UIC John Marshall Journal of Information Technology & Privacy Law

Volume 2
Issue 1 *Computer/Law Journal - 1980*

Article 15

1980

# A Survey of Computer Crime Studies, 2 Computer L.J. 275 (1980)

John K. Taber

# A SURVEY OF COMPUTER CRIME STUDIES

*By* JOHN K. TABER*

TABLE OF CONTENTS


| | | Page |
|---|---|---|
| | INTRODUCTION | 275 |
| I. | PROJECTIONS OF THE INSTITUTE FOR THE FUTURE | 276 |
| II. | THE GENERAL ACCOUNTING OFFICE REPORT | 280 |
| III. | THE STANFORD RESEARCH INSTITUTE STUDY | 287 |
| IV. | CONCLUSION | 310 |
| V. | APPENDIX: THE ROUND-OFF FRAUD | 311 |


## INTRODUCTION

Computer crime provokes considerable interest in the media and political arena. It has engendered alarm and a sense of urgency. In response, a score of states and the federal government have passed or are deliberating hastily drawn computer crime bills. Yet, little is known about computer crime. There is much written on the subject, but the writers too often quote each other without critically examining the sources of information,[1] and once in print a computer crime story tends to live forever. Therefore, it is worthwhile to examine the serious studies of computer crime. These are a report by the General Accounting Office ("GAO") and several reports by Stanford Research Institute ("SRI"). Popular books on the subject, such as *Computer Crime* by Gerald McKnight,[2] are ignored because the sources of such books are these studies and the books are too uncritically accepting of media computer "horror stories" to be of any value. In addition, a report by the Institute for the Future,

---

* B.A. 1964, University of California, Berkeley; systems programmer, International Business Machines Corporation since 1970. Mr. Taber has worked on the development of APL (A Programming Language) and relational data bases.

1. *See, e.g.*, L. KRAUSS AND A. MACGAHAN, COMPUTER FRAUD AND COUNTERMEASURES 14 (1979). The authors intended a serious work outlining management methods to control assets and prevent fraud. The volume is unfortunately marred by the repetition of incorrect computer crime stories.

2. G. MCKNIGHT, COMPUTER CRIME (1974).

*The author is grateful to John S. James and Rob Kling for their review and criticism of this article. The views expressed by the author are entirely his own and should not be construed as reflecting the views of any organization or any other person.

which touches on computer crime, is included for the sake of completeness.

These works are flawed, and only the GAO report has any validity. Part of the problem is definitional. First, what is a computer; then, what is computer crime. Satisfactory definitions are probably impossible. The industry itself has not yet been able to define a computer. The possibility of defining computer crime would seem to be even more difficult.

## I. PROJECTIONS OF THE INSTITUTE FOR THE FUTURE

*Economic Losses* prepared by the Institute for the Future, was sponsored by Skandia Insurance, Sweden, presumably for actuarial purposes.[3] It is not primarily a study of computer crime—errors and malfunctions are found to be far more important—but it attempts to be a serious study in which computer crime is a significant factor. It is discussed briefly by SRI as an earlier study.[4]

*Economic Losses* is a mail survey of thirty-four specialists in various areas of computer technology.[5] Preliminary survey results were resubmitted to the specialists for further refinement. In short, it was an opinion survey of presumably knowledgeable people. The study attempted to identify the most likely major applications of computers during the next fifteen years (to 1985), then concentrated on what losses seemed most likely to occur and tried roughly to quantify them. The authors warn against relying on the study's results because too many unforeseeable factors could influence them.[6] "The numbers are only gross expectations about unknown quantities"[7] and "one must . . . take these expectations with a grain of salt."[8]

Across twenty likely computer applications the estimated total losses due to crime was given as about $158 million.[9] Sabotage accounted for $80 million, and theft and fraud for $78 million. For some applications, crime accounted for little or no losses, and for others, significant losses.[10] For example, no crime losses were fore-

3. G. Salancik, T. Gordon & N. Adams, On the Nature of Economic Losses Arising from Computer-Based Systems in the Next Fifteen Years (Institute for the Future, Rep. R-23, Mar. 1972) [hereafter cited as Economic Losses].

4. D. Parker, Computer Abuse Assessment 15 (Stan. Research Inst. Rep. 1975) [hereafter cited as Assessment].

5. Economic Losses, *supra* note 3, at 2-3.

6. *Id.* at 17.

7. *Id.* at 21.

8. *Id.* at 25.

9. *Id.* at 37 (fig. 7).

10. *Id.* at 38 (fig. 8). *See also id.* app. A, at 54-93.

seen in computer controlled machine tool operations[11] and tire manufacturers,[12] while the most significant type of loss (thirty-seven percent) was projected for electronic funds transfers.[13]

It is surprising that the study attributed a larger loss to sabotage than to theft and fraud. Though some sabotage can be attributed to unhappy consumers smashing computers, the survey respondents thought that most sabotage would be committed by "dissatisfied political activists attacking 'the system.' "[14] This emphasis on political sabotage is dated, notwithstanding a recent rash of political attacks in Italy and France. Political destruction of computers is a transitory phenomenon that emerges only in eras of stress, like in current Italy and France, or in the Vietnam war period in the United States during which time this study was prepared. In short, a transitory phenomenon was treated as a permanent affair, and this treatment unduly biased the study.

Crime dollar losses are not detailed except for a few applications where the crime loss is proportionately significant. There is a major discrepancy; the total of the detailed losses is greater than the overall loss figure. There is no explanation for this discrepancy. Perhaps the overall losses were derived from a different averaging method than the median of the estimate used for the detailed figures, or perhaps different categories were used. In any case, the detailed crimes, applications, and losses are listed in Table 1.

It is evident that most of these crimes are not computer crimes. Bombing a power transformer or 12KVA switch can hardly be considered a computer crime even if the power distribution system itself is under computer control. The last item in the table, the largest loss, is strange and deserves comment. The respondents thought that by sometime after 1985 at least twenty-five percent of American homes would have burglar alarm systems connected by phone to computers in police departments and private agencies. The homes would be wired with sensors that would detect movement and entry. The respondents seemed to think that this would be an exciting application for computers, but they did foresee some difficulties in winning consumer acceptance—basically, objections to "Big Brother" intrusion of the police into private homes.

Thus, they thought that the likelihood of occurrence would be later than 1985 for this one application. Also noteworthy is the

11. *Id.* at 68.
12. *Id.* at 64.
13. *Id.* at 60.
14. *Id.* at 40.

TABLE 1

Institute for the Future's Projected Computer Crime Losses by Application

| Computer Application | Crime/Incidence Rate | Loss (in millions) |
|---|---|---|
| Credit Cards[15] | Forgery, theft, loss of cards: 48,000 per year at $800 each. | 38.4 |
| Electronic Funds Transfer[16] | Programmer siphons funds: 36 thefts per year at $110,000 each. | 3.96 |
| | Small interbank transfer thefts: 1000 per year at $2,000 each. | 2.0 |
| | Few large interbank transfer thefts: 8 per year at $1 million each. | 8.0 |
| Power distribution[17] | Political or criminal bombing of transformers or switches: 10 per year at $4 million each. | 40.0 |
| Rapid transit[18] | Tampering, sabotaging call boxes: 50,000 per year at $600 each. | 30.0 |
| Home burglary alarm systems[19] | Burglars disable sensors then burgle homes: 30,000 homes per year at $1,500 each. | 45.0 |
| | Burglars disable phone lines and burgle homes: 42,000 homes per year at $1,400 each. | 58.8 |
| Subtotal | | 226.16 |

twenty-five percent penetration, rather than the fifty percent used for the other applications. In other words, for the other applications, like tire manufacturing, the report takes fifty percent computerization of the industry as its target, but it takes only twenty-five percent for home burglary systems. It probably should not have been included among the twenty most likely applications (they had forty to play with) for consistency, but it apparently was included because the respondents liked it. The losses were due in part to homeowners deliberately or erroneously disabling the sensors and then being burgled, in part to burglars disabling the sensors or phone lines, and in part to collusion between burglars and the "monitors."

Apart from wealthy enclaves and high crime slums, it does not seem today that home burglary systems (other than the mail order variety) are that widespread, nor likely to become so. Also, burglar alarm technology still does not use computers, advertising claims to the contrary. Essentially, it uses phone switches to telephone an alarm from the home to a private agency, which then, by voice telephone relays the warning to the police.[20] It would appear that the importance that respondents bestowed on this "application" is due to their bias, and not to their personal knowledge. In the late 1960s and early 1970s when this survey was conducted, "crime in the streets" was propagandized by the Johnson, then the Nixon, administrations. The media coverage of "crime in the streets" must have colored the respondents' perceptions with or without their being aware of it.

Credit cards is a heavily computerized application, but forgery and theft of cards should not be called computer crimes. The only computer crime left in this list involves electronic funds transfers. Missing completely are business "computer crimes," such as inventory or payroll thefts. The reason for this is that estimated crime losses expressed as a percentage of the total were too small to be detailed; theft or fraud accounted for only 7.6% of the total business application losses, the largest loss (thirty-one percent) being "peripheral operator mistakes."[21] It is not possible to accurately figure crime losses, given 7.6%, because total loss is not stated. However, doing the arithmetic on the figures that are provided, it is about $119

15. *Id.* at 54-55.
16. *Id.* at 60-61.
17. *Id.* at 70-71.
18. *Id.* at 74-75.
19. *Id.* at 80-81.
20. Personal communication with a locksmith.
21. Economic Losses, *supra* note 3, at 57. They mean keypunch errors and the like.

million.[22] This figure is, of course, completely inconsistent with the total claimed theft and fraud loss for all applications of only $78 million.

The programmer thefts for EFT (thirty-six percent) also require comment. The respondents had in mind the round-off remainder fraud:

> the use of computers to conduct bank transactions . . . is expected to be lucrative for thievery . . . Ingenuity is required to steal and still balance accounts, yet it is done; one computer programmer recently managed to embezzle $200,000, a few mills at a time, by accumulating the rounding errors from customers' bank accounts and having them deposited to his own.[23]

This is a fictitious crime that so far has never been known to have occurred. Mathematically, it is possible to steal small amounts over a period of time, improbable to steal large amounts, and almost impossible to steal $200,000. Once again, popular fancy misled the respondents.

## II. The General Accounting Office Report

The best study for statistics of computer crimes is that conducted by the General Accounting Office ("GAO") of the federal government.[124] Ten Federal investigative agencies searched their files for cases of "computer crime" to provide the GAO with data. While such a search could never be complete—nobody classes cases as computer crimes, there is no such category—the search was reasonably thorough over a reasonable period of time.[25] The agencies which conducted the searches were:[26]

---

22. The arithmetic is as follows:

crime $\cong .071 \times$ total loss

but entry errors $\cong (.31 \times \text{total}) = (10^5 \times 200)+(10^7 \times 50) \cong 5.2 \times 10^8$

therefore, total $\cong \dfrac{5.2 \times 10^8}{.31} \cong 1.677$ billion.

Thus, crime loss $\cong .071 \times 1.677$ billion $\cong 119$ million.

23. Economic Losses, *supra* note 3, at 40.

24. General Accounting Office, Computer Related Crimes in Federal Programs (1976), *reprinted in Problems Associated with Computer Technology in Federal Programs and Private Industry, Computer Abuses, Sen. Comm. on Gov't Operations*, 94th Cong., 2nd Sess. 71-91 (Comm. Print 1976) [hereinafter cited as GAO Report].

25. Just how thorough is, of course, open to question. Donn Parker thought that the GAO arbitrarily picked sixty-nine cases out of literally thousands. Letter from Donn Parker to John S. James. But Walter Anderson of the GAO stated that Donn Parker was mistaken. It was a reasonably thorough search which netted seventy-four cases. Personal communications with Walter Anderson (Mar. 29, 1979).

26. GAO Report, *supra* note 24, at 88.

- Army Criminal Investigations Division
- Navy Investigations Service
- Air Force Office of Special Investigations
- Department of Agriculture Office of Investigation
- Department of Interior Division of Investigation
- Social Security Administration
- Veterans Administration Investigative and Security Services
- Internal Revenue Service
- Executive Office for United States Attorneys
- Federal Bureau of Investigation

This is an impressive list. In the author's opinion, the competence of an investigative agency is inversely related to the agency's glorification in the media. One can be reasonably sure that the crimes in the files of the unpolitical Navy Investigative Service, and the other military agencies, are real crimes, and that the facts of the cases are reasonably close to being as stated. In short, the GAO cases are not myths, and are substantiated by competent investigation, not simply by newspaper clippings.[27]

The file search netted seventy-four cases for analysis by the GAO, of which the GAO rejected five for not fitting their criteria of "computer-related" crime, leaving sixty-nine known cases in the federal government.[28]

The Army provided sixteen cases, of which fifteen were false (that is fraudulent) record entries, and one was a conflict of interest on the part of managers.[29] The Navy found four cases,[30] one of which was a baseless charge that encrypted data and free computer time at a military installation could be obtained from the computer system at a nearby university. Two were false record entries and the fourth was a stolen program.

The Air Force provided sixteen cases,[31] three of which were rejected for not involving computers, and the thirteen remaining were all false record entries. Two of the thirteen involved falsification of records to obtain a preferred assignment and to permit re-enlist-

27. As shown below (text accompanying notes 125-71 *infra*), documentation for the majority of the SRI cases, the largest collection of "computer crimes" known, is almost solely newspaper clippings.

28. In a previous article, this author erred in stating that there were sixty-six cases. The correct figure is sixty-nine. The author failed to notice that the GAO had already dismissed three Air Force cases that were not computer crimes. *See* Taber, *On Computer Crime (Senate Bill S.240)*, 1 COMPUTER/L.J. 517 (1979).

29. *Computer Security in Federal Programs, Sen. Comm. on Gov't Operations*, 95th Cong., 1st Sess. 149 (Comm. Print 1977) [hereinafter cited as *Security*].

30. *Id.*

31. *Id.* at 149-50.

ment of an ineligible serviceman. Overall, the computer itself rejected two Army false record entry attempts and two Air Force attempts. Details of the remaining cases are not available.[32]

Of the sixty-nine cases, nine were incidents such as privacy invasion and involved no dollar loss.[33] For eleven more cases, a dollar loss had not been determined at the time of the report.[34] For the forty-nine remaining cases, the total known and estimated loss was $2,161,413.[35] The average was $44,110 and the median was $6,749.[36]

The majority of cases, forty-three of sixty-nine, about sixty-two percent, were false record entries. At least fifty were committed by technologically naive users of the systems, not by computer professionals.[37] In short, the crimes mainly consisted of submitting manually prepared, but falsified, forms to a computerized record keeping system.

