internal control	9	2	3			2			1		1
j Other relevant information	9	1	3			2			1		2
3. Grant access to resources	13	2	4			2	1		1		3
a. Grant access with exceptions	4	2				1				1	
b. Will not grant access	11	4		3	3		1				

Exhibit B-2

QUESTIONNAIRE ON COMPUTER-ASSISTED FRAUD

NOTE: Please check appropriate responses and return to Prof. C. R. Wagner at Creighton University.

1. In reference to computer-assisted fraud, we maintain files of:

_____First-hand (raw) data	_____News media reports
_____Published cases	_____Library material
_____Other resources	_____No such cases

2. From the files/resources maintained, a researcher can determine for subject computer-assisted fraud (CAF) cases:

_____Type of industry and/or business in which CAF occurred
_____Amount of direct CAF dollar loss
_____Amount of recovery via fideltiy bond insurance
_____Professional liability insurance claims awarded
_____Court-awarded damage or recovery claims
_____Method of discovery of the CAF
_____Role of the CPA (if any) in connection with the cases
_____The weaknesses in auditing procedures
_____The weaknesses in internal control
_____Other relevant information

3. Given assurances of anonymity for persons and firms involved in such CAF cases, we would grant access to the sources and kinds of information indicated by the above-checked items for use in Wagner's dissertation effort.

_____Yes _____No _____With exceptions

4. A "news" note about your research effort has been disseminated via our communication media.

_____Yes _____Date _____No

5. Other remarks: _____ (Please continue on reverse side) _____

Respondent's Name _____ Title _____

Organization _____ Date _____

Address _____

_____

CREIGHTON UNIVERSITY
OMAHA, NEBRASKA 68131

COLLEGE OF
BUSINESS ADMINISTRATION
DEPARTMENT OF ACCOUNTING

Exhibit B-3

Gentlemen:

My doctoral dissertation subject, Computer-Assisted Fraud: Auditing Procedures and the Auditor's Responsibility for Prevention and Detection of Fraud, has recently been approved by my Supervisory Committee at University of Nebraska -- Lincoln. In order to extend the opportunity for input to this research effort to the greatest number of interested persons and thus capture as much of the available relevant data as possible, I am attempting to develop the widest possible network of information sources.

Briefly, I hope to determine the extent of computer-assisted fraud; to ascertain the reasons for its occurrence and how it was discovered in each case; to study each case in an effort to uncover weaknesses in auditing procedures; to examine the characteristics of a computer environment and computer-assisted fraud in relation to auditing procedures and generally accepted auditing standards; and to re-assess the question of the auditor's degree of responsibility for the prevention and detection of fraud in a computer environment.

I would certainly welcome dissemination of notice of this dissertation effort through your channels of communication. Although I intend to follow a structured approach in accumulating and evaluating pertinent information, I would also welcome unstructured responses giving advice, encouragement, information, and additional sources of material. My immediate research objectives are to:

1. Identify and describe all reported -- and as many acknowledged -- cases of computer-assisted fraud as possible.

2. Identify the reasons for computer-assisted fraud occurrences in terms of weaknesses in internal control.

3. Identify the reasons for computer-assisted fraud occurrences in terms of weaknesses in auditing procedures.

Would you please complete the enclosed questionnaire and return it in the stamped, addressed envelope provided? I will greatly appreciate your cooperation in this matter.

Sincerely,

Charles R. Wagner

Charles R. Wagner
Assistant Professor of Accounting

2 Enclosures

CREIGHTON UNIVERSITY
OMAHA, NEBRASKA 68131

COLLEGE OF
BUSINESS ADMINISTRATION
DEPARTMENT OF ACCOUNTING

Exhibit B-4

As you can see by the enclosures I am engaged in a research effort involving auditing responsibilities and computer-assisted fraud. The letter and questionnaire have been mailed to numerous organizations, governmental agencies, and periodicals which I believe should be interested in one or more facets of this dissertation subject.

You have been named by a respondent as having a particular interest and/or expertise in one or more aspects of computer security and/or fraud cases. Therefore, I extend a special invitation to you to take a minute or so to complete the questionnaire and to return it to me. I would also greatly appreciate any additional advice or information that you deem suitable.

Thanks very much for your assistance in this matter.

Sincerely yours,

Charles R. Wagner
Assistant Professor of Accounting

CRW:jw
Enclosures

CREIGHTON UNIVERSITY
OMAHA, NEBRASKA 68131

COLLEGE OF
BUSINESS ADMINISTRATION
DEPARTMENT OF ACCOUNTING

Exhibit B-5

As you can see by the enclosures I am engaged in a research effort involving auditing responsibilities and computer-assisted fraud. The letter and questionnaire have been mailed to numerous organizations, governmental agencies, and periodicals which I believe should be interested in one or more facets of this dissertation subject.

Since I have heard about, or read, some of your work in this area, I know that you also are concerned about one or more aspects of computer security and/or fraud cases. Therefore, I extend a special invitation to you to take a minute or so to complete the questionnaire and to return it to me. I would also greatly appreciate any additional advice or information that you deem suitable.

Thanks very much for your assistance in this matter.

