COMPUTER-RELATED FRAUD IN GOVERNMENT AGENCIES :

PERPETRATOR INTERVIEWS

Department of Health and Human Services

Richard P. Kusserow

Inspector General

MAY 1985

EXECUTIVE SUMMARY

The President's Council on Integrity and Efficiency directed the Inspector General of the U.S. Department of Health and Human Services to follow-up on its 1983 study, "Computer-Related Fraud and Abuse in Government Agencies," by interviewing the perpetrators of computer-related fraud cases. Staff from HHS/OIG interviewed 46 perpetrators regarding how and why they committed their crimes. Although not a statistically valid sample, those interviews provide the following information on computer-related fraud among government agencies.

- The perpetrators were insiders, i.e., they were Federal employees, or employees of state, local, and private agencies administering Federal programs. In general they were young, good employees with an average of 5 years employment with the agency. Most had above average performance ratings, and most had been promoted at least once. Just over one-fifth had a prior criminal record.

- They held a wide variety of positions within the agencies ranging from a senior program manager to an entry level clerk. The more common positions were caseworkers, clericals, and data entry technicians. Most were in a position to cause checks to be issued, although many did not have direct access to the computer.

- Typically, the perpetrators committed their crime by manipulating input data to cause funds to be issued, and most were aided by co-conspirators. They generally used one of three schemes: modifying existing cases in a benefit or payroll system; creating false cases in those systems; or creating false claims in a reimbursement system. Many destroyed the paper or electronic evidence of their crimes.

- On the average, the period of criminal activity took place over six months. The number of illegal transactions per case ranged from 1 to 200 with a median of 8. The reported average loss per case was $45,000, but about one-fifth of the cases exceeded $100,000.

- Three-quarters of the perpetrators reported that they stole money in response to a situational stress. Most commonly it was a personal financial problem or disgruntlement with the job. Others, not motivated by stress, had discovered vulnerabilities in the system and could not resist that temptation.

- Nearly half reported that they didn't even think about the consequences of their actions when they committed the crime; others assessed the risks of getting caught as minimal. Many reported that they were personally aware of crimes like theirs or had heard of such crimes.

- Most perpetrators were aware of computer security controls but assessed them as weak. They described ID numbers and passwords as simplistic, edits and screens as known and therefore avoidable, and supervision as lax or naive regarding automated systems. They pointed out that access to or within computer systems was often not restricted. The perpetrators also made a number of recommendations on how to strengthen government computer systems.

In order to address the vulnerabilities noted in this study, it is recommended that:

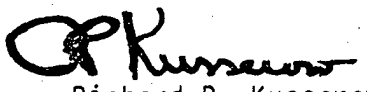
- computer fraud perpetrators be routinely debriefed;
- automated system controls be strengthened;
- security and system control guidance to State, local, and private agencies be reevaluated;
- line managers receive training on internal and system controls; and
- personnel security procedures be reviewed.

ACKNOWLEDGEMENT

This report represents another step forward in our effort to better understand computer-related fraud in government agencies. But this step could not have been taken without the support of others both within and outside of the Inspector General community. I want to recognize the efforts of staff from IG offices who reviewed their files to identify new cases and to provide locating information on old ones. The Department of Justice's Bureau of Prisons and the Probation Division within the Administrative Offices of the U.S. Courts provided valuable assistance in locating perpetrators and setting-up interviews.

I would also like to acknowledge the help of the 46 perpetrators who voluntarily met with us during the study to discuss "their side of the story." This report could never have been written without their cooperation.

Finally, I would like to thank the members of my staff - Jack Molnar, Project Manager, Gail Shelton, Jane Tebbutt, Lois Terry, and Denise Washington - for their many efforts in support of this project.



Richard P. Kusserow
Inspector General
U.S. Department of
Health & Human Services

TABLE OF CONTENTS

INTRODUCTION

In 1982, the President's Council on Integrity and Efficiency (PCIE), concerned about the apparently growing incidence of computer-related fraud and abuse, commissioned the Inspector General of the Department of Health and Human Services (HHS/IG) to study the problem. PCIE's charge was to provide a perspective on the nature and scope of computer-related fraud and abuse and on what the IG community should do to upgrade its audit and investigative skills and activities to deal with the problem.

In response, the HHS/IG surveyed the Federal agencies to gather all cases of computer-related fraud and abuse identified from the period January 1978 through March 1982. That survey obtained 172 cases (69 fraud and 103 abuse) which were analyzed for perpetrator characteristics, techniques of perpetration, losses, methods of detection, and controls. The June 1983 report of this study, "Computer-Related Fraud and Abuse in Government Agencies," included the following findings:

- Fraud cases primarily involved theft of cash or diversion of assets, usually through input manipulation in benefit or payroll systems. Most abuse cases involved use of computer time for outside business or entertainment.