A total of sixty-nine cases of "computer crime" in the federal government is a remarkably low figure, especially when one considers the fact that the government is the largest single user of computers in the world.[38] Either the investigative agencies did a very poor job searching their files, or computer crime is an insignificant problem in the federal government. The GAO Report says that the agencies could not discover all cases, largely because cases are not filed as computer crimes, but under more traditional headings.[39] Also, the GAO warns that there may be cases as yet undiscovered. But the GAO nowhere implies that the file search was cursory.

The GAO was clearly puzzled by their figures; they do not agree at all with those of the Stanford Research Institute, which found an average loss of $450,000, more than ten times the GAO average of $44,000.[40] It is possible that their puzzlement led the report writers to explain the scant sixty-nine cases as file retrieval difficulties. But the GAO Report plainly admits that the GAO cannot account for the

---

32. Personal communication with Walter Anderson, GAO manager for this report. Mr. Anderson would not release detailed case information in order to protect the confidentiality of his sources. Several cases were handled administratively, and the agencies apparently fear criticism for not prosecuting them.

33. GAO REPORT, *supra* note 24, at 91 (note c).

34. *Id.* note a.

35. *Id.*

36. The GAO Report does not give the median, but it was easy to compute from the data given. *Id.* at 89-91.

37. *Id.* at 76.

38. *General Accounting Office, Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities, reprinted in* GAO REPORT, *supra* note 24, at 93, 95.

39. *Id.* at 88.

40. *Id.* at 79.

ten to one difference in averages.[41] It is puzzling because government's uses of computers are no different from the private sector's.[42] Finally, it is even more puzzling, to the point where the GAO should have begun questioning their basic assumptions about the extent and seriousness of computer crime and their belief in SRI infallibility, since the government's cases contained *twice* as many frauds (sixty-seven percent government versus thirty-three percent SRI) and a vanishingly small proportion of unauthorized use and vandalism (three percent government versus forty percent SRI).[43] If the GAO data is good, and it appears to be so,[44] then SRI's data must

---

41. "We do not know why the average losses in detected Government cases are smaller than those in the private sector." *Id.* By "private sector," the GAO is referring to the SRI cases. *Id.*

42. "Government systems are similar. . . . Therefore, as the SRI report to us points out, there should be equal opportunity and temptation for the perpetration of computer crimes." *Id.*

43. *Id.*

44. Personal communications with Walter Anderson. Several of the estimated figures have been questioned. They aroused suspicion because when the losses are sorted to get the median, it appears that all of the largest numbers are estimates, while, in contrast, many of the smaller numbers are exact to the dollar. That observation suggested that one or more of the agencies may have supplied the GAO with estimates whose accuracy are questionable. Normally, one would expect estimates to be more or less scattered among the exact figures, not snobbishly thronging the expensive end. But Mr. Anderson stated that the GAO computed the estimated figures themselves, independently in fact, by duplicate teams, in order to provide cross-checks on themselves. Furthermore, he stated that the GAO estimates things conservatively and is prepared to defend its estimates before suspicious congressmen.

These responses are still not satisfactory. On general principle, random data that departs too greatly from chance distribution is suspect. Also, Mr. Anderson could vouch for only one of the larger losses—the $134,000 figure —which, indeed, is precise to one more significant digit than its neighbors in the sorted list (another neighbor is $79,780, which is obviously an exact figure, the only one among the highest fourteen). Additionally, the estimates appear to have different sources, because their precision is not consistent. These observations are important, because the largest numbers are atypical and have the greatest effect on the GAO average. If they are impeached, the average would be considerably smaller. The sorted figures are listed in the following table.

| | | |
|---|---|---|
| 101 | 11000 | 100000 |
| 184 | 12740 | 134000 |
| 320 | 13000 | 250000 |
| 358 | 14000 | 250000 |
| 360 | 14400 | 330000 |
| 668 | 15480 | 530000 |
| 766 | 16113 | |
| 961 | 22600 | |
| 971 | 25000 | |
| 978 | 28000 | |
| 1120 | 29000 | |

be in error. Nothing else, not file retrieval difficulties, unknown and unreported cases, or whatever, can explain this enormous discrepancy between the GAO and the SRI averages.

Yet, the GAO did not draw this obvious conclusion. On the contrary, the body of the report attempted to make more of a case for computer crime than the GAO data supported. The commentary cited the larger cases, sometimes cases not even in their list. For example, a $7 million loss borrowed from SRI's cases,[45] a $90,000 case not in their list,[46] and a $48,000 case also not in their list.[47] This extraneous data is not pertinent, and serves only as larding for their own meager cases. Nor does the GAO Report mention the median loss of $6,749 which, because of the distribution of the losses (it is skewed toward the low end), is probably a fairer statistic than the arithmetic average. Instead of citing extraneous figures, the GAO should have compared their actual loss figures with those of comparable crimes. This they did not do.

SRI cites the FBI for a mean loss of $19,000 for bank fraud and embezzlement.[48] If that figure is good, and if the appropriate figure

---

| | |
|---|---|
| 1293 | 30000 |
| 1411 | 53000 |
| 1500 | 64000 |
| 1832 | 69000 |
| 2609 | 79780 |
| 2989 | |
| 3074 | |
| 3680 | |
| 3800 | |
| 4300 | |
| 4400 | |
| 4476 | |
| 6000 | |
| 6749 | |
| 8000 | |
| 8000 | |

45. GAO REPORT, *supra* note 24, at 74.

46. *Id.* at 77.

47. *Id.* at 81.

48. Assessment, *supra* note 4, at 18. The figure is derived from the FBI Uniform Crime Statistics and, therefore, there is no particular reason to give it much credence. *See* Zeisel, *The Future of Law Enforcement Statistics: A Summary View*, in 2 FEDERAL STATISTICS REP. OF THE PRESIDENT'S COMM'N 527 (1971), for a discussion of the inadequacies of FBI statistics. In brief, the FBI is given high praise for attempting to bring uniformity into the reporting of crimes among some 8,000-10,000 local police jurisdictions. Nevertheless, the FBI data base remains unreliable. Further, the FBI uses the statistics to support its viewpoint, both political and bureaucractic. There is something basically wrong with allowing the very agency whose statistics are supposed to measure its effectiveness to maintain those statistics. But the FBI is powerful, and has successfully resisted all attempts to award custodianship of crime

TABLE 2

| | Description/ amount of loss | Method used by perpetrator: Fraudulent record initiation | Improper use of facilities | Processing alteration | Misappropriation of output |
|---|---|---|---|---|---|
| | Fraudulent direct payments: | | | | |
| 1 | $ 3,680 | X | | | |
| 2 | 250,000 | X | | | |
| 3 | 1,120 | X | | | |
| 4 | 28,000 | X | | | |
| 5 | 100,000 | X | | | |
| 6 | 25,000 | X | | | |
| 7 | (a) | X | | | |
| 8 | 8,000 | X | | X | |
| 9 | 14,000 | X | | | X |
| 10 | 15,480 | X | | | X |
| 11 | 79,780 | X | | | |
| 12 | 30,000 | X | | | |
| 13 | 134,000 | X | | | |
| 14 | (a) | X | | | |
| 15 | 16,113 | X | | | |
| 16 | (a) | X | | | |
| 17 | 371 | X | | | |
| 18 | 4,400 | X | | | |
| 19 | 668 | X | | | |
| 20 | 360 | | X | X | |
| 21 | 4,476 | X | X | | |
| 22 | 1,411 | X | | | |
| 23 | 6,000 | | | X | |
| 24 | 14,400 | | | X | |
| 25 | (a) | X | | | |
| 26 | 320 | X | | | |
| 27 | (a) | X | | | |
| | Fraudulent inventory/supply actions: | | | | |
| 28 | 53,000 | X | | | |
| 29 | (b)766 | X | | | |
| 30 | (b)11,000 | X | | | |
| 31 | (b)64,000 | X | | | |
| 32 | (a) | X | X | | |
| 33 | 3,800 | X | X | | |
| 34 | 13,000 | X | X | | |
| 35 | (b)330,000 | X | X | | |
| 36 | 978 | X | | | |
| 37 | 8,000 | X | | | |
| 38 | 69,000 | | | X | |
| 39 | (a) | X | | | |
| 40 | 29,000 | X | | | |
| 41 | 12,740 | X | | | |
| 42 | (b)530,000 | X | | | |
| 43 | 22,600 | X | | | |
| 44 | 184 | X | | X | |
| 45 | 1,500 | X | | | |
| 46 | 250,000 | X | | | |

TABLE 2 (Continued)

| Description/ amount of loss | | Method used by perpetrator: Fraudulent record initiation | Improper use of facilities | Processing alteration | Misappropriation of output |
|---|---|---|---|---|---|
| 47 | 101 | | | | X |
| 48 | 1,293 | | | | X |
| 49 | 6,749 | | | | X |
| 50 | 358 | | | | X |
| 51 | 2,989 | | | | X |
| 52 | 3,074 | | | | X |
| 53 | 961 | | | | X |
| 54 | (a) | | | | X |
| 55 | 2,609 | | | | X |
| Unauthorized altering of personnel records: | | | | | |
| 56 | (c) | | X | X | |
| 57 | (c) | | X | X | |
| 58 | (c) | | X | X | |
| 59 | (c) | | X | X | |
| 60 | (c) | | X | X | |
| 61 | (c) | | X | X | |
| 62 | (c) | | X | X | |
| 63 | (c) | X | X | X | |
| Use of facilities for personal benefit: | | | | | |
| 64 | (c) | | X | | X |
| 65 | 1,832 | | X | | |
| 66 | (a) | | X | | |
| 67 | 4,300 | | X | | |
| Sabotage of operations: | | | | | |
| 68 | (a) | | | X | |
| 69 | (a) | | | X | |
| Total | $2,161,413 | (d)43 | (d)18 | (d)16 | (d)12 |

Notes:
(a) Loss has not been determined at the time of our review.
(b) Potential loss. Crime was discovered before total loss occurred.
(c) No monetary loss. Effect was of another type, *e.g.*, invasion of privacy.
(d) Total exceeds sixty-nine since some crimes involved more than one method.

for comparison is the GAO's mean of $44,000, then the average computer crime loss is more than twice the average bank loss. The original hypothesis first advanced by SRI was that computers should

statistics to another, impartial agency, ever since the Wickersham Commission first suggested that it do so in 1931. *Id.* at 542. One of SRI's problems in its study of computer crime is its unquestioning acceptance of FBI statistics.

reduce the incidence of crime by, in effect, removing records from people, while increasing the loss per incident because computers tend to concentrate assets.[49] The GAO data tends to confirm the hypothesis.

Table 2 repeats the GAO data.[50]

## III. THE STANFORD RESEARCH INSTITUTE STUDY

The most ambitious study of computer crime is Donn Parker's work at SRI. So far, the study has produced three reports to the National Science Foundation[51] and a popular book.[52] Other reports have been written for government agencies under specific contracts, but the book and the NSF reports are the ones examined here. This section also include SRI's more recent cases, unpublished as yet, spanning 1977-78.[53] For convenience, the whole of the available data is called the "SRI study."

This study is unquestionably the major source of the computer crime cases that have appeared in the literature. It is Thomas Whiteside's source for his article and book.[54] Earlier, it was Porter's source for an article in the *New York Times*.[55] This article, in turn, was August Bequai's source for several law journal articles.[56] Hardly any feature article in the popular or trade media is complete without reference to the SRI Study.

The apparent intent of SRI was a "multi-disciplinary" study of "abusive" computer usage (and non-usage) involving criminology, sociology, law, and technology.[57] The first report, *Computer Abuse*,

---

49. D. Parker, S. Nycum, & S. Oura, Computer Abuse 7, 77-80. (Stan. Research Inst. Rep. 1973) [hereinafter cited as Computer Abuse]. This hypothesis seems to be very reasonable, and it is surprising that it is seldom mentioned in later reports from SRI. Though it is reasonable, it has not yet been established. SRI has apparently put the hypothesis on a back burner, and has made no effort to verify or discredit it.

50. GAO REPORT, *supra* note 24, at 89-91.

51. Computer Abuse, note 49 *supra*; Assessment, note 4 *supra*; D. Parker, Computer Abuse Perpetrators and Vulnerabilities of Computer Syatems (Stan. Research Inst. Rep. 1975) [hereinafter cited as Perpetrators].

52. D. PARKER, CRIME BY COMPUTER (1976).

53. SRI case numbers 7711-78402, inclusive (more than seventy cases).

54. Whiteside, *Annals of Crime: Dead Souls in the Computer*, THE NEW YORKER, Aug. 21, 1977, at 35 (pt. 1); Aug. 29, 1977, at 34 (pt. 2); T. WHITESIDE, COMPUTER CAPERS (1978).

55. Porter, *Computer Raped by Telephone*, N. Y. TIMES MAG., Sept. 8, 1974, at 33.

56. *See, e.g.*, Bequai, *The Impact of EFTS on Our Criminal Justice System*, 35 FED. B.J. 190 (1976); Bequai, *A Survey of Fraud and Privacy Obstacles to the Development of an Electronic Funds Transfer System*, 25 CATH. U.L. REV. 765 (1976). August Bequai's other major source of references is G. MCKNIGHT, COMPUTER CRIME (1974).

57. Computer Abuse, *supra* note 49, at 3. *See also Federal Computer Systems Pro-*

implemented the intent; it was co-authored by Parker for technology, Nycum for law, and Oura for sociology, and it was reviewed by academics in related fields before release.[58] Subsequent reports, however, were authored solely by Parker, and the acknowledgements do not credit any learned reviewers. The multidisciplinary intent is still there, but not implemented. The result has been a deterioration in scholarly standards.

The SRI study enjoys more importance than it should. It is used to support the proposition that computer crime is growing at an alarming rate; in 1973, SRI had about 144 cases; in 1974, 381; recently, 620; and perhaps over 700 by now. It is the source of two uncritically accepted statistics—an average loss per incident of $450,000, and an estimated annual loss of $300 million. Speculations advanced by SRI have been just as uncritically accepted as fact, and have been perhaps even more influential. One is the "tip of the iceberg" conjecture: the known cases represent only a fraction of all cases. A second is the "sophisticated" computer crime: one committed by an unscrupulous but highly skilled "technologist," who tampers undetected with the computer itself or its programs. A third, and perhaps the most damaging hypothesis, is that programmers are unethical, and therefore, a threat to society.[59]

The SRI study causes much confusion because it is not a study of just computer crime. SRI's term is *computer abuse*. The cases in the SRI collection include many non-criminal matters, such as civil suits and errors. SRI's term is not well-chosen. Many people take *abuse* to mean *crime*, in spite of the fact that in the formal reports, SRI is careful to make clear that the study is not limited to criminal conduct.