Sincerely yours,

Charles R. Wagner
Assistant Professor of Accounting

CRW:jw
Enclosures

Exhibit B-6

LIST OF SURVEY RECIPIENTS

A--Selected Accounting Firms

Alexander Grant & Company, 8401 W. Dodge Road, Omaha, NE 68814
Arnett and Foster, Roger L. Osborne, CPA, Manager, P. O. Box 2629, Charleston, WV 25301
Arthur Andersen & Co., 1700 Farnam Street, Omaha, NE 68102
Arthur Young & Co., 525 Barker Boulevard, Omaha, NE 68102
Coopers & Lybrand, 500 City National Bank Bldg., Omaha, NE 68102
Elmer Fox & Co., 200 Park Plaza West Bldg., Omaha NE 68131
Ernst & Ernst (Beresford), Union Commercie Building, Cleveland, OH 44115
Ernst & Ernst, Gene Sovecka, 515 S. Flower St., Suite 2700, Los Angeles, CA 90071
Gessner & Anthony, Samuel J. Anthony, CPA, Medical Tower, Wheeling, WV 26003
Haskins & Sells, 1444 Woodmen Tower, Omaha, NE 68102
Hayflich & Steinberg, Jerome B. Hayflich, CPA, P. O. Box 2094, Huntington, WV 25721
Hertz, Herson & Company, Robert B. Nadel, Partner, Two Park Avenue, New York, NY 10016
Howell & Paterno, Gary W. Turner, CPA, P. O. Box 1191, Charleston, WV 25324
H. S. Hutzell & Co., W. Foster LaRue, Jr., CPA, 512 Laconia Building, Wheeling, WV 26003
John Wiseman & Compnay, John W. Bole, CPA, 1219 Chapline Street, Wheeling WV 26003
Mason & Company, David H. Bashaw, CPA, P. O. Box 1204, Bechley, WV 25801
McGladrey, Hansen, Dunn & Co., Leo Burger, Partner, 828 Merchants Bank Bldg., Cedar Rapids, IA 52401
Peat, Marwick, Mitchell & Co., Kiewit Plaza Building, Omaha, NE 68131
Philip P. Cox, CPA, P. O. Box 1183, Martinsburg, WV 25401
Price Waterhouse & Company, 60 Broad Street, New York, NY 10004
S. D. Leidesdorf & Company, 111 East Wacher Drive, Chicago, IL 60601
S. D. Leidesdorf & Company, Elliott R. Green, 125 Park Avenue, New York, NY 10017
Seymour Schneidman & Company, Arnold Schneidman, Partner, 405 Park Avenue, New York, NY 10022
Somerville & Company, William L. Shomo, CPA, P. O. Box 1236, Huntington, WV 25714
Stone, Gray and Company, 101 South Madison Street, Denver, CO 80209
Tanner and Tanner, Douglas H. Tanner, CPA, P. O. Box 588, Morgantown, WV 26505
Taylor & Callaway, Carl M. Callaway, CPA, P. O. Box 2327, Huntington, WV 25724

Toothman & Company, C. Eugene Toothman, CPA, P. O. Box 629, Clarksburg, WY 26301
Touche Ross & Company, 780 Northstar Center, Minneapolis, MN 55402
Witschey, Harman & White, Charles L. Badger, CPA, P. O. Box 129, Charleston, WV 25321
Witschey, Harman & White, Everett L. Thompson, CPA, P. O. Box 1603, Parkersburg, WV 26101

B--Selected Consultants, Educators, and Researchers

Prof. Brandt T. Allen, Graduate School of Business, University of Virginia, Charlottesville, VA 22904
Arthur D. Little, Inc., Acorn Park, Cambridge, MA 02140
Tom Bianco, Computer Audit Corporation, 1320 Fenwick Lane, Silver Springs, MD 20910
Booz, Allen and Hamilton, Inc., 245 Park Avenue, New York, NY 10017
Dr. Douglas R. Carmichael, Director, Technical Research, American Institute of CPAs, 666 Fifth Avenue, New York, NY 10019
Computer Resources, Inc., Jerome Priest, 770 Post Road, Darien, CT 06820
Dr. J. Couger, Prof. Management & Computing Science, School of Business Administration, Colorado Springs, CO 80907
Cresap, McCormick and Paget, Inc., 245 Park Avenue, New York, NY 10017
Prof. Gordon B. Davis, School of Business Administration, University of Minnesota, Minneapolis, MN 55455
Dun and Bradstreet, Inc., 99 Church Street, New York, NY 10017
EDP Security, Inc., Century City, Los Angeles, CA 90067
Dr. James C. Emery, Professor of Management, Wharton School Finance & Commerce, University of Pennsylvania, Philadelphi, PA 19104
Ken Falor, Cullinane Corporation, One Boston Place, Boston, MA 02108
Prof. David Farber, University of California at Irvine, Irvine, CA 92664
Wm. Howard Gammon, Ass't Prof., American University (CTA), Washington, C. S. 20016
George S. May International Co., 111 South Washington Street, Park Ridge, IL 60068
H. B. Maynard & Co., Inc., 2040 Ardmore Boulevard, Pittsburgh, PA 15221
McKinsey & Company, Inc., 245 Park Avenue, New York, NY 10017
Mesa Computer Utilities, Richard Murphy, 1607 Mitchell Avenue, St. Joseph, MO 64503
Donn B. Parker, Stanford Research Institute, Menlo Park, CA 94025
Pinkerton's, Inc., 100 Church Street, New York, NY 10017
Unicorn Systems Company, 3807 Wilshire Blvd., Los Angeles, CA 90010
Joe Wasserman, Computer Audit Systems, Inc., 725 Park Avenue, East Orange, NJ 07017

Harold Weiss, Automation Training Center, 1930 Isaac Newton Square East, Reston, VA 22090

Dr. Marvin M. Wofsey, School of Government and Business Administration, George Washington University, Washington, D. C. 20006

C--State Boards of Public Accountacy

Alabama State Board of Public Accountancy
Alaska State Board of Public Accountancy
Arizona State Board of Accountancy
Arkansas State Board of Accountacy
California State Board of Accountancy
Colorado State Board of Accountancy
Connecticut State Board of Accountancy
Delaware State Board of Accountancy
District of Columbia Board of Accountancy
Florida State Board of Accountancy
Georgia State Board of Accountancy
Guam Territorial Board of Public Accountancy
Hawaii Board of Accountancy
Idaho State Board of Accountancy
Illinois Committee on Accountancy and Department of Registration and Education
Indiana State Board of Public Accountancy
Iowa Board of Accountancy
Kansas Board of Accountancy
Kentuckey State Board of Accountancy
Louisiana State Board of CPAs of Louisiana
Maine Board of Accountancy
Maryland State Board of Public Accountancy
Massachusetts Board of Public Accountancy
Michigan Board of Accountancy
Minnesota State Board of Accountancy
Mississippi State Board of Public Accountancy
Missouri State Board of Accountancy
Montana State Board of Public Accountancy
Nebraska State Board of Public Accountancy
Nevada State Board of Accountancy
New Hampshire Board of Accountancy
New Jersey Board of Certified Public Accountants
New Mexico State Board of Public Accountancy
New York State Board for Public Accountancy
North Carolina State Board of CPA Examiners
North Dakota State Board of Accountancy
Accountancy Board of Ohio
Oklahoma State Board of Public Accountancy
Oregon Board of Accountancy
Pennsylvania State Board of Examiners of Public Accountants