- Most perpetrators were Federal, nonsupervisory employees. Four out of five of the fraud perpetrators earned $20,000 per year or less. Two-thirds of the fraud perpetrators were functional users of the computer system, rather than data processing personnel.

- Confirmed losses ranged up to $177,383 per case, although actual losses were thought to be higher in many cases.

- Operating personnel found over half of the frauds and over two-thirds of the abuses. More importantly, half of the cases were detected by accident, which was twice the incidence of detection by either controls or audits/reviews.

The report recommended that the IG community upgrade its expertise through computer training and awareness programs, and also that controls in automated systems be given especially close scrutiny. Because the survey responses were incomplete in some areas, the PCIE felt that more study was called for. Specifics about the controls in the environment of the victimized systems were thought to be a particularly vital area for further inquiry.

OBJECTIVE OF THE STUDY

The PCIE therefore asked the HHS/IG to expand upon the original study by interviewing the perpetrators identified in the original study. The objective was to determine what the perpetrators would tell us about their crimes and the vulnerabilities in government computer systems. Specific study questions included:

- Who were the perpetrators?
- What jobs did they have?
- How was the crime committed?
- Why was the crime committed?
- What was the work environment?

SCOPE AND METHODOLOGY

To accomplish this objective, we first had to identify perpetrators involved in the 69 computer-related fraud cases from the original study. That study, to preserve confidentiality and encourage cooperation, had not identified individual perpetrators, and therefore used only data descriptive of the crime. Upon our request for identifying and locating information for each perpetrator, the agencies were able to identify perpetrators from 60 of the original 69 cases.

Because most of the crimes had been committed over three years earlier, much of the locating information was no longer correct. In addition to using traditional field work techniques to locate the perpetrators, we were assisted by two other agencies: the Bureau of Prisons at the Department of Justice located those who were in Federal Correctional Institutions or in pre-release programs; and the Division of Probation in the Administrative Office of the United States Courts assisted by locating perpetrators under the supervision of Federal Probation Officers. Overall, we were able to locate perpetrators for 39 of the original cases. The primary reason for failing to get such locating information on the others was that many of the case files had been archived. This was particularly true of Department of Defense cases where the perpetrator had been discharged from military service.

We were able to interview 29 perpetrators from 21 of the original cases. We were unable to interview the others because perpetrators in 9 cases were not prosecuted, 7 perpetrators refused to be interviewed, and 2 cases were still open.

Because more cases had occurred since the original study two years earlier, we requested that IGs identify all computer-related fraud cases occurring after the original request for cases. That request yielded 18 additional perpetrators of which we interviewed 17 (one refused). We were able to interview three of these newer cases during their pre-sentencing period.

In total, we interviewed 46 perpetrators (29 original and 17 new) who were involved in 39 cases of computer-related fraud. These cases involved seven Federal agencies.

Department of Agriculture
Department of Defense
Department of Health and Human Services
Department of Justice
Department of Labor
Department of the Treasury
Veterans Administration

The findings of this study are based largely on discussions with these 46 perpetrators. In addition to the data gathered during the discussions, other sources of information, such as case files, FBI "rap" sheets, and the survey questionnaires from the original study, were used in the analysis. The 46 discussions do not represent a statistically valid sample of government computer-related fraud cases. They represent the voluntary comments of perpetrators identified for this study, and are presented to add new insights to our understanding of this relatively new type of crime.

I. Who Were The Perpetrators?

> When I got out of the Navy I was job hopping. I took the PACE test to find a secure government job and was hired as a casework representative. I was promoted and knew I had a career. A FEDERAL CASEWORKER

Perpetrators Were Employees, Not Outsiders

Persons using computers to defraud the government could be anywhere given today's technology. However, as was found in the original study, virtually all perpetrators were employees of an agency administering a Federal program. With virtually all of the computer-related frauds being committed by employees, two related points can be made: (1) since none of the perpetrators who had gained access to the government computer system was from outside the agency, none was a beneficiary, client, or hacker; (2) all of the perpetrators were authorized users, i.e., it was a necessary part of their job either to query, enter, or modify data in the computer system or to direct the operation of the computer system.

Just over half of the perpetrators were Federal employees, while the remaining employees represented State (16 percent), local (16 percent), and private (12 percent) agencies. The private sector employees were under contract to a government agency to administer a Federal program or manage an automated system; all acted independently, rather than as part of a corporate scheme. It should be noted however that many of the perpetrators had co-conspirators who were not employees, but none of those personnel gained direct access to the computer (discussion of co-conspirators in Section III).

The one perpetrator who was not an agency employee was a health care provider. A terminal was placed at his facility by the fiscal intermediary to expedite the submission of State Medicaid claims.