SRI's intention is to include non-criminal matters which it feels are abusive in some sense. SRI defines computer abuse to mean an "intentional act in which one or more victims suffered, or could have

---

*tection Act: Hearings on S.1766 Before the Subcomm. on Criminal Law and Procedures, Senate Comm. of the Judiciary*, 95th Cong., 2d Sess. 57 (1978) (testimony of Donn B. Parker) [hereafter cited as *Hearings*].

58. Computer Abuse, *supra* note 49, at 4.

59. This view has been very influential. *See, e.g.*, Whitmarsh, *No Action on DP Crime Since Florida Law Passed*, Computerworld, Aug. 13, 1979, at 4, col. 1. The Florida computer crime bill became law more than a year ago. State Representative S. Curtis Kiser, the bill's sponsor, was chagrined to learn that there had yet to be any prosecutions under the new law. "I just don't know why there has been no action," he said. *Id.* He was impressed with testimony on the bill indicating "an appalling lack of ethics and morality in the data processing profession." *Id.* Parker was one of the witnesses at those hearings.

suffered, a loss and one or more perpetrators made, or could have made, a gain. The incident must be associated with computer technology or its use."[60] The definition is impressive, but many of SRI's cases simply do not fit it. SRI has contributed to the confusion of *crime* versus *abuse* by referring to the collection of cases as "crimes" in several published reports.[61] In brief, SRI is inconsistent in its own terminology—an inconsistency that has caused great confusion, distortion and unwarranted claims of massive incidents and losses.

SRI apparently uses the more neutral term *computer abuse* on formal occasions, such as its reports to the NSF, and *computer crime* in public appeals, such as in its seminar and consulting advertisements, its press releases and newspaper interviews. Apparently, SRI's interest was crime, but its researchers were not formally qualified to conduct criminological studies, and were constrained to adopt *computer abuse* to win government acceptance:

> The first proposal for my research was titled "Computer-Related Crime." Law researchers reviewed the proposal, saying "Parker, you are a computer technologist. What are you doing, trying to decide what is a crime? After all, there are only six people in the whole world qualified to address that subject." I next changed the name of the research to "Anti-Social Use of Computers." Sociologists who reviewed the proposal came back to me and said, "Parker, you are a computer technologist. What are you doing, trying to decide what is social and antisocial? After all, there are only six people in the whole world qualified to address that subject." I thought to myself, "All right, you guys, I will play your game." I changed the title of the research to "Computer Abuse"—a term that had not been used or at least formalized before. I was then able to define the problem as I wished. . . .[62]

To dispel confusion, it is necessary to review SRI's cases. The

---

60. Assessment, *supra* note 4, at 3.

61. D. PARKER, *supra* note 52, at 294 ("374 computer-related crimes have been reported . . ."). At that time 374 incidents was the extent of the SRI collection, of which about one third of the cases were non-criminal. In a recent brochure advertising his seminar on computer crimes, Donn Parker referred to his entire collection, without exception, as computer crimes. In the media, Parker is always referred to as the "computer crime expert," not the "computer abuse expert." *See, e.g.*, Rapoport, *Sherlock Holmes of Computer Crime*, S.F. Chronicle, Mar. 30, 1979, at 6, col. 1. In that newspaper article the entire collection (more than 650 at that time) was referred to as crimes: "verified thefts, embezzlements, forgeries, extortion, larceny and espionage." *Id.*

62. D. PARKER, *supra* note 52, at xi. Parker holds a Master of Arts degree in mathematics. *Hearings, supra* note 57, at 55.

review must be incomplete because only synopses of some two hundred cases[63] and copies of over seventy of SRI's more recent cases have been made available. But what is available would appear to be indicative of the entire collection.[64]

The SRI case number system is used for the remainder of the article, and the system needs some explanation. The case numbers are a four or five digit number, sometimes with a Y or N suffix, for example 7022N. The Y means "verified", the N means not verified. The first two digits are the year in which the "abuse" occurred. The third is a classification of the abuse, as follows:

1 vandalism
2 information or property fraud or theft
3 financial fraud or theft
4 unauthorized use or sale of services

The last digit, or last two digits, is the SRI accession number. The suffixes, Y or N, occur only in one report,[65] and apparently SRI no longer lists cases as verified or non-verified in its reports.

The SRI study includes many non-criminal matters. Some examples are:

* errors — 77340, 78301, 78310, 78309.[66] Bank error (digit transposition on keying account numbers for deposits). Credited deposit to wrong account. These errors led to crimes when account holders withdrew the unexpected bonanzas and fled. Case 77316 is a similar banking error that did not result in any crime.[67]

7234N.[68] Keypunch error resulted in too low a tax rate for Woonsocket, R.I.

7022N.[69] Mailing list accidently destroyed by operator error.

---

63. Synopses are given for 150 cases in Computer Abuse, *supra* note 49, at app. A and for seventy-two cases in Perpetrators, *supra* note 51, at app. A few of the cases are duplicates, and several are misnumbered.

64. Consecutive cases from the SRI collection were copied by the author to avoid any claim that the author "selected" isolated cases to support his own biases.

65. Computer Abuse, *supra* note 49, at 91-112.

66. SRI files. These are newspaper articles.

67. SRI files. *See* note 136 *infra.*

68. Computer Abuse, *supra* note 49, at 107.

69. *Id.* at 95. Note the inconsistency in the SRI classification. This case is neither theft of information nor property, but the number "2" was erroneously assigned as the third digit. There are many cases that are improperly classified, especially the error cases.

* civil suits

7023Y.[70] *Honeywell v. Lithonia*

7043Y.[71] *TWA v. Burroughs*

7126Y.[72] Software firm sued for selling program developed for one firm to another as well.

7127Y.[73] Computer service firm used registered voters list for its own commercial purposes. Sued by state.

7128Y.[74] Suit involving three employees who went to work for a rival time sharing company.

71210Y.[75] Two case workers sued for reinstatement when dismissed by state for refusing to submit welfare data. They claimed that the computer system could not guarantee privacy for their welfare clients.

7222Y.[76] Insurance company appeal of civil suit verdict against it rejected. Company argued that wrong date on renewal notice was computer error for which company was not responsible.

7224N.[77] Similar insurance claim dispute.

7225N.[78] Suit over use of mailing list of civil service employees, allegedly used for political campaigning.

* abuses, not necessarily criminal

6741N.[79] Employees used equipment without authorization.

6913N.[80] Anti-war demonstration. Students occupied university computer center.

7123N.[81] Obtaining other users' passwords.

7144N.[82] Computer training school closes.

7145N.[83] Computer training school fined for falsely advertising career opportunities.

7228Y.[84] Student copied five thousand passwords.

---

70. *Id.* at 95.
71. *Id.* at 96.
72. *Id.* at 98.
73. *Id.* at 99.
74. *Id.*
75. *Id.*
76. *Id.* at 104. Again, note the inconsistency of classification. SRI's categories are designed for criminal "abuses," and are inconvenient for civil torts.
77. *Id.* at 105.
78. *Id.*
79. *Id.* at 92.
80. *Id.* at 93. This case is mislabeled as extortion. It should have been categorized as trespass.
81. *Id.* at 98.
82. *Id.* at 103.
83. *Id.*.
84. *Id.* at 105.

7245N.[85] Five students in Yugoslavia printed anti-government slogans on computer instead of business data.

7744.[86] Los Altos, California high school students printed spurious report cards giving Los Altos students straight A's and rival Awalt High School students all F's.

78402[87] Three high school students, given access to ARPANET, mischievously changed passwords and ordered manuals. Stopped by telling parents.

There are more such cases, but these examples should give the reader the idea of what SRI considers a "computer abuse."

The SRI collection includes cases that do not even involve computers. The most glaring of these is 7248N[88] , where telephone equipment was falsely wired to allow outside calls to be placed from certain phones. The reason this case was included was because SRI was toying with the idea of classifying telephone systems as computers.[89]

There are other cases where the offense, if any, is precisely the lack of a computer.

* non-computer (number missing).[90] Newspaper advertisement for Albuquerque auto dealer who claimed that "computer goof" forced "sale."

7725.[91] Fraudulent sales of non-existing computer equipment.

---

85. *Id.* at 108. SRI curiously labels this case as "Sedition and Hostility to the State."

86. SRI files. Apparently, this particular computer "crime" upset Mr. Parker, occurring as it did at his son's school.

> Even Parker's own family has been hit by computer crime [the report card prank is then related in Parker's words]. "We are rapidly reaching the point in this country where one sophisticated electronic thief could systematically loot and destroy a firm," Parker went on, "and no one would know what happened until it was too late. . . ."
>
> "That is why I don't laugh when someone tells me about a computer prank."

Rapoport, *supra* note 61.

87. SRI files. ARPANET is the university and military nationwide computer network developed under the aegis of ARPA. *See* Kleinrock, *The ARPANET—An Operational Description of an Existing Network*, in 2 L. KLEINROCK, QUEUING SYSTEMS 304 (1976), for a description of ARPANET. Professor Kleinrock was one of the principal designers of ARPANET.

88. Computer Abuse, *supra* note 49, at 109.

89. Personal communication with Donn Parker.

90. SRI files. The SRI case number did not survive copying.

91. SRI files. The documentation consists of three Santa Maria (California) Times articles; one claimed a $17,000 loss, a second $28,000, and a third $17,242.94.

78307.[92] Thief forged company checks (entirely by manual means) and deposited them to his account via an unrelated automatic teller machine.
7041N,[93] 7044N,[94] 7143N.[95] Dating bureau frauds. Ads claimed dates matched by computer, when firms had no computer service.

Some of these cases are crimes, but they can hardly be called "computer" crimes. There are other cases where the involvement (or non-involvement) with computers escapes explanation:

* unexplained 6832N.[96] Credit cards forged with valid names and accounts.
77334.[97] Camera dealer forged credit card receipts. There is no mention of computers in the source.
78304.[98] A one sentence squib in an unidentified paper claiming a "computer-credit card mail fraud."
78305.[99] A stolen ATM card used to withdraw money.
77310.[100] Bank embezzlement from dormant accounts. No mention of computers in source.
7733.[101] Bank embezzlement. No mention of computers in the source.
7737.[102] Bank embezzlement. No mention of com-

92. SRI files. The sole documentation is one Jacksonville (Florida) Times-Union article.

93. Computer Abuse, *supra* note 49, at 96.

94. *Id.* at 97.

95. *Id.* at 103.

96. *Id.* at 92. The source for this case was probably an article in Computerworld, which appeared on Sept. 18, 1968, at 1, col. 4. Supposedly, the Gallo mob forged Diners Club credit cards with authentic names and account numbers obtained from a mysterious copy of a printout of members.

97. SRI files. The sole documentation is a New York Times article, dated Jan. 5, 1978.

98. SRI Files. "San Francisco (UPI)—John Jay Beattie, 39, was sentenced to a five-year prison term Tuesday for computer-credit card mail fraud." That is the sole documentation.

99. SRI files. The sole documentation is one San Francisco Examiner article of June 5, 1978. The case is the lead-in paragraph "horror" story of an article on a House Banking Committee bill to limit credit card customer liability to $50. There is no other information.

100. SRI files. The sole documentation is a note of a phone conversation. The respondee specifically denied computer involvement, according to the note.

101. SRI files. The documentation consists of three Boston Globe articles, claiming various losses of $56,000, $70,000, $56,000, and $25,000.

102. SRI files. The documentation is three Boston Globe articles and one Wall Street Journal (Pacific Coast edition) article. The Globe claims losses of $349,224 and $348,622 at different times, while the Journal claims $350,000.

puters in the source.

77325.[103] Fraud, check kiting. Mo mention of computers in the source.

The collection includes two cases of round-off frauds: 7133N[104] from France, and 71318N[105] from Germany which supposedly netted 480,000 DM. SRI says that round-off fraud stories are probably apocryphal,[106] but SRI does not eliminate doubtful cases until they are proven false.[107] The amount of 480,000DM is impossible to steal in this manner.[108] There are four more cases that are probably myths: 71319M[109] (certainly so, since it too involves round-offs), and the MICR stories 6431N, 6432N, and 6433N.[110]

---

103. SRI files. The sole documentation is one Oakland (California) Tribune article, which claims a loss of $832,000.

104. Computer Abuse, *supra* note 49, at 100.

105. *Id.* at 102.

106. D. PARKER, *supra* note 52, at 114.

107. Assessment, *supra* note 4, at 10.

108. 108 *See* the Appendix to this article *infra.*

109. Computer Abuse, *supra* note 49, at 102. This is the "Zwana" story, a variant of the round-off fraud myth. According to the story, a programmer in a mail order company in England created a false sales commission account in the name of Zwana, in order to force it to be the last account. He then collected remainders after roundoffs into that last account. After three years, the fraud was discovered when Marketing (sic) pulled the first and last names of their salesmen for a promotional campaign.

An identical story was reported by Brandt Allen in Allen, *Embezzler's Guide to the Computer*, HARV. BUS. REV., Jul.-Aug. 1975, at 87. In the latter story, the false account was in the name of Zzwicke, who was a fictitious customer rather than a salesman. The fraud was discovered in an identical manner. These stories are myths on their faces. The programmer can steal only about $.0012 per account. If the company had one thousand salesmen (a good size) and if their commissions are computed monthly (a reasonable assumption), the programmer can steal only about $43.00 over three years. *See* the Appendix to this article *infra.*

The provenance of the story is second generation computers where records were kept in sequential tape and card files. That is why the programmer's phony account must be last. The myth, however, is oblivious to the fact that people files are not ordered by name, since there are too many identical names, but instead by unique account numbers whose assignment is not under programmer control.

110. The Magnetic Ink Character Recognition (MICR) story is as follows: a clever fellow (not necessarily a programmer) has printed his own MICR account number on otherwise blank deposit slips, which he surreptitiously places in the bank's convenience bins for customers. Customers without their own deposit slips use the doctored ones for their deposits, and the machines that process the MICR slips credit the funds to the clever fellow's account. In a few days, he withdraws a large sum (always a round number like $100,000 or $200,000) and disappears forever.

Donn Parker believes this story and even speculates on a "skyjack" syndrome (Assessment, *supra* note 4, at 12) because the MICR stories were reported by the media in a short time span. By "skyjack" syndrome, Parker means an imaginative crime that spurs a rash of imitations. It apparently never occurred to Parker that the frequency of these stories in the media is perhaps not due to a "skyjack" syndrome, but

It is clear that the SRI study is not just of computer crime, in spite of SRI's misleading statements. It is just as clear that the cases are not all computer abuses—SRI's formal term. The collection includes crime or not, computer or not, and abuse or not. SRI refuses to debate whether a particular case is computer abuse because "[t]his seems to serve little useful purpose."[111] In effect then, the cases are computer abuse because SRI deems them to be.

Just as objectionable is the use of doubtful data. Contrary to all accepted standards of research, SRI uses suspected mythical cases, which they themselves doubt, and unvalidated data, which they admit is unverified. SRI says that no case is removed from the collection unless it is proven not to have occurred.[112] The normal method for research dictates that only proven cases be used.