Puerto Rico Board of Accountancy
Rhode Island Board of Accountancy
South Carolina Board of Accountancy
South Dakota Board of Accountancy
Tennessee State Board of Accountancy
Texas State Board of Public Accountancy
Utah Committee for Public Accountancy
Vermont State Board of Accountancy
Virginia State Board of Accountancy
Virgin Islands Board of Public Accountancy
Washington State Board of Accountancy
West Virginia Board of Accountancy
Wisconsin Accounting Examining Board
Wyoming The State Board of Accountancy

D--State Societies of Certified Public Accountants

Alabama Society of Certified Public Accountants
Alaska Society of Certified Public Accountants
Arizona Society of Certified Public Accountants
Arkansas Society of Certified Public Accountants
California Society of Certified Public Accountants
Colorado Society of Certified Public Accountants
Connecticut Society of Certified Public Accountants
Delaware Society of Certified Public Accountants
D. C. Institute of Certified Public Accountants
Florida Institute of Certified Public Accountants
Georgia Society of Certified Public Accountants
Hawaii Society of Certified Public Accountants
Idaho Society of Certified Public Accountants
Illinois Society of Certified Public Accountants
Indiana Association of Certified Public Accountants
Iowa Society of Certified Public Accountants
Kansas Society of Certified Public Accountants
Kentucky Society of Certified Public Accountants
Society of Louisiana Certified Public Accountants
Maine Society of Certified Public Accountants
Maryland Association of Certified Public Accountants
Massachusetts Society of Certified Public Accountants
Michigan Association of Certified Public Accountants
Minnesota Society of Certified Public Accountants
Mississippi Society of Certified Public Accountants
Missouri Society of Certified Public Accountants
Montana Society of Certified Public Accountants
Nebraska Society of Certified Public Accountants
Nevada Society of Certified Public Accountants
New Hampshire Society of Certified Public Accountants
New Jersey Society of Certified Public Accountants
New Mexico Society of Certified Public Accountants

New York State Society of Certified Public Accountants
North Carolina Association of Certified Public Accountants
North Dakota Society of Certified Public Accountants
Ohio Society of Certified Public Accountants
Oklahoma Society of Certified Public Accountants
Oregon Society of Certified Public Accountants
Pennsylvania Institute of Certified Public Accountants
Instituto De Contadores Publicos Authrizados De Puerto Rico
Rhode Island Society of Certified Public Accountants
South Carolina Association of Certified Public Accountants
South Dakota Society of Certified Public Accountants
Tennessee Society of Certified Public Accountants
Texas Society of Certified Public Accountants
Utah Association of Certified Public Accountants
Vermont Society of Certified Public Accountants
Virgnia Society of Certified Public Accountants
Virgin Islands Society of Certified Public Accountants
Washington Society of Certified Public Accountants
West Virginia Society of Certified Public Accountants
Wisconsin Society of Certified Public Accountants
Wyoming Society of Certified Public Accountants

E--Selected Business and EDP Periodicals

Administrative Management
Barron's
Business Week
Collegiate News and Views
The Commerical and Financial Chronicle
Computer Decisions
Computerworld
Data Management
Datamation
Defense Management Journal
Dun's Review
Finance
Financial Executive
Financial World
Forbes
Fortune
Government Data Systems
Information and Records Management
Infosystems
The Internal Auditor
The Journal of Accountancy
Knickerbacher News
Management Accounting
Modern Data

The Practical Accountant
Software Digest
The Wall Street Journal

F--Selected Information Centers and Regulatory Agencies

Air Force Audit Agency
Army Audit Agency
American National Standards Institute
American Stock Exchange
Applied Computer Research
Auerbach Corporation
Automated Data Management Services, General Services Administration
Battelle Memorial Institute
Bell and Howell Company
Cambridge Computer Associates, Inc.
Capital Systems Group, Inc.
Compustat, Investors Management Sciences
Conference Board, Inc.
Defense Contract Audit Agency
Deputy Assistant Secretary of Defense (Audit)
Federal Bureau of Investigation
Fraud Section, Department of Justice
General Accounting Office
Internal Renenue Service
International Data Corporation
Institute for Computer Sciences and Technology
Kiewit Computer Center, Dartmouth College
Midwest Stock Exchange
Moody's Investors Service, Inc.
Mutual of Omaha Insurance Co. Lending Library
National Archives and Records Service (GSA)
National Clearinghouse for Mental Health Information, Crime and Delinquency Section
National Technical Information System, U. S. Department of Commerce
Naval Audit Service
New York Stock Exchange
New York Times Company
N. W. Ayer and Son, Inc.
Pacific Coast Stock Exchange
Predicasts, Inc.
Rand Corporation Library
Securities and Exchange Commission
Small Business Administration
Standard and Poor's Corporation
System Development Corporation
Time, Inc., Information Processing Department
Treasury Department
TRW Systems Group

University of Georgia, Computer Software Management Information Center (COSMIC)
USAF, JAG, Legal Information Thru Electronics (LITE)
U. S. Department of Commerce, Office of Audits
U. S. Library of Congress

G--Selected Business, Commercial, Industry, Professional, and Trade Organizations/Associations