It is in this light that the strange cases listed above become understandable. Perhaps they are included in the hope that someday computer involvement may be found. But more likely they are unexamined cases, provided by clipping services whose staff could not tell the difference between a credit card and a computer. Most of SRI's cases are supplied by clipping services. Whether such cases are really computer crimes is a debate that serves no useful purpose, and they are computer crimes (or abuses) until proven otherwise.

Part of SRI's difficulties are no doubt definitional, namely: what is crime (or abuse); what is a computer; and finally, what is a computer crime (or abuse). SRI case 7248N, the telephone case, illustrates SRI's difficulties in defining computer. Case 7245N, the Yugoslavian free speech by computer case, illustrates SRI's difficulties in defining a crime. SRI, because of the label "sedition," does seem to consider this case a crime, contrary to American law and the constitution.

The credit card cases, the ATM cases, and any number of false record entry cases, illustrate SRI's difficulties in defining "computer

---

to the media's love of a good myth. One can be fairly confident that these stories are myths. MICR printers sell for as much as $130,000, according to DATAPRO REPORTS ON BANKING AUTOMATION—a buyers' catalog of banking hardware and software. Obviously, only authorized people have access to them. Use of these machines appears to be controlled. Banking equipment capable of MICR printing (there are several) produce tapes, called proofs, and contain counters so that unauthorized use can easily be detected. MICR printing is expensive, technically demanding, and uses a special, magnetically sensitive ink. Most banks do not do their own printing, but contract the printing out to specialty printers. SRI lists these cases as "unverified."

111. D. PARKER, *supra* note 52, at 12.

112. "Several unverified reported cases in the file are suspected of being without basis of fact but they remain in the file as real cases until proven otherwise." Assessment, *supra* note 4, at 10.

crime." These cases are real crimes, often involving significant losses. They constitute the bulk of SRI's real crimes. Although computers process the input, the false records are manually prepared. They involve altering the input and occasionally the output of automated record-keeping systems.

A good example of falsified input is SRI case 77331.[113] Briefly, one Raymond D. Ressin, an employee of Hanifen, Imhoff, and Samford, stock brokers, and his outside accomplice, Robert N. Millar, defrauded the firm of $171,756.17. Millar opened a legitimate "cash" account with the firm, purchasing 200 shares of Loren Industries stock for a total of $300.[114] "Cash" accounts had to be paid in full and did not qualify for loans from the firm. Ressin changed the account number suffixes from those of a "cash" account to those of a "margin" account.[115] Up to fifty percent of the market value could be borrowed for "margin" accounts from the firm. In addition, Ressin changed the company code for Loren Industries to LILM, the authorized code for Long Island Lighting, an approved margin stock worth $130 a share (instead of $1.50, the value of Loren).[116]

The effect was to fraudulently increase the value of Millar's account in the firm's record-keeping system from $300 to $26,000, giving Millar a borrowing power of $13,000. The thieves then borrowed and bought other stocks, parlaying the initial $300 investment to a net of $171,756.17.

> The first two purchases of Loren Industries stock in the Robert Millar account were fraudulently switched to a "margin" account by altering the last two digits . . . on the customer buy form. . . . Thereafter fraudulent transfer from "cash" to "margin" was accomplished by some person with access to the corporate records, making adjustment entries in accounting input records fed to the computer. These entries are handwritten on forms provided for the purpose.[117]

And again, the stock code LILN was manually entered in the booklet for approved margin stocks published by the firm.[118] Ressin never touched so much as a computer terminal. The theft was discovered by the firm (how is not explained) and when Ressin was questioned about the propriety of LILN coding for Loren, he com-

113. SRI files. This case is one of the few in the entire collection that is well documented, chiefly because it contains the investigating officer's report and the Affidavit for Arrest Warrant, Criminal Action No. 122398, City and County of Denver, Colorado. The report is clearly written and detailed.

114. Affidavit, *id.* ¶ 6.

115. *Id.* ¶ 7.

116. *Id.* ¶ 8.

117. *Id.* ¶ 10.

118. *Id.* ¶¶ 8 & 18a.

plained of illness and never returned to the office. Ressin and Millar were arrested, tried, and convicted. They received a very light sentence (sixty days for Ressin, probation for Millar) vigorously protested by the prosecutor, who had trumpeted the case as a "computer crime."[119]

The connection of SRI case #77324 with computers is obscure, but perhaps it is an example of tampering with output forms.[120] In that case, a Sacramento city accountant allegedly forged voided checks, for a total of $17,000 (a newspaper amount). The checks were computer forms stamped "void" and were originally used by the computer operators to align the printer for a subsequent check run. The accountant and his accomplices passed the voided checks in retail stores.

Such cases are the bulk of SRI's collection where there is real crime. But are they "computer crimes"? Some would claim that they are, arguing that a computer is not just a computer, but all input in whatever form, all output in whatever form, and the organization and procedures as well (even manual ones), constitute a computer.[121] Such a definition is not useful, since it is too broad. Almost any crime that entails an attack upon the integrity of records would be a "computer crime," and valid distinctions, such as fraud, embezzlement, theft, vandalism, and malicious mischief, would be lost.

Is theft a "computer crime" if the record-keeping is automated, but a drab fraud if it is manual? Such a classification scheme is logically indefensible. It would mean defining offenses by the instrument of the acts, rather than by the acts themselves. But if one accepts such an argument, then why does SRI have so few cases? There must be thousands of credit card frauds; why does SRI have only a half dozen? A significant portion of white collar crime involves false vouchers, false orders, false billings, and so on. Why so few in this collection of computer crimes?

If SRI defined its terms and applied them in a logically consistent manner, it would have either few computer crime cases, or a

119. *See* Delsohn, *Tooley Hits Slap-on-Wrist Sentence*, Rocky Mountain News, July 20, 1978 (page and column not discernible); Seldner, *Brokerage Embezzler Receives Suspended Sentence*, Denver Post, July 20, 1978 (page and column not discernible).

120. SRI files. The sole documentation is one article—Abramson, *City Employee Faces Forgery Charges*, Sacramento Union, Oct. 1, 1977 (page and column not discernible).

121. GAO REPORT, *supra* note 24, at 74. *See also* A. BEQUAI, COMPUTER SECURITY 188-89 (1978); *Hearings, supra* note 57, at 7-8 (statement of Sen. Abraham Ribicoff); 125 CONG. REC., Jan. 25, 1979 at S711-S712 (statement of Sen. Abraham Ribicoff in introducing S.240).

flood of them. Either way, their value is dubious. SRI seems to have struck a compromise: a handful of credit card cases, but not thousands; a few ATM cases, but not hundreds; a few bank embezzlements, but not all. The result of this compromise is inconsistency and statistical invalidity.

There are genuine crimes that do involve computers in the collection. There is a large number of vandalism and sabotage cases, sixty-six out of a collection of 375 total cases, and more now due to a recent rash of bombings of data processing centers in Italy by the *brigate rosse*. These cases involve shooting, stabbing, burning and bombing of computers. A few, involving disgruntled employees, may be apocryphal. Half of the vandalism or malicious mischief cases involving destruction of computerized records or programs are listed by SRI as unverified.[122]

A smaller, but still significant amount (30 out of 150[123]) involved theft of computer services, computer parts, and even whole computers. Exactly half of these (fifteen) were listed as unverified. It should be noted that this list of 150 cases is dated 1973, and many unverified cases could easily be verified by now. On the other hand, there is no reason to believe that they have been.

There are also genuine computer crimes. There are at least two in SRI's case files and there must be a few more. By genuine computer crime, is meant a crime that, in fact, occurred and in which a computer was directly and significantly instrumental. One, SRI Case #66314Y is also one of the earliest reported in the media.[124] Apparently, in 1965, the National City Bank of Minneapolis computerized its checking. The malefactor programmed the computer to ignore overdrafts on his account and, according to *Computerworld*, stole $1,357. He was caught when the bank reverted to manual processing due to a computer failure. The programmer made restitution and received a suspended sentence. He intended an extended "float" rather than theft, but lost control, and soon his overdrafts piled up so that he could not readily cover them.

The second valid case of computer crime, the Flagler Dog Track trifecta fraud (SRI case #77322), is also the sharpest example of such crimes. This case is one of the few in the SRI collection that is well documented.[125] Flagler Dog Track in Florida used two PDP-8 computers to compute odds and payoffs in trifecta betting. Because the

122. Computer Abuse, *supra* note 49, at 91-112 (app. A).

123. *Id.*

124. *Id.* at 91. *See also Whir, Blink—Jackpot! Crooked Operators Use Computers to Embezzle Money*, Wall St. J., Apr. 5, 1968, at 1, Col. 6; *Journal Warns of Dishonest "Computer Operators,"* Computerworld, Apr. 17, 1968, at 1, col. 1.

125. D. Maloney, Report on Investigating the "Skimming" at Flagler Dog Track

betting was fast and furious, and the computations were time-consuming—even for a computer—the dog race was often over before the computers finished their calculations.

A confederate communicated the results of the race to the computer room, where the computer operator threw the stop switch on one of the PDP-8s, causing the program to halt execution. At the console, the operator then "deducted" a number from the count of losers in computer storage, and added that same number to the count of winners, also in storage. He then restarted the computer to allow the program to complete its computations. Later, the gang ran the ticket printers to print fraudulent winning tickets, which other confederates cashed the next day. Since winners are paid from a pool formed by the losers' money, dog track officials would not detect the loss—each true winner would simply get less than he should.

The duplicate PDP-8 was intended to prevent such frauds, besides providing backup. The gang, however, turned in the doctored report to track officials, and disposed of the incriminating report produced by the untampered, second computer. In the opinion of the investigators, the crime could not have succeeded without lax auditing.

Cases of indisputable computer crime in the SRI collection are extremely rare, probably no more than a half dozen in the entire collection, though just how many is impossible to say.[126]

SRI's source of cases is mainly newspapers. What this means is that SRI documentation is inconsistent and unreliable. When the collection consisted of 375 cases, SRI sources were:[127]

| | |
|---|---|
| survey questionnaires | 71 |
| *Computerworld* (trade paper) | 71 |
| newspapers | 76 |
| private communications | 62 |
| magazines, journals | 43 |

(Conn. Comm'n on Special Revenue, 1977). This is a detailed description of the crime and its detection provided by the investigator, Mr. Dardis.

126. Rob Kling, a professor at the University of California at Irvine, assigned four of his students to check the accuracy of this author's impressions of the SRI cases. The students took a statistical sample of forty cases and found only two to four sufficiently researched to be usable. Kling's impression is that about two dozen cases are usable out of the entire collection. The author's impression is that only about a dozen are usable. The difference may be that the author's interest is the narrower one of crime, while Professor Kling's interest is a broader one of social abuse. Professor Kling is both a sociologist and a computer scientist. Personal communications with Rob Kling.

127. Assessment, *supra* note 4, at 8; D. PARKER, *supra* note 52, at 24 (shows only 75 newspaper references).

| | |
|---|---|
| books | 22 |
| speeches | 13 |
| law enforcement | 13 |
| unpublished papers | 4 |
| | 375 |

The magazine and journals are almost all *Datamation*, a trade magazine, or security industry organs. Both *Computerworld* and *Datamation* use a clipping service for computer crime stories, thus these sources are, in reality, mostly newspapers. With the exception of Alan Westin's *Databanks in a Free Society*,[128] a respected book, the remaining books are "pop" books. Thus, the source "books" are also sensationalized newspaper stories, except the four privacy intrusion cases from Westin's book.

The cases taken from speeches should also be attributed to newspaper stories (and hearsay), even more distorted because they are inevitably garbled in retelling. This results in about 208 cases out of 375 whose actual source is newspapers (or rumors). Only thirteen cases were provided by law enforcement or court documents. Of more than seventy of SRI's later cases, the documentation consists almost entirely of newspaper articles, sometimes a single "filler" paragraph, and only about six are supported by law enforcement or court documents.

Some of the articles are obviously press releases.[129] Others

128. A. WESTIN, DATABANKS IN A FREE SOCIETY (1972).

129. A brief, but otherwise typical, press release under the letterhead of Lobsenz-Stevens Inc., and dated May 8, 1979, was given to the author by the editor of a trade paper. (A copy of the press release is on file at the Journal offices.)

LORSENI-STEVENS INC. CONTACT: Nat Gilbert or John Neeson
Public Relations
For Release Tuesday, May 8, 1979

COMPUTER CRIME OFTEN UNDETECTED FOR YEARS;
COOPERS & LYBRAND SEMINAR OUTLINES METHODS
FOR CURBING AMERICAS NEWEST ILLICIT INDUSTRY

NEW YORK, May 8 — The average armed robbery involves less than $10,000; but the average reported corporate computer theft involves about half-a-million dollars. Computer theft often not only goes unsolved, but undetected for years

To explore new ways to stop America's newest illicit industry—corporate computer crime—Coopers & Lybrand, one of the world's largest accounting and consulting firms, today held a special seminar for top executives conducted by its own battery of computer consultants.

Today, with more than 50% of major U.S. corporations' assets controlled by computers, a new type of criminal and sleuth, outthinking each other within the intricacies of computerized corporate accounting, is making his way into the business world, according to Charles F. Jacey, New York Group Managing Partner of Coopers & Lybrand.

Jacey says that corporate computer crime, and the means of stopping it, may well

seem to be "assignment" stories that are probably disguised publicity.[130] But all of them are formula articles that begin with a fetching, "horrible" example, perhaps fictional or a grossly distorted news story, in the first paragraph to grab the reader's interest. Then, there are two or three additional paragraphs that explain the problem, real or imaginary. As a rule of thumb, the fourth or fifth paragraph usually cites the story's sponsor as an "expert." The rest of the article elaborates on the "problem" and the suggested "cure." The tone

---

be America's newest boom industry. "The computer criminal may be a mild-mannered intellectual carrying a floppy disc or magnetic tape reel; but he is far more dangerous to a company than anyone carrying a gun," according to Jacey. To illustrate, he briefly mentioned three recent thefts totalling over $12 million:

- A computer expert with access to a California bank's fund transfer system drained off $10 million by manipulating the bank's computerized accounts;
- An enterprising computer expert set up an elaborate business distributing millions of dollars of telephone equipment that he was able to expropriate by manipulating their computer;
- The chief teller on a major New York savings bank was able to fleece that institution of $1.5 million over several years by directing its computers to make payments to phoney accounts.

With these incidents, and many others, in mind, Coopers & Lybrand's hundred-man EDP consulting group has devised elaborate systems to keep client's computers safe and secure. A good security system should encompass several basic controls: limited physical and electronic access; limiting what authorized personnel can do with the computer; and simplified electronic reporting of all unauthorized use of the equipment for management.

"Building and maintaining computer security systems is a form of insurance—and like other forms of insurance, every corporation needs a program in keeping with their potential risks," according to Salvatore C. Catania, a Partner of Coopers & Lybrand. "Our studies have shown that most organizations have inadequate EDP security systems—with potential loss of millions of dollars."

The Coopers & Lybrand seminar also treated problems of contingency planning for power outages and natural disasters that may befall corporate computer operations. With more and more business functions becoming computerized, the number of days, hours, and even minutes a computer is "down" can seriously disturb customer relations and income.

Other Coopers & Lybrand speakers, in addition to Mr. Jacey and Mr. Catania, include Martin E. Silverman, Manager, discussing contingency planning details; John F. Owens, Senior Consultant, explaining the basic elements of a computer security system; Vincent Campetelli, Partner, talking about security and controls; and Samuel A. Ruello, Partner, summarizing security and contingency systems for general executives.

A booklet describing EDP security is available without charge from the Director of Communications, Coopers & Lybrand, 1251 Avenue of the Americas, New York, New York 10020.

It is probably not generally appreciated just how much of a newspaper's pages are filled with this sort of "junk mail" masquerading as news or feature articles.

130. Reporters refer to a certain type of story as "assignments." The term is significant; reporters do not pick their stories but are assigned them by the editor or publisher. There are several motives for assignments, not the least of which is the editor's receipt of an interesting press release.

is persuasive: buy the computer security firm's services, support the legislator's bill, accept the idea being advanced. Such "horrible" examples are the sole documentation for the following SRI cases:

7727[131] horrible example of student tapping into a computer in article on dangerous "computerniks."

77210[132] horrible example of student stealing from computerized inventory system in computer crime article originating with a computer security firm.

77214[133] horrible example of John Draper (Captain Crunch) using hobby computer as a "blue box" in article on dangerous hobby computers.

77313[134] horrible example of welfare fraud in computer crime article originating with a computer security firm.

77314[135] horrible example of ATM thefts in data security section of article on EFT.

77316[136] amusing example of bank error in computer crime article whose source is one of the authors of the Ribicoff computer crime bill.

77342[137] no specific case, just an article on phony invoice frauds, apparently provided by the Postal Service.

77344[138] horrible example of an ATM customer robbed by dupery in feature on ATM crime apparently provided by the Federal Trade Commission.

---

131. Gribbin, *Beware Computerniks at Work. They're Compulsive, Brilliant—and a Key to Computer Crime*, Nat'l Observer, May 23, 1977, at 1 (column not discernible). Attribution is to August Bequai, one of the authors of Senator Ribicoff's computer crime bill, and to Donn Parker.

132. Gutman, *Most Computer Users "Easy Targets" for Fraud Security Consultant Says*, Baltimore Sun, Oct. 2, 1977, at 1 (column not discernible).

133. Schrage, *Telecommunications Thief Uses Home Computer as a Weapon*, Wash. Post, June 23, 1978 (page and column not discernible). This story was apparently released by the prosecutor of the case to justify the questionable prosecution of Draper. The reporter apparently also checked with Radio Shack and Donn Parker, whose opinions were also quoted.

134. *Computer Crime a Corporate Menace*, Star-Telegram (city not discernible), Mar. 27, 1977.

135. *News Perspective*, DATAMATION, June 1977, at 180. Attribution is not clear, and the story may be straightforward.

136. *Great Computer Robbery*, Memphis Commercial Appeal, Feb. 27, 1977 (page and column not discernible). Attribution is to August Bequai.

137. Lehner, *Businesses Still Fall For the Old Racket of Phoney Invoices*, Wall St. J., June 16, 1978 (Pacific Coast ed.) (page number not discernible).

138. Blumenthal, *Electronic Fraud Accompanies Move Toward Tellerless Banking*, N.Y. Times, Mar. 26, 1978, at 1. Attribution is to the Bureau of Competition of the Federal Trade Commission. Citibank is quoted in paragraph 6, but this was not the source, since the reporter indicated that he was merely checking the story with another "expert."

78205[139] no specific case, just a feature on thefts of hobby computers from retail stores.

78305[140] horrible example of customer forced to pay for money withdrawn by a stolen ATM card in article on a bill to limit customer liability. The apparent source is a legislative committee.

Documentation for these cases is at best a scanty paragraph, sometimes just a paragraph. One example will suffice

> People got a laugh out of Christopher Cossette, the 36-year-old Floridian who received more than $110,000 in checks before a computer error could be corrected. The interest he collected while trying to find a way to get somebody to do something about the mistake bought him a sport car and a swimming pool.[141]

This is the sole documentation for this case. It is deplorable, and in addition, it is irrelevant to any serious study of computer crimes.

Generally, newspaper accounts of "computer crimes" are unreliable. SRI says

> Newspaper accounts of computer abuse are treated with particular skepticism. My experience is that the most one can derive from a newspaper article about computer abuse is that something interesting may have happened.[142]

This well deserved skepticism is not evident in the collection of cases. SRI explains that it "feels" justified in presenting statistics based on such documentation because "there seems to be a little bit of truth, at least" in these stories.[143] SRI offers no evidence to support this contention. In fact, some of the newspaper stories contain no truth. In any case, "a little bit of truth" is worse than worthless for a serious study, because it is misleading.

Some newspaper stories are more accurate than others, but generally, a newspaper article is never fully correct. There is simply too much haste, and the only qualification most news people have for covering technical and scientific events is a degree in journalism. At worst, newspaper stories of "computer crimes" are so bad that they beggar description. A good example of egregious reporting concerns the so-called ILLIAC time theft at Ames Research Center in Mountain View, California. According to the *San Francisco Chronicle*, whose report was carried world-wide by UPI, two "computer experts" stole millions of dollars worth of computer time by making

---

139. Scannell, *Crime Wave Hitting Retail Shops*, Computerworld, June 26, 1978, at 59, col. 2. Attribution is to a retail store owner.

140. *Checkless Society Might be a Loser*, S.F. Examiner, June 5, 1978 (page number and column not discernible).

141. *See* note 136 *supra*.

142. D. PARKER, *supra* note 52, at 25.

143. *Id.*

unauthorized use of the ILLIAC-4 at Ames.[144] The indictment charged only that the men stole time of a value in excess of $100.[145] The reporter checked this value with another "computer expert" (actually a computer security consultant) who opined that $100 would buy a mere millisecond of time on the ILLIAC-4.

Apparently, the reporter was duly impressed. Since the theft supposedly covered a two month period, that would amount to "millions of dollars." Amusingly, the Chronicle couldn't even get the arithmetic straight ($100 x 1000 milliseconds) and printed $10,000 a second instead of the correct figure of $100,000. But $100 a millisecond is a preposterous figure, almost twice the Gross National Product. The facts were that the two men were not computer experts, and had not used the ILLIAC-4, which cannot be used directly, but a PDP-10. Their real offense was the theft of electronic equipment (oscilloscopes and terminal parts). They used a text editor installed on the PDP-10 to write documents for a business they were trying to set up, in part using the stolen equipment.[146]

Later, other papers got the story more accurately. *Computerworld* gave the value as $2000[147] as did a few suburban papers.[148] The *San Jose Mercury* and *News* quoted $1,000.[149] Unfortunately, the *Chronicle*'s absurd story was the one disseminated by UPI, which apparently never got the straight story.

Not one article in any paper was fully correct. All quoted usage for a two month period for which even $2,000 is excessive.[150] In fact, the estimated usage, based on the men's own admission, was about six hours a week over a thirty-two week period, which Ames calcu-

144. Cooney, *Case of the Stolen Time*, S.F. Chronicle, Jan. 21, 1978 (page number and column not discernible).

145. The number stamped on the face of the court document is CR 78025 WAI (United States District Court for the Northern District of California).

146. Personal communication with Marcelline Smith, director of the Ames Research Computer Center.

147. French, *Two Charged in Theft of Nasa System Time*, Computerworld, Feb. 6, 1978, at 6, col. 1.

148. *Pair Charged in Plot to Steal Computer Time*, Sunnyvale (California) Valley J., Jan. 25, 1978 (page and column not discernible). *See also Pair Charged in Computer Time Theft*, Palo Alto Times, Jan. 21, 1978, at 1. Both articles repeat the $100,000 per second figure—apparently too juicy to be resisted.

149. San Jose News, Feb. 3, 1978 (page and column not discernible); San Jose Mercury, Feb. 3, 1978 (page and column numbers not discernible).

150. A local computer service company contacted by the author quoted a rule of thumb figure of either $6 or $10 per hour, depending on whether usage was prime time or not. The quote included connect time, cpu time, and storage on roughly comparable hardware. This is less than $500 for a two month period.

lated at $1,924, just about right.[151] The trouble was that a reasonably accurate estimate took time for the computer center's staff to prepare; time that none of the papers, even the more conscientious, could afford to grant. And really, there is no reason for newspapers to be more accurate. It is not important for the reader, but it is all important for research. Coverage of this one story illustrates exactly the full range of newspaper reliability—from almost right to completely wrong.

Related to the unacceptable documentation of SRI's cases is the inadequacy of SRI's verification of cases. SRI does attempt to verify cases reported in the press. SRI mails letters to the paper or named participants pointing out the inaccuracies of news articles and soliciting confirmation. It also attempts to verify by telephoning sources; there are a few handwritten notes or logs, usually frustrated, of these attempts. SRI has had a few notable successes, but progress is slow.[152] For example, it has determined that the Pennsylvania Railroad boxcar thefts were not a computer crime, and that the theft of $10.2 million from Security Pacific by Stanley Mark Rifkin was actually accomplished by the impersonation of a bank officer over the phone and not by manipulating a computer. Illogically though, SRI still includes the latter as a computer crime because the transfer cage, where Rifkin learned the bank's funds transfer password by observing the teletype operators, and to which he should not have had access, is located in a section of the computer room.[153]

Their verification attempts, however, are spasmodic with little or no follow up. An attempt, by phone or letter, that is frustrated is rarely attempted again. The fact is that it is almost impossible to track down a newspaper story, especially if the story is substantially in error, since newspaper staff react defensively and are uncooperative. It is worse if the story is "old" (more than a few weeks). For real current events, the principals have reasons for not cooperating; victimized firms generally refuse to comment because the matter is before the courts, and perpetrators refuse to reply for obvious reasons.[154]

Thus, for 375 cases, at that time the total of SRI's cases, only seventy-seven had been verified.[155] To what degree of detail, SRI does not explain. Based on knowledge of two cases in SRI's files, verification is erratic. SRI's documentation for the Ames Research

151. Personal communication with Marcelline Smith. *See* Taber, *On Computer Crime (Senate Bill S. 240)*, 1 COMPUTER/L.J. 517 (1979).

152. D. PARKER, *supra* note 52, at 25.

153. Personal communication with Donn Parker.

154. D. PARKER, *supra* note 52, at 42-43.

155. Assessment, *supra* note 4, at 10.

case is eight newspaper clippings, two UPI wires, the indictment (which, by the way, is short of details), and notes of defendants' behavior and appearance at arraignment, prepared by one of the assistants. There was also a memo on SRI stationery, expressing grudging admiration for "all the press our buddy" got for his absurd estimate of the ILLIAC time. There is no apparent attempt, reflected in the file, to get the accurate story from the director of the Ames Research computer center, who kept complete notes of the incident.

The second case, #77411, is the University of Alberta case, where three students were indicted under Canada's telecommunications theft law for obtaining unauthorized computer services from the University of Alberta. The total documentation is two *Computerworld* articles.[156] Lacking is a third *Computerworld* article[157] announcing the conviction of two of the students (the third was acquitted). There is no attempt to communicate with the director of the computer center reflected in the file.

SRI is confusing in its use of the word *verified.* It claims 174 cases verified out of 374.[158] This is misleading, and amounts to a pun on the generally-accepted meaning of *verified* and SRI's own private definition. In the private definition a case is "verified" if

- a legal documents describe the case
- a staff member obtained the case from a person considered by SRI as reliable
- a newspaper article seems complete enough.[159]

In other words, the private definition is a scale of confidence, largely judgmental, that an event reported in the news more or less occurred. What this means is that for 381 cases, 77 were more or less verified, SRI chooses to believe 218 more, and 86 were unverified by any definition.[160]

Probably, more cases are verified (in the generally accepted sense) by now, but that is not certain. From available information, it would appear that the number of genuinely verified cases today is not substantially different from 1975—the date of the National Science Foundation report.[160] The lack of adequate verification of data is one of the most serious defects of the study.

---

156. Schultz, *Students' Conviction for Theft Held Unlikely*, Computerworld, June 26, 1978, at 4, col. 1; Schultz, *DP Service Theft Case to Test Canadian Code*, Computerworld, June 26, 1978, at 5, col. 1.

157. Schultz, *Students Guilty of Service Theft*, Computerworld, Jan. 8, 1979, at 1, col. 2.

158. D. PARKER, *supra* note 52, at 24 (table 1).

159. Assessment, *supra* note 4, at 9-10.

160. *Id.*

It should be little wonder then that SRI's statistics do not jibe with the GAO report. SRI counted 144 cases with "attributable" losses of fraud, embezzlement, and theft out of 381. This excludes Equity Funding because its huge loss simply cannot be included in the average (but otherwise SRI insists on counting it as a "computer crime" in spite of serious objections).[161] "Attributable" is not explained, but apparently means a loss figure quoted in a newspaper, presumably like Christopher Cossette's $110,000 windfall. The 144 cases are arbitrary crimes of false entry, credit card frauds, and the like, with disputable computer connections. Also, because the source is newspapers, the cases are "newsy," remarkable cases, rather than the ordinary matters, which usually never gets reported. From this, SRI got an average loss of $450,000 per "computer crime" case.[162] SRI derived the estimated annual loss of $300 million based on this average and the following unwarranted assumptions:

> Assume an average of 100 cases per year (reported). Assume also that only 15 percent of known cases are reported. With an average loss of $450,000, a total annual loss . . . would be $300 million.[163]

There is no good reason to accept any of these assumptions; one hundred cases a year is the asymptote of SRI's projection of reported cases in the media based on the past experience of SRI in its gathering of these articles. There is no reason given for the fifteen percent figure. And $450,000 is highly questionable. In sum, neither $450,000 nor $300 million have a shred of validity.

A thorough discussion of SRI's speculations on "sophisticated" computer crimes, which seem to arouse the most fear, will have to be deferred because of the length of this paper. But in brief, SRI's "sophisticated" computer crimes such as "trojan horses," "trapdoors," "time bombs," "salamis" (all essentially booby-trapped programs)[164] are unworkable. From a strictly technical view, a deliberately perverted operating system or application program is not impossible, but from a broader view, it is improbable.