Administrative Management Society
American Accounting Association
American Association of Attorney-Certified Public Accountants
American Bankers Association
American Bar Association
American Finance Association
American Federation of Information Processing Societies
American Federation of Police
American Institute of Certified Public Accountants
American Insurance Association
American Management Association
American Savings and Loan Institute
American Society for Industrial Security
American Society of Women CPAs and Accountants
Armed Forces Management Association
Association for Computing Machinery
Association for Systems Management
Association of Computer Programmers and Analysts
Association of Data Processing Service Organizations
Bank Administration Institute
Center for the Study of Automation and Society
Chamber of Commerce of the United States
Data Processing Management Association
EDP Auditors Association
Federal Government Accountants Association
Financial Analysts Federation
Information Industries Association
Institute of Chartered Financial Analysts
Institute of Internal Auditors
Institute of Management Sciences
Insurance Accounting and Statistical Association
Insurance Crime Prevention Institute
Insurance Information Institute
Insurance Services Office
Investors League
Life Office Management Association
Loss Executives Association
National Association of Accountants
National Association of Independent Insurers

National Association of Insurance Commissioners
National Association of Investment Clubs
National Association of Securities Dealers
National Association of State Auditors, Comptrollers and Treasurers
National Association of State Boards of Accountancy
National Federation of Independent Business
National Science Foundation
National Sheriff's Association
National Small Business Association
National Society of Public Accountants
Operations Research Society of America
Society for Automation in Business
Society for Management Information Systems
Society of Certified Data Processors
Society of Data Educators
Society of Insurance Accountants
Surety Association of America

H--Selected Computer Vendors

Burroughs Corporation
Control Data Corporation
General Electric Company
Hewlett-Packard Company
Honeywell, Inc.
International Business Machines Corporation
National Cash Register Company
Sperry Rand Corporation
Univac

I--Selected Insurance Companies

Aetna Casualty and Surety Co.
Buckeye Union Insurance Co.
Federal Insurance Company
Fidelity and Casualty Company of New York
Fidelity and Deposit Company
General Reinsurance Corporation
Hartford Accident and Indemnity Co.
Insurance Company of North America
Liberty Mutual Insurance
Maryland Casualty Company
Mutual of Omaha
National Surety Corporation
Travelers Idemnity Co.
United States Fidelity and Guaranty Co.

J--State Officials Having Supervision of Insurance Activities

Alabama	Walter S. Houseal, Superintendent of Insurance
Alaska	A. W. Lingle, Director of Insurance
Arizona	George A. Bushnell, Director of Insurance
Arkansas	John Norman Harkey, Commissioner
California	Richard S. L. Roddis, Insurance Commissioner
Colorado	J. R. Barnes, Commissioner of Insurance
Connecticut	William R. Cotter, Commissioner of Insurance
Delaware	Robert A. Short, Commissioner of Insurance
District of Columbia	Albert F. Jordan, Superintendent
Florida	Broward Williams, Insurance Commissioner
Georgia	James L. Bentley, Insurance Commissioner
Guam	Joaquin C. Guerrero, Insurance Commissioner
Hawaii	S. I. Hashimoto, Commissioner of Insurance
Idaho	John R. Blaine, Commissioner of Insurance
Illinois	John F. Bolton, Jr., Director of Insurance
Indiana	J. G. Wood, Sr., Commissioner of Insurance
Iowa	L. R. Worthington, Commissioner of Insurance
Kansas	Frank Sullivan, Commissioner of Insurance
Kentucky	S. R. Woodall, Jr., Commissioner of Insurance
Louisiana	D. A. Guglielmo, Commissioner of Insurance
Maine	George F. Mahoney, Commissioner
Maryland	Norman Polovoy, Commissioner
Massachusetts	C. Eugene Farnam, Commissioner of Insurance
Michigan	David J. Dykhouse, Commissioner of Insurance
Minnesota	Joe Haveson, Acting Commissioner of Insurance
Mississippi	Walter D. Davis, Commissioner of Insurance
Missouri	Robert D. Scharz, Superintendent of Insurance
Montana	E. V. "Sonny" Omholt, Commissioner of Insurance
Nebraska	Frank J. Barrett, Director of Insurance
Nevada	Louis T. Mastos, Insurance Commissioner
New Hampshire	D. Knowlton, Commissioner of Insurance
New Jersey	C. R. Howell, Commissioner of Banking & Insurance
New Mexico	R. F. Apodaca, Superintendent of Insurance
New York	R. E. Stewart, Superintendent of Insurance
North Carolina	Edwin S. Lanier, Commissioner of Insurance
North Dakota	K. O. Nygaard, Commissioner of Insurance
Ohio	William R. Morris, Director of Insurance
Oklahoma	J. B. Hunt, Commissioner & President, State Ins. Bd.
Oregon	J. R. Faulstich, Insurance Commissioner
Pennsylvania	David O. Maxwell, Commissioner of Insurance
Philippines	F. Y. Mandanas, Insurance Commissioner
Puerto Rico	Jorge Soto Garcia, Commissioner of Insurance
Rhode Island	W. R. Campbell, Commissioner of Insurance
South Carolina	C. W. Gambrell, Chief Insurance Commissioner
South Dakota	W. E. Dirks, Commissioner of Insurance
Tennessee	D. M. Pack, Commissioner of Insurance & Banking

Texas	Clay Cotten, Commissioner of Insurance
Utah	C. N. Ottosen, Commissioner of Insurance
Vermont	J. H. Hunt, Commissioner of Banking & Insurance
Virginia	T. Nelson Parker, Commissioner of Insurance
Virgin Islands	Cyril E. King, Commissioner of Insurance
Washington	L. I. Kueckelhan, Insurance Commissioner
West Virginia	F. R. Montgomery, Commissioner of Insurance
Wisconsin	R. D. Haase, Commissioner of Insurance
Wyoming	William G. Walton, Commissioner of Insurance

APPENDIX C

Summaries of Selected Computer Programs for Auditors

SUMMARIES OF SELECTED COMPUTER PROGRAMS FOR AUDITORS

ABLE--THE ACCOUNTING LANGUAGE

Evansville Data Processing Corporation
1010 South Weinback Avenue
Evansville, Indiana 47714

Combination interpretive-compiler and accounting system capable of preparing almost any financial statement at the same time it generates an audit trail. It will keep payroll records and prepare 941A and W2 forms. Through the use of the accounting language, it can automatically prepare most standard, adjusting and variable entries from an unlimited chart of accounts. There are no output format restrictions and it can compute depletion as well as any other entry based on the client's own chart of accounts.