Operating systems, and even application programs, are too difficult and complex for even a privileged and gifted programmer to booby-trap without considerable time and resources.[165] In effect, the National Security Agency (NSA) or the FBI or a corporation

---

161. *Id.*

162. *Id.* at 6, 13.

163. *Id.* at 18.

164. *See* D. PARKER, *supra* note 52, ch. 12.

165. *Id. See also Of Trojan Horses and Trap Doors*, DATAMATION, Sept. 1979, at 71. The Datamation article cites the Federal Deposit Insurance Corporation as its source. However, it would appear that the source was actually Donn Parker, who authored the report for the FDIC under a government contract.

could commit such crimes, but not an individual programmer. He lacks the time and the resources. Programmers cannot write code that works correctly the first time it is executed. This is especially so in a complex system, where the slightest misunderstanding of a seemingly unrelated program will "crash" the system. Operating systems and application systems lean heavily on implicit conventions and protocols, often poorly documented, if at all.

Raw code must be tested and reworked. Testing requires organization, coordination of several people, much time and resources. In contrast, coding is done alone with pencil and paper. Clearly collusion is needed to effect such crimes, but SRI fancies that the programmer poses all this danger. In fact, SRI's assumption for the "trojan horse" is that the perverted code works correctly without even the possibility of testing. That is preposterous.

In this connection, it should be noted that Rifkin did indeed contemplate a sophisticated computer crime, a "trojan horse" attack.[166] He rejected this approach as "too complex" and contented himself with a more possible crime.[167] SRI reports one case of a "trojan horse" that SRI believes occurred. A student without system privileges coded a utility program to be adopted by the installation.[168] Utility programs perform specific utilitarian functions, such as copying the contents of a tape to a printer, and are invoked from time to time by other programs. A non-privileged program cannot execute critical machine instructions; it must request services involving critical functions of the operating system, which validates the correctness of the request. These critical functions are necessary to vandalize files or programs. If the student's program were inadvertently privileged, however, then theoretically it could vandalize the installation. So, according to SRI, the student's utility program tested its machine state to see if it were invoked with the privileged bit inadvertently left on.[169] If not privileged, the program remained well behaved, but if privileged, the program would wipe out the operating system, load a file and print it out explaining in detail just how clever the long departed student had been.

The story sounds apocryphal. In any case, according to SRI, the program was eventually invoked in privileged state, the perverted code executed, and it promptly failed. SRI marvels that it failed, and that the system programmer, analyzing the ensuing dump,

166. *See* Computer Abuse, *supra* note 49, at 125-26. This was the point made in a discussion at a computer security conference held at SRI, and included as a part of Computer Abuse. It has not received sufficient emphasis.

167. *A Question of Vulnerability*, DATAMATION, Sept. 1979, at 70.

168. *Id.*

169. D. PARKER, *supra* note 52, at 112.

could find the perverted code. It would be marvelous (indeed miraculous) if it succeeded and if the systems programmer did not discover the trick, and at that, rather quickly. For the student's prank to work, he had to gain privilege, which he expressly did not have, because for his code to work it had to be tested and debugged. But for that, he had to be privileged to begin with. He needed the very resource he was trying to get in order to get the resource he was trying to get. In computer terminology, the situation is a deadlock. In the student's case, it is a hopeless situation.

SRI's "sophisticated" crimes have not occurred in fact, with the possible exception of the "trojan horse" cited above. They are speculative. It is important to emphasize this point, because the "sophisticated" crime is precisely the one that arouses the most fear, and in academic computer science literature enjoys the most intensive interest.[170] In other words, the least likely type of crime, of which there is no record that it ever occurred, receives a disproportionate amount of attention, while the common, feasible, unsophisticated crime, like the entry of a false record, is mislabeled as a "computer crime," but otherwise ignored.

People without an intimate knowledge of programming can easily be misled into believing these stories, and even programmers, who should know better, may believe them. But once a knowledgeable person thinks about it, their unworkability becomes apparent—like Rifkin, who did think about it and rejected it.[171]

SRI's charge that programmers are unethical or suffer from a poorly developed sense of professional behavior[172] is unwarranted. Supposedly, programmers commit irresponsible pranks, essentially "crashing" the system as a joke. On the contrary, programmers struggle with commendable dedication to keep faulty and inadequate systems going. The basis for SRI's misguided charge seems to

170. *Id.* Parker's technique, elaborated at pages 109-10, will not work without more complications than described. The author therefore corrected Parker's technique for technical simplicity and accuracy. Parker either distorted the story for lay readers or described an antique computer.

171. *See* note 166 *supra.*

172. D. PARKER, *supra* note 52, at 53-56. The besmirching of dedicated programmers as dangerous "compulsive bums, disheveled" (*id.* at 49-50) is particularly offensive where Parker quotes approvingly from a diatribe by Joseph Weizenbaum. Parker is not alone in this view. *See also* Zientara, *Survey Cites Decline in DP Student's Ethics*, Computerworld, Aug. 20, 1979, at 11, col. 1. The "survey" consisted of hidden questions in an exam given by a professor to his students in a computer science course at the University of Western Ontario, and is obviously invalid as a "survey." According to the Computerworld story, in a previous survey of open questions, the students scored well, so the professor hid the questions the second time, and in essence, tricked his students into providing the answers he wanted.

be the custom in an academic environment of computer science professors encouraging students to "crash" the system.[173] It is hoped that the victim system is a student system, not used by the university for business purposes. The motive is twofold: pedagogic, to teach students the need for system reliability; and for research, to make good use of willing, free labor to develop systems reliable enough to withstand determined and ingenious attack.

SRI's objection to this practice is that the university is training future professionals in criminality. The objection is incomprehensible. SRI seems to be really objecting to the development of high reliability systems. The minute the student changes his environment from academic to professional, his goal changes to keeping his employer's system going. Any other behavior would probably cause his peers to lynch him.

There is indeed confusion over the propriety of making incidental personal use of an employer's computer, for example, playing tic-tac-toe or Adventure, or balancing one's checkbook. There is certainly no consensus in either the industry or the profession. But such practices do not warrant the impression that there is "an appalling lack of ethics and morality in the data processing professions."[174] SRI's accusation is contrary to truth, an insult to the profession, and a disservice to all.

## IV. Conclusion

To summarize, the GAO report provides the only reliable data because it is based on well-documented cases with verifiable losses. No firm conclusions can be drawn from it because it is too skimpy, amounting to no more than a listing of dollar losses, and because its definition of "computer-related crime" is disputably broad. Nevertheless, it does indicate that "computer crime" is insignificant, and its figures accord well with SRI's own hypothesis that computers should minimize the incidence of crimes such as fraud and embezzlement while increasing the losses for each incident.

The SRI study is unreliable because it is based on poor documentation, unacceptable methods, and unverified (indeed unverifiable) losses. In addition, it is unfocused, and inconsistent within its own definitions and terminology, which are themselves disputable. There is a marked deterioration in quality from the first report, *Com-*

173. "I am very concerned about this because I think we are creating whole new generations of computer criminals." *Hearings, supra* note 57, at 61-62. This theme is continually adverted to by Mr. Parker in his writings and speeches.

174. *See* note 59 *supra.*

*puter Abuse*,[175] far from perfect itself, to the later reports, due no doubt to lack of adequate review. However, we are indebted to the SRI study for its hypothesis, for debunking several so-called computer crimes, and for unearthing a few genuine computer crimes. At best, the study is preliminary, and one of its most serious faults is the publication of raw, preliminary data without careful qualifications. This is a breach of accepted social research standards.

The passage of time alone has invalidated the projections of *Economic Losses*. This does not leave much. "Computer crime" is a media creature, largely fed by computer security industry press releases, that has superseded the earlier creature, the "computer error." In 1970, the California state legislature, exasperated by media reports of "computer errors," contemplated enacting licensing requirements for data processing professionals.[176] It was an unwise plan to end "computer errors." According to *Datamation*, the media "ill-wrought" such stories.[177] It came to nothing.

"Computer crime" has gone further in legislation than "computer error." Computer crime laws, hastily and carelessly drawn, have already been enacted in about a dozen states, and are being considered in many more. A federal bill is pending as well. None of them are necessary, and it is appalling that they are justified by such inadequate research.

## APPENDIX: THE ROUND-OFF FRAUD

The best known and the most cherished of all computer crimes is the round-off fraud. There is scarcely a programmer in the world who has not heard of it. The fraud is an article of faith in the profession. In a study of future economic losses caused by computers, thirty-four computer specialists believed that thirty-six such thefts would occur each year with an average loss of $110,000 per theft.[178] This prediction was based on a case where a programmer reportedly stole $200,000 in a successful round-off fraud.[179] Donn Parker of SRI has at least three such cases in his collection of computer crimes. One involved stealing the remainders in sales commission computations for the salesmen of a mail order company[180]; another was the theft of 480,000 deutche marks by stealing remainders in a German

175. Computer Abuse, note 49 *supra*.

176. *State to Hold Hearings on Programmer Licenses*, DATAMATION, Nov. 1, 1970, at 97.

177. *Id.*

178. *See* Table 1 *supra*.

179. *See* the text accompanying note 23 *supra*.

180. Computer Abuse, *supra* note 49, at 102 (SRI Case #71319N).

bank[181]; while the third was a similar theft from employee salaries in a French company.[182]

Not just computer professionals know about this fraud. A former prosecutor who advises the federal government on computers gave the alarm in a *Saturday Review* article,[183] and claimed that a victim was a major New York bank. The Department of Justice offered this computer crime in Senate testimony in support of Senator Ribicoff's computer crime bill.[184] Knowledge of this sophisticated computer crime has spread from programming circles through the business world, law enforcement, to state legislatures, and finally to Congress. It is the best and most important example of a sophisticated computer crime, on which there is wide agreement, and is cited as an impressive instance of the widespread problem of criminal programmers.

It has never happened.[185]

This Appendix will review the mechanics of the fraud. However, the reader is cautioned not to draw any inferences about actual banking practices. This discussion oversimplifies the complexities of interest computations, and may not conform to actual practice. The discussion deals with the details of the round-off fraud as com-

---

181. *Id.* (SRI Case #71318N).

182. *Id.* at 100. (SRI Case #7133N).

183. DeWeese, *The Trojan Horse Caper—and Assorted Other Computer Crimes*, SATURDAY REV., Nov. 15, 1975, at 58. Probably, "advisor to the federal government" means lobbyist.

184. *Hearings, supra* note 57, at 28 (statement of J. Keeney, Acting Ass't Att'y Gen., Crim. Div., Dep't of Justice.)

185. Some of this author's older programmer friends hotly insist that the round-off fraud actually occurred, supposedly in a New York bank in about 1968. Parker claims that the Wall Street Journal reported such a fraud on page one in 1968, but he gives no references. D. PARKER, *supra* note 52, at 113. Extensive research of the Wall Street Journal's indexes for the years 1961-74 fails to uncover any references to such a story under either the "computer" or the "crime" heading. There were two computer crime articles, both published on April 5, 1968, but this "crime" was not mentioned in either article. The author also searched the New York Times index for the years 1966-72, under "data processing," "fraud," and "embezzlement," and found one doubtful reference. In Smith, *Controls Haven't Caught Up to Boom in Computers*, N.Y. Times, Feb. 22, 1970, Sec. III, at 11, col. 4, the author states:

> a programmer in a Mid Western bank was able to alter a savings account program to transfer the "round-off fractions" of cents in the interest calculations of every depositor to an account maintained under a fictitious name. He was able to withdraw large sums of money before he was detected.

Section III was the business news section, and the "source" for the story was Joseph J. Wasserman of Computer Audit Systems, Inc. This article has every appearance of being a press release. It is interesting to note that it was alleged to be a "Mid-Western bank" in a New York paper. Presumably, the mid-west press release attributed the "crime" to a New York bank.

monly understood, and does not necessarily reflect actual practice. Its purpose is to demonstrate that mathematically the round-off fraud is improbable, especially as described by SRI. Should actual practice be factored in, the round-off fraud becomes too preposterous to discuss, regardless of how many people (including senators) believe it.

If there are pennies in an account, fractions of a penny result when interest is computed. Even if an account has no pennies, or if pennies are ignored as is the case for credit unions, fractions of a penny may still result from non-integer interests, like 5-¼%.

There are several strategies to handle these remainders: the bank may always roundup to the nearest penny; the bank may always truncate (round down) to the nearest penny, in effect, keeping remainders for itself; or it may round up to the nearest penny for remainders of five mills or more. The last technique, the one taught in grade school, is the most common, though the second is sometimes used.

But there is a problem with this technique—it is not fair to the bank. Only for four and eight percent interest is the average mills given away when rounding up exactly equal (on the average) to the mills kept when truncating. Most interest rates result in a loss to the bank. The reasons for this odd behavior lead immediately into number theory, which, to treat rigorously, is beyond the scope of this Appendix. Part of the problem is that the average of the integers 0 to 9 is 4.5 and *not* 5; yet one rounds at 5. Thus, for the integers 0 to 9 we give .5 on the average for every integer

| | | | | | | |
|---|---|---|---|---|---|---|
| integers | 0 | 1 | 2 | 3 | 4 | keep by truncation |
| integers | | 9 | 8 | 7 | 6 | 5 |
| (n>5)−10 | | −1 | −2 | −3 | −4 | −5 give by round up |

On the average, for every 1, which we keep, there is a corresponding 9 for which we give 1. Similarly, for every 2, 3 and 4, which we keep, there is a corresponding 8, 7 and 6 for which we give 2, 3, and 4. But there is no corresponding 5 to keep for the 5 we give away. Thus our average loss in rounding is .5.

The situation is more complicated for interest because we are no longer rounding the integers 0 through 9 but multiples of the interest, for example 0 2 4 6 8 0 2 4 6 8, which is "balanced," and the net of giving and keeping is zero. Again by threes this time

0 3 6 9 2 5 8 1 4 7

whose complete residue class modulus 10 contains a 5, thus it is not "balanced" and again we lose an average of .5 per integer. Consider now the bank's disaster, the multiples of 5 mod 10

0 5 0 5 0 5 0 5 0 5

Here the loss is an average 2.5 per integer.

But even this is not complicated enough. Actually, in interest computations, we are dealing with multiples of the integers 0 through 99 and rounding at 50; or the integers 0 through 999 and rounding at 500; depending on the number of decimal places to the right of the pennies, which is the function of the significant digits of the interest. Thus, the grade school rounding rule is "fair" if and only if the multiples of the interest rate I, mod $10^d$ (where d is the number of significant digits of the interest rate) does not contain the rounding number, $5 \times 10^{d-1}$ (that is, 5, 50, or 500, etc.)
Otherwise, the bank loses

$$\frac{E \times 5 \times 10^{d-1}}{10^d}$$

(where E is number of occurrences of the rounding number in the multiples of the interest)

on the average, per interest computation. Note that 50 is a multiple of 2 mod 100 and occurs twice in the sequence

$$2(0,1,...,99) \pmod{100}$$

so the bank loses for two percent. However, 50 is not a multiple of 4, mod 100, and of the interest rates extant for the past thirty years, it and eight percent are the only ones that are "fair" using the grade school method of rounding.

What this means is that for all actual interest rates, except four and eight percent, the sum of remainders after round-off is *negative* and if grade school rounding is used, the larcenous programmer, or the bank, will *lose* money, not gain it. For four and eight per cent, the sum of remainders is *zero*, so the "unscrupulous technologist" would steal *nothing*.

To keep the myth alive, more complex methods of rounding must be assumed. Parker explains one supposed method:[186]

The bank keeps a running total of remainders as follows: if truncating (say for .173) it adds the positive quantity .003 to the running

186. D. PARKER, *supra* note 52, at 114-17. Parker cites no authority for it, and it would appear that this technique is not used. The author has checked with the chief analyst in the headquarters of a major bank, and at his bank the interest algorithm adds .005 to the computed interest, whether needed or not, then truncates at the penny. The remainder is not carried to the next account, it is "thrown away," *i.e.*, the bank keeps it. The net effect is that the bank *loses* a slight amount, except for four and eight percent where the average remainder is zero. The analyst did not know if this algorithm is a banking industry standard, but the presumption is strong that it is the *de facto* standard. The amount that the bank loses is insignificant, except for five percent interest, and it is simply not worth the effort to program Parker's technique, nor is it worth the extra computer time to execute it. At 5-3/4% interst, the loss for five million accounts is $62.50. The technique suggested appears to be inventive imagination spurred by a strong desire to believe the round-off fraud.

total; if rounding up (say for .178) it adds the negative quantity (the complement actually) − .002 to the running total. The resulting accumulated remainder $\Sigma r$ is then used to control round-up or truncation for the next account. If $\Sigma r \geq 1$, the next account is rounded up, regardless of the interest computation, and $\Sigma r$ is docked accordingly. If $\Sigma r \leq -1$, the next account is truncated, regardless of the interest computation, and $\Sigma r$ is replenished accordingly. If $-1 < \Sigma r < 1$, rounding occurs in the grade school manner. Thus the bank is never more than a penny out of balance. The practical effect of this is that sometimes an extra penny is not paid to an account even if the interest computation indicates that it ought to be, and sometimes an account gets an "undeserved" penny. Table 3 illustrates the technique. The parentheses indicate negative quantities, and the slashes indicate round-up or round-down caused by $\Sigma r$. The interest rate used is 2.6%.

TABLE 3[187]

| Old Balance | New Balance | Rounded New Balance | Remainder | Accumulating Remainder |
|---|---|---|---|---|
| $ 15.86 | $ 16.27236 | $ 16.27 | $0.00236 | $ 0.00263 |
| 425.34 | 436.39884 | 436.40 | (0.00116) | 0.00120 |
| 221.75 | 227.51550 | 227.52 | (0.00450) | (0.00330) |
| 18.68 | 19.16568 | 19.17 | (0.00432) | (0.00762) |
| * 564.44 | 579.11544 | ~~579.12~~ | (0.00456) | (0.01218) |
| | | 579.11 | | (0.00218) |
| 61.31 | 62.90406 | 62.90 | 0.00406 | 0.00188 |
| 101.32 | 103.95432 | 103.95 | 0.00432 | 0.00620 |
| * 77.11 | 79.11486 | ~~79.11~~ | 0.00486 | 0.01106 |
| | | 79.12 | | 0.00106 |
| 457.12 | 469.00512 | 469.01 | (0.00488) | (0.00382) |
| 111.35 | 114.24510 | 114.25 | (0.00490) | (0.00872) |
| * 446.36 | 457.96536 | ~~457.97~~ | (0.00464) | (0.01336) |
| | | 457.96 | | (0.00336) |
| 88.68 | 90.98568 | 90.99 | (0.00432) | (0.00768) |
| * 14.44 | 14.81544 | ~~14.82~~ | (0.00456) | (0.01224) |
| | | 14.81 | | (0.00224) |
| 83.27 | 85.43502 | 85.44 | (0.00498) | (0.00722) |
| 127.49 | 130.80474 | 130.80 | 0.00474 | (0.00248) |
| 331.32 | 339.93432 | 339.93 | 0.00432 | 0.00184 |
| 37.11 | 38.07486 | 38.07 | 0.00486 | 0.00670 |
| * 111.31 | 114.20406 | ~~114.20~~ | 0.00406 | 0.01076 |
| | | 114.21 | | 0.00076 |
| $3,294.26 | Total | $3,379.91 | | |

Widely misunderstood is just what remainders the programmer steals. It would be too obvious, perhaps, if he simply truncated *all* accounts; for nobody would get a round-up penny, and an auditor sampling the accounts might wonder why. The fraud consists of

187. D. PARKER, *supra* note 52, at 115.

stealing the *positive* remainders (the truncated amounts). The effect is that many accounts will indeed be rounded up correctly, however, a number of accounts that should be rounded up will not because Σr will go to −1 more often. Also, the accumulated remainder will never go to +1, thus the scattered "undeserving" accounts will also not get an extra penny. Table 4 illustrates this theft.

TABLE 4[188]

| Old Balance | New Balance | Rounded New Balance | Remainder | Accumulating Remainder | Programmer's Remainder |
|---|---|---|---|---|---|
| $ 15.86 | $ 16.27236 | $ 16.27 | $0.00236 | $0.00000 | $ 0.00236 |
| 425.34 | 436.39884 | 436.40 | (0.00116) | (0.00116) | 0.00236 |
| 221.75 | 227.51550 | 227.52 | (0.00450) | (0.00566) | 0.00236 |
| 18.68 | 19.16568 | 19.17 | (0.00432) | (0.00998) | 0.00236 |
| * 564.44 | 579.11544 | ~~579.12~~ | (0.00456) | (0.01454) | 0.00236 |
| | | 579.11 | | (0.00454) | |
| 61.31 | 62.90406 | 62.90 | 0.00406 | (0.00454) | 0.00642 |
| 101.32 | 103.95432 | 103.95 | 0.00432 | (0.00454) | 0.01074 |
| 77.11 | 79.11486 | 79.11 | 0.00486 | (0.00454) | 0.01560 |
| 457.12 | 469.00512 | 469.01 | (0.00488) | (0.00942) | 0.01560 |
| * 111.35 | 114.24510 | ~~114.25~~ | (0.00490) | (0.01432) | 0.01560 |
| | | 114.24 | | (0.00432) | |
| 446.36 | 457.96536 | 457.97 | (0.00464) | (0.00896) | 0.01560 |
| * 88.68 | 90.98568 | ~~90.99~~ | (0.00432) | (0.01328) | 0.01560 |
| | | 90.98 | | (0.00328) | |
| 14.44 | 14.81544 | 14.82 | (0.00456) | (0.00784) | 0.01560 |
| * 83.27 | 85.43502 | ~~85.44~~ | (0.00498) | (0.01282) | 0.01560 |
| | | 85.43 | | (0.00282) | |
| 127.49 | 130.80474 | 130.80 | 0.00474 | (0.00282) | 0.02034 |
| 331.32 | 339.93432 | 339.93 | 0.00432 | (0.00282) | 0.02466 |
| 37.11 | 38.07486 | 38.07 | 0.00486 | (0.00282) | 0.02952 |
| * 111.31 | 114.20406 | ~~114.20~~ | 0.00406 | (0.00282) | 0.03358 |
| | | 114.23 | | 0.00076 | 0.00000 |
| $3,294.26 | Total | $3,379.91 | | | |

The "programmer's" remainder, r+ is accumulated until the end of the run, at which time, his program credits Σr+, rounded to the nearest penny, into his own account. All crossfoot totals will balance. The amount stolen per account is practically undetectable, unless one independently recomputes all interests. Donn Parker points out that the programmer steals only three cents (for his example), but if 180,000 accounts were processed, he might steal $300. Done four times a year (quarterly interest) for ten years, he could get $12,000. However, as shall be seen, Donn Parker's figures are improbable. Making reasonable assumptions, the amount that can be stolen is less than $9,000 over ten years for 180,000 accounts—and 180,000 accounts is an unlikely large number.

188. *Id.* at 116.

It appears to be a clever crime, and it is no wonder that it catches one's fancy. But it does have a serious practical problem, which is that it is impossible to deposit the accumulated positive remainders into the programmer's account without risk. The simple rule of banking is that no sum is credited or debited without a transaction code, and, except for interest payments, it must have supporting paper. Practically speaking, the programmer will most likely elect to post the deposit as an interest payment. A bank adjustment should require paper and counter-signatures. A customer deposit requires supporting documentation, and the summary reports would reveal a discrepancy between the total of deposits received and the total of deposits credited.

Thus, if the programmer is practically minded, he will not use adjustment or customer deposit to mask his deposit. That would require considerable forgery in the transaction logs, and even collusion if it is to have a chance of succeeding. Even so, there will be an unavoidable discrepancy of timing; the timestamp of the credit will precede the timestamp of the forged transaction entry. Thus, the simplest and most natural transaction for the programmer to use is interest payment. After all, it is the interest run that posts the amount.

But now, there is a clear and obvious discrepancy; the interest posted does not agree with the previous balance. If anybody looks, the programmer is caught. Parker, of course, argues that in a large number of accounts, it is not likely that anybody will look. If the auditor samples one thousand accounts out of 180,000, the programmer has pretty good odds (180:1) against being detected. But, his account is looked at to some extent when he withdraws the money or closes the account. That is an unavoidable risk if he wants to realize his gain. The teller just might scan his most recent transactions. If the bank is using an on-line system, it is an excellent time for automatic verification of his account. Of course, banks may not do this; as it happens, bankers are secretive about their practices, especially their internal audit procedures. The point is not that the programmer certainly will be caught (though that is probably the case) but that he certainly runs a risk. He has an inexplicable, and obviously wrong, amount in his account.

Apart from risk, it is clear that it *is* mathematically possible for the programmer to steal money in this fashion. But the question is, how much? The stock answer is a considerable amount if carried out with a large number of accounts over a period of time. But one can be more specific and compute the amount to within a few cents.

If the programmer steals only mills per transaction and he steals a considerable amount, and a considerable amount in orders of magnitude greater than each theft, then an even larger magnitude

of transactions is required. The universe, the totality of transactions, though large, is clearly finite. Of that universe, a programmer has access to a vastly smaller subset. It is extremely unlikely that any one programmer can ever have access to enough transactions, which in this case are interest computations, to be able to steal a considerable amount.

The following will determine how much can be stolen per transaction, and then, knowing that, will compute the number of transactions required to steal any given amount. Finally, the number of transactions available to a programmer can be estimated, and a rough calculation can be made as to how much he can steal.

Determining the average amount stolen per transaction is a matter of brute force computation for each of the interest rates extant for the last thirty years. These range by 1/4 from 3 to 7-3/4%.[189] Higher interest rates are very recent and therefore can be ignored. For integer interests (3,4,..,7) one can compute interests on all possible pennies from .00 to .99. This assumes equal distribution of pennies over all accounts, and there is no reason to suspect any other kind of distribution.

TABLE 5

Remainder totals per account at extant interest rates

| interest | average round down remainder $\Sigma r+$ | average round up remainder $\Sigma r-$ | average remainder, no rounding $\Sigma r$ |
|---|---|---|---|
| 0.03 | 0.001225 | −0.001275 | 0.00495 |
| 0.0325 | 0.00124375 | −0.00125625 | 0.0049875 |
| 0.035 | 0.0012375 | −0.0012625 | 0.004975 |
| 0.0375 | 0.00121875 | −0.00128125 | 0.0049375 |
| 0.04 | 0.001248 | −0.001248 | 0.0048 |
| 0.0425 | 0.00124375 | −0.00125625 | 0.0049875 |
| 0.045 | 0.0012375 | −0.0012625 | 0.004975 |
| 0.0475 | 0.00124375 | −0.00125625 | 0.0049875 |
| 0.05 | 0.001125 | −0.001375 | 0.00475 |
| 0.0525 | 0.00124375 | −0.00125625 | 0.0049875 |
| 0.055 | 0.0012375 | −0.0012625 | 0.004975 |
| 0.0575 | 0.00124375 | −0.00125625 | 0.0049875 |
| 0.06 | 0.0012 | −0.0013 | 0.0049 |
| 0.0625 | 0.00109375 | −0.00140625 | 0.0046875 |
| 0.065 | 0.0012375 | −0.0012625 | 0.004975 |
| 0.0675 | 0.00124375 | −0.00125625 | 0.0049875 |
| 0.07 | 0.001225 | −0.001275 | 0.00495 |
| 0.0725 | 0.00124375 | −0.00125625 | 0.0049875 |
| 0.075 | 0.0011875 | −0.0013125 | 0.004875 |
| 0.0775 | 0.00124375 | −0.00125625 | 0.0049875 |

189. Maximum Interest Rates Payable on Time and Savings Deposits, Statistical Abstract of the United States (various years). Retrospective rates are also published occasionally in the Federal Reserve Bulletin.

Note that for integer interests, only the pennies count—the dollars do not affect the mills or fractions of mills in any way. Similarly, for interests of 3-1/2, 4-1/2, etc., one can compute all interests on amounts ranging from 0.00 to 9.99. Here, the dollars are included, since they do affect the mills. And so on. For each interest, you can sum the positive remainders, that is, all remainders less than 5 mills, and divide by the number of "accounts" to get the average. By the law of large numbers, this average will be close to reality. The results are set forth in Table 5. In case banks use the simple grade school method, or merely truncate, the average of the negative remainders (what the bank gives away rounding up) and the average remainder for no rounding (the bank, or the programmer, keeps all remainders) are also included. The round-up remainder is the average of the .01 complement of all remainders of five mills or greater. The algebraic sum of the round-down and the round-up remainders is the bank's average loss if it does not use accumulated remainders to determinate rounding.

As can be seen, the interest rate does not greatly affect the average stolen per transaction; it really does no more than add precision, not significance, and therefore, it can be ignored. Using four percent as the nominal interest, .001248 is the nominal average stolen. This is not so arbitrary; four percent is the most prevalent interest since computers have been widely employed. And the error for any other interest rate is negligible. The bottom line is that a little more than 1-1/4 mills is the average stolen per transactions. Using this nominal remainder against random figures works out very close—no more than a few pennies in error for one thousand accounts.