ACCOUNTS RECEIVABLE AGING

Klane, Gillman & Schecter
3033 Excelsior Boulevard
Minneapolis, Minnesota 55416

Breaks down accounts receivable into current, 30-, 60-, over 90-day age classifications. Adaptable to most accounts receivable systems.

AUDASSIST--AN INFORMATION ANALYSIS AND RETRIEVAL SYSTEM FOR AUDITORS AND CONSULTANTS

Alexander Grant & Co.
One First National Plaza
Chicago, Illinois 60670

There are three phases to AUDASSIST--data conversion, processing, and output. Any file on computer tape may be reformatted to a fixed format AUDASSIST tape. During processing selected information may be

extracted to meet the user's objectives. There are several choices of printed output--standard listing, stratification listing, or positive confirmation formats. The following functions may be used in any order required to achieve the desired results.

Age Calculation--Allows the user to obtain the age of a data record. Must choose one of four date formats. May determine age based on business days or calendar days. May determine time since last activity data.

Stratification--Classifies an amount or age into as many as five continuous categories.

Sampling--Provides for use of three systematic random sampling techniques. User may choose every nth item, every random 2nth item, or every random nth item from the universe, which may be an entire file or a stratified file.

Calculate--Performs basic mathematical operations of add, subtract, multiply, or divide.

Tag Setting and Testing--Used to design logic for selecting accounts or for routing processing of information.

AUDIT-THRU

Computer Resources Corporation
215 Danbury Road--P. O. Box 431
Wilton, Connecticut 06797

Retrieval and reporting system in which selection of data is based on specification of defined criteria. Data selected may be stratified. Has the power to calculate, sort, select, total, and cross-foot. May be used on any file. Need to compile only once.

CARS--COMPUTER AUDIT RETRIEVAL SYSTEM

Computer Audit Systems, Inc.
725 Park Avenue
East Orange, New Jersey 07017

A retrieval system which will perform a variety of audit functions on stored data. The program is independent to the form of the data base and to the type of record format. Record formats may be blocked, unblocked, fixed length or variable length. Does not require the editing or restructuring of the data base. Has extended boolean logic capabilities. Handles auditing functions singly or in combination.

Extraction--Select only those records which meet predetermined criteria. Input parameters specify selection based on inclusion or exclusion, exact matches, values within a given range, or combination/relational tests.

Mathematics--Provides addition, subtraction, division, and multiplication for, among others, summation, cross-footing and balancing, and extension procedures.

Counting--Take item and amount of all records meeting certain criteria, without extracting the individual records.

Subtotaling--Print subtotal when there is a change in a given sequence. Three levels are provided--minor, intermediate, and major, in addition to final totals.

Summarization--Totals amounts for all records within a given sequence. Result may be tested for extraction, printed, or written on tape.

Aging--Allows comparison of dates in the records to a given date, with stratification of each record into under 30 days, over 30 days, over 60 days, over 90 days, over 120 days, and over 150 days.

Sampling--Selection may be based on a given interval beginning with a given starting point, or by the use of random numbers. There are three sampling strata.

Sequence Checking--Examines input file for ascending order.

Missing Ticket or Sequence Gap Detection--Examines input file for consecutive numbering.

Comparison of Two Files--Match two files on given sequence and compare data in one file to data of the other.

Printing and/or Tape Output--Report format determined by user. Complete detail listings or a listing of control totals only. Up to 18 fields may be selected for output either on hard copy or magnetic tape.

Confirmation Notices--Variable output to fit pre-printed confirmation letters. Extracted records may be separated for positive and negative confirmations.

DATAMACS--AUTOMATIC TEST DATA GENERATOR

Management and Computer Services, Inc.
104 Park Towne Place East
Philadelphia, Pennsylvania 19130

Designed to work through the use of control cards interspersed through the data division of a COBOL program, in either a load-and-go or stand-alone environment. Uses a language similar in syntax to COBOL with control cards in the source deck for normal pattern of compiling and testing. Generates every kind of file, to include tape and disk, in one step. In stand-alone, data files can be generated for use with other programs written in any language by communication with DATAMACS through control cards and an abbreviated file description.

EDP AUDITOR

Cullinane Corporation
One Boston Place
Boston, Massachusetts 02108

Any type of file--tape, card, disk, or other device--can be produced as selected records for audit or test data purposes or as condensed (selected fields) records. Fields may be added, deleted, expanded, reformatted, or re-ordered. Multiple files or selected fields therefrom may be merged. Variable report formats with minor, intermediate, major, and conditional control fields. Summary, control, detail,

and statistical reports. Unlimited computations which include group statistics, percentages, averages, maxima and minima, arithmetic operators, random number generation, sampling selections, etc. Produces audit verification notices. Prepares name and address labels. Extensive default structure. Variety of edit options. File comparisons.

EPG-II--EDIT PROGRAM GENERATOR

Computer Sciences Corporation
9841 Airport Boulevard
Los Angeles, California 90045

Generates edit programs which read input transactions, verify key numbers to external files or tables, edit the format and content of input records to the edit specifications, make relational tests between input records, accumulate batch and grand total balances and check these to batch control inputs, format and write output files for subsequent processing, and prepare printed processing logs. These logs constitute journals of all batches and show specified and computed totals. Within each batch, detected errors are printed along with an image of the error record. EPG-II reads coded edit language, assembles and compiles the statements into the edit program, diagnoses code for validity, and prints English language documentation.