Based upon the foregoing, it is possible to compute exactly how many transactions are required to steal the amounts of $110,000, $200,000 and 480,000 DM cited in *Economic Losses* and the SRI Study. They are respectively

88,141,026 160,256,411 384,615,385

There are difficulties already for our larcenous programmer. Except for the first figure, these figures exceed the total of savings accounts, including time deposits, for all commercial banks in the United States, and the last may exceed the number of savings accounts in the free world. As of June 1975, there were 96,103,310 commercial savings accounts in the United States, plus an additional 35,034,733 time deposits.[190] Of course, this is not the totality of interest accounts, since it includes only individual, partnership, and cor-

190. Federal Deposit Ins. Corp., Summary of Accounts and Deposits in All Commercial and Mutual Savings Banks, National Summary 22 (table 1-1) (June 30, 1975) [hereinafter cited as Summary of Accounts].

porate deposits in commercial banks, and not public deposits (government), credit unions, etc. It is, however, the largest subset of accounts, and the larcenous programmer had or has access to far less than this subtotal. In other words, the figure 96.1 million (just the savings deposits) is a ridiculous upper bound.

Although these figures are based upon the generous assumption that the larcenous programmer has access to both savings and time deposits, in practice this would be unlikely. Time deposits are usually segregated from savings, and banks use entirely different programs to compute interest on these two types of accounts because of the difference in interest methods between them.[191]

Attempting to estimate the number of accounts to which a programmer has access, for the 131,138,043 (savings plus time) accounts there are 14,331 banks in the country.[192] This figure has been rather stable for the past forty years—what has increased is the total number of branches. This makes an average of 9,150 accounts per bank. For about ninety-eight percent of the banks, this is an excellent upper bound.

The following calculations will assume that interest is computed quarterly. It is true that some financial institutions compound interest daily, in which case, the interest per account is in fact computed 365 times in a year. But this can be ignored, since it means that $.45 = 365 × .001248 is stolen from *every* account on the average per year, and that much would in all likelihood be noticed. If the customers receive quarterly statements, which is the usual case, at least one out of 9,150 should notice that he is eleven cents short and complain; and if not, the auditors most certainly would. Federal auditors do indeed verify that the interest advertised is the interest paid.[193] The following also ignores interest computed monthly; it just multiplies results by three, which hardly matters, and the largest banks do not pay monthly interest anyway.[194]

It also ignores credit unions because they have small numbers of accounts and a peculiar way of computing interest that for four percent just does not leave *any* remainders to steal. They ignore pennies and pay interest only on even five dollar shares. However

191. Actual practice is inferred from the software section of DATAPRO REPORTS. Programs for passbook (savings) accounts are described separately from those for certificate of deposit (time) accounts.

192. Summary of Accounts, *supra* note 190.

193. Personal communication with Vince Dougherty, Federal Deposit Ins. Corp.

194. In general, the largest banks pay the least interest with the more unfavorable (for the customer) interest computation methods. *See How to Pick the Best Savings Account*, CONSUMER REPORT, Feb. 1975, especially the section entitled "Big Banks Can Be Stingy," at 92.

the interested reader may compute this for fractional interests knowing that a medium size credit union has about 5,000 accounts and a very large one about 30,000.

Thus, in short, for the average bank holding, the larcenous programmer can steal

$$\$45.68 = 9150 \times .001248 \times 4$$

per year. Donn Parker asks in a paroxysm of rhetoric "[h]ow many programmers have retired to a life of leisure as their programs . . . pump the pennies into their accounts at nearly the speed of light?"[195]

The mean of 9,150 accounts is an excellent upper bound for the overwhelming majority of banks. The distribution of accounts among all banks is not even; it appears to be a pulse contained below 9,150, and odd perturbations extending out far beyond 9,150. If the distribution were even, then fifty percent of the banks would have more than 9,150 savings and time deposits, and fifty percent would have less. This is not the case. The largest 145 banks (one percent of the banks) hold 46.77% of all deposits (demand, savings, time and government). Approximately two hundred banks hold half of all deposits. Cumulative holdings, as a percentage of the total are as follows[196]:

| Banks | Percentage of total |
|---|---|
| 1 | 4.21 |
| 3 | 9.86 |
| 5 | 13.73 |
| 10 | 20.12 |
| 14 | 23.75 |
| 72 | 38.67 |
| 100 | 42.24 |
| 145 | 46.77 |

If these cumulative figures are plotted, one obtains a steep rising curve that levels off into a gradual linear curve at about 250 to 300 banks. This, of course, is by estimation. It means that about 14,000 banks, more or less, equally share less than half the total deposits. If one knew what the 300th largest bank actually held in savings and time deposits, one would have the upper bound for 98% of all banks. The FDIC has this information, but it is not available to the public—it is specifically excluded from the Freedom of Information Act. However, understanding the distribution even in this limited way, it is clear that about ninety-eight percent of the banks

195. D. PARKER, *supra* note 52, at 117.

196. Summary of Accounts, *supra* note 170, at 15 (table I).

actually hold less than the mean of 9,150 accounts. Therefore, for 14,000 banks, it is impossible to steal more than $45.68 per year by means of Parker's round-off fraud. Thus, for ninety-eight percent of all banks, at least 2,408 years would be required to steal $110,000, and 4,378 years to steal $200,000. If German banks are at all comparable in account distribution, it would require 10,507 years to steal 480,000 DM.

Remaining for consideration is the maximum amount that can be stolen from the two percent of all banks with over 9,150 accounts. Exact figures are unobtainable, but the FDIC did provide the savings and time deposit holdings for three unidentified banks which are among the ten largest in the country. One figure is from the few (two or three perhaps) that are the largest of the largest ten. One figure is from the few that are in the midrange of the largest ten. And the last is from the few that are the smallest of the largest ten. These figures are[197]:

| | Top few of ten | Mid few of ten | Last few of ten |
|---|---|---|---|
| Savings | 4,098,952 | 736,545 | 492,430 |
| Time | 955,639 | 347,249 | 120,606 |
| Total | 5,054,591 | 1,083,794 | 613,036 |

Using quarterly interests and the nominal remainder .001248, the amount that can be stolen per year by the round-off fraud from each of these banks is

| | Number of Accounts | Total Possible |
|---|---|---|
| Top few | 5,054,591 | $25,232.51 |
| Mid few | 1,083,794 | $ 5,410.29 |
| Last few | 613,036 | 3,060.27 |

In other words, in theory, about three programmers in the entire country could steal $25,000 per year, about three more $5,400, and about three more $3,000. Strictly as a guess, about another one hundred could steal between $1,000 to $3,000 per year, providing that Parker's round off method was used.

To steal the quoted amounts from each of these banks would require:

197. Personal communication with Vince Dougherty, Fed. Deposit Ins. Corp. A major west coast bank is rumored to have about eight million accounts. As such, it would appear that the FDIC provided information for the second or third largest bank, and not the largest. However, this major bank uses two regional data processing centers, with the accounts split 60:40. Thus, 5,054,4591 is more than adequate as a maximum.

| Total theft | Years to accomplish for a bank holding | | |
|---|---|---|---|
| | 5,054,591 | 1,083,794 | 613,036 |
| 110,000 | 4.36 | 20.33 | 36 |
| 200,000 | 8 | 37 | 65.35 |
| 480,000 | 19 | 88.7 | 156.8 |

Note that for the largest banks, it would take nineteen years to steal $480,000, and because this is pure mathematics, not currency exchange rates, it would take just as long to steal 480,000 DM from the same size German bank. But, probably, no German bank has this many accounts. Remember, this loss was "reported" in 1971. Therefore, the theft would have to have begun before 1952. This was the era of vacuum tube and delay line computers, and even before these were commercially available. Clearly, this particular crime is impossible. It never happened, and SRI's reporting of this as a legitimate case is without justification.

By similar reasoning, the $200,000 theft could have occurred at only two or three banks in the world, and if so, must have begun about 1960 to 1962, since the case was reported in 1970. This time period was the era of second generation computers. IBM's 360 series did not appear on the market until about the end of 1964; it was announced in April, but the first customer shipment was about the end of the year. The odd fact is that the very largest banks were slow to computerize. There is an interesting letter in *Datamation* from Chase Manhattan explaining this delay.[198] Basically, the largest banks were well aware of the disruption that automating could cause, and proceeded very cautiously. The largest banks could least afford disruption exactly because of their volume. Chase Manhattan computerized checking in the late 1950s (approximately 1958-59), and did not computerize other applications until later—in the early 1960s. Timing here is close, but this crime may have begun a year or two before the bank automated savings accounts. In short, this case too appears to be nonsense. But since timing is close, assume that it did occur. Then for a few years, it operated on second generation computers and miraculously survived conversion to third generation computers.

This was the time of the six-tape installation. Old master tapes 1 and 2 occupied the first two tape drives, transaction tapes 1 and 2 occupied the next two drives, and new master tapes 1 and 2 the last two drives. The files were sequential, sorted in account number order. All processing was designed to avoid going to-and-fro in the tapes. Programs read a record but once from a tape (or card) file

198. Letter from Charles Block, Chase Manhattan Bank, *reprinted in* DATAMATION, Sept. 1965, at 13.

and wrote a record but once to tape. They did not pass the same spot on a tape twice in the same run. When old master tape 1 was exhausted, the program switched to old master tape 2 and unloaded old master 1. The processing time for tape 2 gave the operator enough time to replace tape 1 with old master tape 3. A similiar procedure was used for the transaction tapes and the new masters.

A necessary part of the round-off fraud is that the programmer's account is in the file. Also, for the maximum possible theft, the programmer's account must be the last record in the file. But the order of his account in the file is a function of his account number over which the programmer has no control. When he opened his account, the bank gave him a number from a block of available numbers, and it is impossible to know where his resulting tape record appears in the tape file.

The necessity in second generation systems to be the last record in the file for the round-off fraud to work has created some amusing myths. The programmer opens his account with an unlikely name like Zwana or Zzwicke. However, the order of his account in the file is not a function of his name, but of his account number, which the myth ignores. There are too many identical names to think of ordering a file by name. If a listing in name order was required, the master file would be sorted to produce the listing as needed. But the master file always remained in account number order.

Therefore, the programmer could steal mills only from those accounts that preceded his account in the master file. It is impossible to know how much this could amount to, but it is almost certain to be less than the theoretical maximum. Thus, it would take more than eight years to steal $200,000 at the largest bank using second generation equipment. The result again is that this crime would have had to begin before the bank even had a computer.

There remains one more possibility related to this theft on second generation equipment. Actually, tales of the round-off fraud are a little unimaginative. Why not, knowing the number of accounts, precompute how much can be stolen, just as we have done, and simply deposit that amount less a safety factor into the programmers account, regardless of where it is on the tape? Thus, the programmer deposits $25,222.51 in his account as soon as his program encounters it, and $10.00-e into the last account, whose ever it is. "e" is the actual difference between the precomputed amount and the accumulated remainder. The owner of the last account, which receives the unexpected bonus of ten dollars perhaps will not complain. This would appear to be a brilliant solution.

The problem is that the programmer must guarantee that he

does not steal more than the accumulated remainder, or else he will have to dock the last customer to make the crossfoot totals balance. While the last customer may not complain if he receives a bonus of ten dollars, he will scream if he is docked ten dollars. This means that the programmer must know the bank's future holdings. This can only be estimated, and to be good, the programmer must have a profound understanding of our economy. In short, he must be an economic analyst provided with all requisite data. This is unlikely, and if the number of savings accounts drops, as it has lately, he is caught. Also, if the last customer gets too much because the programmer's estimate is not valid, he may notify the bank of an error. The data that he needs, furthermore, is not in the public domain.

The reported theft of $200,000 is also nonsense. Only the projected theft of $110,000 looks possible, and only at the two or three largest banks because of the applicable time constraints—a twenty or thirty-six year period seems unreasonable on its face. However, these were projected thefts. Computer specialists, probably using Ouija boards, projected thirty-six of these crimes per year. But clearly only two or three of these thefts could occur, and they would take 4.36 years, not one year. It is impossible that there could even be one per year, let alone thirty-six.

Not much is left of this most famous of computer crimes. Some 14,000 programmers, if they cared to take the risk, could theoretically steal a maximum of $45 a year. For this, computer crime experts, and even senators, tremble in fear for the safety of America's corporate assets? The reader should not take 14,000 programmers seriously. Most banks purchase their interest calculating programs from a relative few banking software firms, often owned by other financial institutions. Thus, the number of programmers who code interest programs for specific banks is far less than fourteen thousand.

If the round-off fraud were indeed a problem for financial institutions, it would be easy to prevent. There is no law requiring banks to round up; some do not. Indeed, a few rural banks with no competition do not even pay interest. The bank merely has to truncate *all* accounts—no rounding up at all—accumulate the remainders for itself, and at the end of the run, deposit the remainders in its very own account. The bank can figure to a farthing how much it should get.

The round-off fraud is a fool's crime. There is no evidence that it has ever happened, not even in small amounts where it is mathematically possible. According to Donn Parker, experienced account-

ants and auditors claim that it would never work because their procedures would detect it.

Programmers believe the round-off fraud because, while they understand computation and remainders very well, they know nothing about banking. However, programmers in banking do not believe it; they say that it is possible only for banks that compound interest daily, not realizing that it is impossible— especially there.

The round-off fraud is an old story, known long before computers. It may be as old as banking itself. In medieval Italy, poorly paid gold workers supposedly stole from their masters by rubbing gold dust in their flaxen hair. Why didn't the masters insist on baldheaded or brunette workers? The answer is, the story is a myth. Such myths do two things; they appeal to our wishful thinking, and they express a guilt-ridden fear. Interest, in the Middle Ages, was usury, condemned by the Church. The prohibition goes back to biblical times—the Jews were forbidden by the Law of Moses to lend money for interest among themselves "lest ye enslave your brothers." To this day, there is a minor, but strong feeling against interest. Pound excoriated it:

> With usura hath no man a house of good stone each block cut smooth and well fitting that design might cover their face . . . .[199]

Pound goes on at length (he has that tendency) to conclude emphatically

> CONTRA NATURAM
>
> They (ie the bankers) have brought whores for Eleusis
> Corpses are set to banquet
> at behest of usura . . . .[200]

Pound means by *usura* not *excessive* interest, but any interest, in the same sense as the Church. Many states have usury laws on their books, largely unenforced and being revoked one by one, but attempts nevertheless to limit evil. Political struggle engendered by popular suspicion of banking is a fascinating thread throughout American history. The ancestors of our own bankers were doing, for the ethics of their time, an evil well known to be a wrong. Since the Protestant revolt, which among its religious reforms sanctified bourgeois business practices, interest has at least been legal.

Today, of course, interest is well established and no banker would feel guilty about it, regardless of Ezra Pound. But this was not so for the medieval banker. He gained money wrongfully and in his guilt must have feared that his employees were paying him in kind. In the pathological form of this suspicion, the banker refuses

---

199. E. POUND, CANTO XLV.
200. *Id.*

to believe all evidence to the contrary. If there is no visible theft, that is only because the theft is fiendish—it is invisible. The round-off fraud is exactly the invisible theft.

It is a myth.