GENERAL ELECTRIC TIME-SHARING SERVICE

General Electric Company
Information Service Department
409 South Seventeenth Street
Omaha, Nebraska 68102

Application programs available over wide range of coverage--business and finance, engineering, manufacturing, mathematics, project

planning and management, and statistics and probability. Typical applications of possible interest to auditors are the following, among others--

Sampling Aids for Auditors--Generates random numbers for sampling, appraises results of audit samples, and determines sample size to meet confidence levels.

General Ledger Accounting System--Maintains files for chart of accounts, general ledger, journal entries, control. Prepares general ledger reports, income statement, balance sheet, and schedules.

Others--On line and off line modes, include more than 300 programs, such as, critical path scheduling, capital investment analysis, cash flow analysis, present value analysis, depreciation analysis, and bond analysis.

GENERAL LEDGER

Transnet Corporation
60 English Plaza
Red Bank, New Jersey 07701

Normal accounting and reporting activities for a general ledger system.

GENERAL LEDGER FOR PUBLIC ACCOUNTING PRACTICE

R. H. Wilmore Accounting & Tax Service
2624 Chestnut Street
Columbus, Indiana 47201

Designed for the public accounting practice to handle multiple clients or can be used as a single operating system. Double entry system providing for all books of original entry and for automatic creation of financial statements.

GL-II--GENERAL LEDGER SYSTEM

Computer Sciences Corporation
9841 Airport Boulevard
Los Angeles, California 90045

Performs a total, integrated general ledger function for use by the large corporation operating a number of divisions in many locations or for use by the small business. Some of the features are--

Produces total of 44 varied operating & summary reports

Accepts the existing chart of accounts

Permits any type of depreciation scheduling

Optional departmental or cost center reporting

Separate compilations for subsidiaries but with consolidations into parent company chart of accounts

Preparation of quarterly and year-end tax reports

Optional financial analyses--comparisons, trends, etc.

Accommodation of flexible budget projections

Automatic accrual, deferral and closing entries

INFOMACS--A FILE STRIPPER REPORT GENERATOR

Management and Computer Services, Inc.
104 Park Towne Place East
Philadelphia, Pennsylvania 19130

Designed to produce customized reports on one-time or repetitive basis and to obtain information on a crash basis. Selects records from a file based upon criteria submitted by the user to create a live test file. Displays records on a printer in either record image or report format or allows writing those records on a file. Provides report titles and column headings, accumulations of up to ten fields with four levels and a final total, record counts by each selection criteria, padded input record elimination, and a summary printing capability when totals or record counts only are desired. Read and write

fixed or variable length tape files, or sequential or indexed sequential disk files on 2311 or 2314 disk drives. Provides print editing, subtotals, page skipping, packed field processing.

MARGEN--MANAGEMENT REPORT GENERATOR

Randolph Computer Corporation
8060 Mongomery Road
Cincinnati, Ohio 45236

A report generation system and a file maintenance system which will generate multiple reports and perform file maintenance in one pass of the data. Creates, updates, edits, and reformats files. Report generation features include--pictorial report layout, choice of report type, variable column width and spacing, eight levels of totals, record selection, predefined dictionary of names, and others.

RSVP--REPORT SERVICE, VERY PROMPT

National Computing Industries
1 Jackson Place
San Francisco, California 94111

Designed for use by non-technical users. Can be learned and usable in less than one-half day. Provides retrieval, sorting, selection printing, and arithmetic functions.

SCORE III--SELECT, COPY OR REPORT

Programming Methods Inc.
51 Madison Avenue
New York, New York 10010

May be classified as a file management utility system since it can be used in many different ways. Non-procedural formats are used to define parameters.

Report Generation--Any desired format for all or selected records with heading and detail line formatting, control total formatting, editing and computing. Files can be re-sequenced and collated to create desired report sequence and format. Up to eight files may be specified.

Retrieval System--Retrieve selected records from given input files based on any combination of parameters within the record. Selection may be relational or statistical.

Utility Program Generator--Permits data input from any device, and any access method (supported by the particular COBOL compiler), and allows for creation of output on any device and access. Records may be re-blocked, reformatted, and/or re-sequenced and written either to the same or different device.

File Generator--Generate files for production of testing purposes. Selection and formatting of data/records as explained above.

Conversion Aid--Ability to specify generation of COBOL code to handle second generation labels automatically. This permits processing of existing data files without costly conversion.

COBOL Source Program Generation--Based on input parameters, SCORE will generate a customized COBOL source program which can be either directly executed, catalogued, or punched out as a COBOL source deck.

SERIES 100 INFORMATION RETRIEVAL SYSTEMS

Computer Corporation of America
565 Technology Square
Cambridge, Massachusetts 02139

High-speed information retrieval; combinations of search keys; on-line file maintenance; supports multiple users.

STRATA

Touche Ross & Co.
1800 Ten Main Center
Kansas City, Missouri

After precisely defining the problem and objectives, user completes specification forms describing what information is wanted, where

to find the data, the calculations to be performed and the format, content and sequence of his output. Basic functions provided are--

Create--File of information desired. Each work record can contain up to 800 bytes in up to 99 fields.

Update--A file with data from another file. Selected fields may be used or records added or deleted.

Select and Print or Punch on Cards--Records that meet user specified criteria. Full set of conditional and arithmetic operations to define selection criteria. Columnar reports produced complete with headings, totals, and subtotals.

Summarize--Records of a file to produce summary records containin subtotals of the numeric fields of detail records.

Sort--Files in ascending or descending sequence in up to five fields. Automatic sorts as required before update or summarize functions.

Calculate--Additional values to be included in the desired file or to be used to test existing values in the file. All arithmetic and conditional operations in any sequence allowed. May branch during calculations. Work may be performed on single records or groups.

SOURCE: Compiled from responses received in answer to a questionnaire survey cn generalized computer audit programs. Information was furnished by the firms indicated under each program listing. No attempt was made to test or verify via test or benchmark runs of the programs any of the capabilities claimed. Details were taken from the returned survey questionnaire, and respondent's letter (if any received) or program brochure/ manual (if furnished).

APPENDIX D

Details of Survey for Generalized Computer Audit Programs

DETAILS OF SURVEY FOR GENERALIZED COMPUTER AUDIT PROGRAMS

Purpose of Survey

The original intent of the research questionnaire was to survey software companies specializing in generalized computer audit programs and selected CPA firms for the purpose of accumulating detailed information about such audit programs. From the results of the survey, it was hoped that a directory could be created to list the generalized audit program name and the capabilities possessed. In addition, it was thought desirable to include short descriptive paragraphs for each audit capability possessed by the audit program, when such information was furnished by the respondent.

Preliminary Respondents

Library research along with inquiry to auditing and data processing "trade" periodicals revealed that there were no readily available references that would serve to easily provide a desired mailing list from which potential survey candidates could be selected. Suggestions received from two periodical editors then pointed the inquiry toward software information publishers. Two of these publishers were kind enough to furnish copies of their pertinent publications as resource material.

Selection of Survey Recipients

Information furnished by the preliminary respondents in regard to sources of adequate mailing lists served as an important factor in the selection of survey respondents. Recipient firms were selected on

a judgmental basis from those listed in the resource materials. The three types of firms receiving survey questionnaires were software package suppliers, CPA firms, and computer company/affiliate.

Software package suppliers were selected primarily on the basis of their product or service offering. Although there are an estimated 1,000 software companies supplying a program market that extends across all industry and commerical segments, only a very, very few concentrate on the needs of the CPA firm. Software firms were chosen from those listing applications or programs in the publications of the software information publishers. In many cases, an abstract describing the program offering was available. Many of the software firms listed programs in two or more classifications. Ninety-five (95) software firms were selected as potential respondents. Of these, thirty-four (34) were listed in both the Business Automation and the ICP Quarterly publications; forty (40) were listed in only the Business Automation source; and twenty-one (21) were listed only in the ICP Quarterly.

Since the preliminary inquiries revealed there were only three software package suppliers that had developed generalized audit programs, it also seemed likely that only a very, very few of the AICPA member firms had created such audit programs. Accordingly, all of the "big eight" CPA firms were included and several regional firms were selected on the basis of personal recognition of the firm name. These two categories seemed to give the most promise as creators and/or users of generalized audit programs. CPA addressees included: Eight (8) national firms, five (5) regional firms, and twelve (12) local firms.

Twenty-five (25) CPA firms were selected as potential respondents.

All of the major computer vendors were included as they all offer applications programming service for developmental and operational software packages. This service may originate with the parent company or a subsidiary electronic data processing utility. The latter often takes the form of time-sharing or computer facilities rental on a "job" basis. Independent companies also compete aggressively for this service-type business. As a consequence, both independents and major computer vendors were included. Computer company/affiliate addressees were: Six (6) major computer vendors, three (3) vendor utility facilities, two (2) independent utility facilities, and two (2) mini-computer vendors. Thirteen (13) computer company/affiliates were selected as potential respondents.

An effort was made to insure representation from the several major geographical areas of the United States: Northeast, east, southeast, southwest, west, northwest, mid-central, and overseas. Thirty (30) states were represented in the sample population which consisted of all survey recipients. A total of 133 survey forms were mailed: 95 to software package suppliers, 25 to CPA firms, and 13 to computer company/affiliates.

Responses

Responses have been classified either as negative or positive. A negative response is defined as one in which the respondent returned the survey questionnaire and positively indicated that that firm did not have a generalized audit program. A positive response is defined

as one in which the respondent either returned the survey questionnaire indicating that that firm did have a generalized audit program or a program that could be used for the same purpose. In addition, respondents offering helpful suggestions or directions toward other resources of information were classed among the positive responses.

Negative responses included 13 from software package suppliers, one from a CPA firm and one from a computer company/affiliate. Included in the positive responses were replies from 12 software package suppliers, three CPA firms, three periodicals, three software information publishers, and one computer company/affiliate. There were 15 negative responses and 22 positive responses.

EXHIBIT D-1

SURVEY RESPONSES

Postiive Responses

Alexander Grant & Company
Auerbach Software Reports
Business Automation
Computer Audit Corporation
Computer Corporation of America
Computer Decisions
Computer Resources Corporation
Computer Sciences Corp
Cullinane Corporation
Datamation
Datapro 70
Evansville Data Processing Corporation
GE Time-Sharing Service
ICP Quarterly
Klane Gillman & Schecter
Management & Computer Services Inc.
National Computing Industries
Programming Methods Inc.
Randolph Computer Corporation
R. H. Wilmore Accounting & Tax Service
Touche Ross Bailey & Smart
Transnet Corporation

Negative Responses

Adapt Inc.
Cambridge Computer Associates Inc.
Collateral Investment Co.
Computer Guidance Associates
Digimatics Inc.
IBM Corporation
Information Science Inc.
McDonnell Douglas Automation Co.
National CSS Inc.
Scientific Time Sharing Corporation
Siedel Computer Associates
Synergistic Computer Systems Inc.
Valley Computer
Walter I Horlick
William M. Brobeck & Associates Inc.

EXHIBIT D-2

SURVEY TRANSMITTAL LETTER

THE CREIGHTON UNIVERSITY

OMAHA, NEBRASKA 68131

Business Administration
Department of Accounting

Gentlemen:

As part of the course work in my doctoral program at the University of Nebraska, I am engaged in a research project in connection with computerized, generalized audit programs. Working under the guidance of Dr. George C. Holdren, Professor of Accounting, I am making this survey in order to identify as many as possible of the available generalized audit programs--for example, Audassist and others.

From the results of the survey, it is intended that a directory will be built that, as a minimum, identifies the audit program name, each unique audit capability possessed, computer configuration(s) to which it has been adapted, programming language used, proprietary rights, current sale/lease price, and form in which available (cards, magnetic tape, computer service firm, etc.). Further, if availability of information permits, it seems desirable to include descriptive paragraphs of 40-80 words for the general scope and for each of the unique audit capabilities possessed.

It is anticipated that the dictory and explanatory paper would be of benefit to all CPAs who want to know more about the availability of a diversity of generalized audit programs. Your responses are needed in order to make the directory as complete as possible. Please complete the enclosed questionnaire and return it in the stamped, addressed envelope provided.

Thanks very much for your cooperation.

Sincerely yours,

/s/ Charles R. Wagner

Charles R. Wagner
Assistant Professor of
Accounting

CRW:ss
ENC. (1) Survey Form

EXHIBIT D-3

SURVEY OF COMPUTERIZED, GENERALIZED AUDIT PROGRAMS
(Please fill in blanks and encircle yes or no as appropriate)

Audit program name _____

Capabilities possessed
1. _____
2. _____
3. _____
4. _____
(Note others on reverse side, please)

Usable on computer
1. _____
2. _____
3. _____

Programming language
1. _____
2. _____

Proprietary rights owned by _____

Sale/lease price _____

Form in which available _____

In operational status Yes No

Copy of manual forwarded Yes No

Additional comments: _____

_____

_____

Permission is granted for use of above information and our firm name in the summarization and presentation of survey results as part of a research paper for academic purposes. We understand that additional release approval will be requested in the event any formal publication is subsequently deemed appropriate.

Name _____ Title _____

Firm _____ Address _____

EXHBIT D-4

LIST OF SURVEY RECIPIENTS

Periodicals

Business Automation
Computer Decisions
Data Management
Datamation
Data Processing
Journal of Accountancy
Management Services
Modern Data
Nebraska CPA Magazine
Software

Software Information Publishers

Auerbach Software Reports
Datapro 70
ICP Quarterly
Software Packages--An Encyclopic Guide

Software Package Suppliers

Adapt Inc.
Advanced Computer Techniques Corp.
Analysts International Corporation
APL Services Inc.
Applied Data Processing Inc.
Automated Information Systems Inc.
Burlington Management Services Co.
BVC Systems Service
Cambridge Computer Associates Inc.
CDS Computing Inc.
Century Computer Services Inc.
Cerebus Corporation
Collateral Investment Co.
Com-Share Inc.
Computer Advisors
Computer Applied Systems Inc.
Computer Business Consultants Inc.
Computer Corporation of America
Computer Credit System
Computer Generation Inc.

Computer Guidance Associates
Computer Information Systems Corp.
Computer Innovations
Computer Sciences Corp.
Computer Synergy Inc.
Computer Systems & Education Corp.
Computer Wares Inc.
Compu-Time Inc.
Compac Computer Systems Inc.
Computer Audit Corporation
Computer Audit Systems Inc.
Computer Resources Corporation
Concept Implementation Corp.
Consolidated Analysis Centers Inc.
Consolidated Computer Services International Inc.
Continental Illinois National Bank & Trust Co.
CTC Computer Corporation
Cullinane Corporation
Datasonics Inc.
Data Processing Applications Inc.
Digimatics Inc.
Ecco Consulting Inc.
EDP Dimensions Inc.
Electronic Processors Inc.
Ennis Brandon Computer Services
Evansville Data Processing Corporation
Fedder Data Centers Inc.
Florida Institute of Technology
H. G. Maynard & Company Inc.
Informatics Inc.
Information Science Inc.
Lambda Corporation
Macro Services Corporation
Maine Computer Center
Management Information Service
Management Science America Inc.
Management Systems Corporation
Management & Computer Services Inc.
Mauchly & Company Inc.
Mauchly Management Services Inc.
McDonnell Douglas Automation Co.
MDC Systems Corporation
National CSS Inc.
National Computing Industries
O'Brien and Lowe Inc.
PDA Systems Inc.
Photo Magnetic Systems Inc.
Program Generators Inc.
Programming Methods Inc.

Proprietary Software Systems Inc.
Publicate Inc.
R. H. Wilmore Accounting & Tax Service
Randolph Computer Corporation
Remote Computing Corporation
Republic Software Products Inc.
SAB Inc.
Scientific Time Sharing Corporation
Sequoia Electronics
Siedel Computer Associates
Sigma Data Computing Corporation
Simulation Associates Inc.
Soft-Pac Corporation
Synergistic Computer Systems Inc.
Systek Incorporated
Systemation Inc.
TBA Educational Information Processing Center
Telcomp Corporation of America
Trans Computer Associates
Transnet Corporation
Tymshare Inc.
Valley Computer
Western Data Sciences Inc.
Westinghouse Tele-Computer Systems Corp.
William M. Brobeck & Associates Inc.
Zale Data Processing Services

CPA Firms

Alexander Grant & Company
Anchin, Block & Anchin
Arthur Andersen & Co.
Aruthr Young & Co.
B. R. Sharp and Company
Crowe, Chizek and Company
Elmer Fox & Company
Ernst & Ernst
Hanson, Raun & Hanson
Haskins & Sells
Joseph Hartman & Associates
Klane, Gillman & Schecter
Lower, McClean, Berndt & Taylor
Lybrand, Ross Bros., & Montgomery
Markwardt, McGuire & Co.
Nave, Clark & Chaffin
Peat, Marwick, Mitchell & Co.
Pol, Toro & Co.
Price Waterhouse & Co.

Roush, Good, Nevin & Murray
S. D. Leidesdorf & Co.
Seidman & Seidman
Touche, Ross, Bailey & Smart
Vanboskirk, Fry, Trumble & Associates
Walter I. Horlick

Computer Company Affiliate

Burroughs Corporation
CDC Data Center
Digital Equipment Corporation
GF Time-Sharing Service
Hewlett-Packard
Honeywell EDP Systems
IBM Corporation
Information Systems Inc.
NCR Data Processing
Omaha National Data Processing
RCA Computer Systems
Service Bureau Corporation
Univac Data Processing Center