Perpetrators Were Young, Good Employees

In general the perpetrators appeared to be the younger employees of the agency. While those contacted during the study ranged in age from 20 to 50, their median age was 30 at the time they committed the crime. In comparison, the average age of Federal employees is about 40.

Three-quarters of the perpetrators told us that they had attended college. A third of those attained at least a bachelor's degree, with some doing post graduate work. The other two-thirds reported spending between one and four years in college, with some attaining an associate degree. Even among those who did not attend college, many had attended classes in business or computer academies.

During our meeting with the perpetrators, we asked them about their job performance ratings. In general, they reported that they were good employees; only two noted unsatisfactory performance appraisals. Two-thirds noted that they had received above average, excellent, or outstanding ratings and one-third reported that they got average or satisfactory performance evaluations. It was not uncommon for the perpetrator to be considered one of the better employees in the office -- the one to whom other employees went to with problems. Many were also "students of the computer system," and were called upon to assist others. Additionally, a quarter of the perpetrators told us that they had received awards for their performance. Ironically, four of those award recipients received their award for designing or implementing the computer system they ultimately stole from. For example, a programmer with a Federal agency working on a payroll system got a cash award in 1981 when he set up the electronic funds transfer for his agency's payroll system. In 1982, he used that same system to steal to support his cocaine habit.

Another indicator of the perpetrators' success with the agencies, is the fact that about three-quarters had been promoted or advanced in job responsibilities while at the agency.

Based upon our discussions with the perpetrators, it appeared that most of them had sought out permanent, government employment. For example, for a third of the perpetrators this was the job they sought after getting out of school. For another third, they had consciously sought out a permanent, government job after having worked elsewhere.

Although they were among the younger employees of the agencies, the computer-related fraud perpetrators had spent an average of over five years with the agency before they began to commit the crime. Time on the job before the crime ranged from one year to 20 years, and varied by type of employer. While Federal employees had been with their agency for an average of six and a half years when they committed their crime, this figure dropped to five years for State employees and three for employees of local public agencies.

Some Had Criminal Records

One of the most surprising findings that resulted from our discussions with the perpetrators was that almost one-quarter of them had prior criminal records when they were hired by a government agency. While a few admitted that they had hidden that fact from their employer, others reported that they were hired under special programs for ex-felons or that their employment was an acknowledged condition of their probation. The earlier crimes of the perpetrators ranged from rape and armed robbery to white collar crimes of embezzlement and forgery. For some, the computer-related fraud was their second crime, but for others, it was but one in a series of criminal activities. It is also noteworthy that while 18 percent of the Federal employee perpetrators had previous criminal records, this figure was as high as 43 percent for State and local employees. None of the private employees had a former criminal record.

Time on the job before the fraud was committed varied between those with a criminal record and those without one. For example, only 14 percent of those without criminal records committed their computer-related fraud within one year of being hired, as compared to 40 percent of those with a criminal record. Similarly, the median length of employment with the victimized agency for ex-offenders was only 3 years, in contrast to 6 years for those without a criminal record. And, two-thirds of the ex-offenders were in the specific job from which they committed the crime for less than one year, compared to only one-third of those without prior records. Apparently the opportunity to commit fraud was seized more quickly by those with prior records. Carla and James are two such perpetrators.

When we talked to Carla it was in a Federal prison. This was her third time in jail. In the early 1970's, she was sentenced to 3 years in a State prison for forgery and was later convicted of welfare fraud in the mid-1970's. In fact, she was on probation for welfare fraud when she was hired by a county welfare agency as a clerk-typist in their data center. An A.A. degree in accounting, hard work, and good evaluations won her a data center supervisory position within one year.

At about this time, she met James, a data input technician working on the same program. James had been hired under a special program for ex-offenders. He had been arrested and convicted at least five times in the six years prior to being hired. The charges included theft of government property, credit card theft, forgery (27 counts) and fire arms violations. During our interview, he readily admitted that he was a career criminal. During his first year on the job, he too had been promoted, but he also acquired a drug addiction that could not be financed by his $10,000 per year salary.

Together, James and Carla developed a plan to steal to support his drug habit and supplement her salary. Four months, fifty cases, and $120,000 later they were caught by a computer match.

II. What Jobs Did They Have?

I didn't need to sit at a terminal to do my job. I just filled out forms. In keypunching, they never check anything. They just entered what was on the form. A FEDERAL VOUCHER CLERK

Perpetrators Had A Broad Range Of Jobs

The perpetrators held a wide variety of jobs at the time they committed the crime. The positions ranged from secretaries to senior program managers and from entry level clerks to highly trained systems analysts.

The most commonly occupied job type (35 percent) was that of caseworker. This is a relatively discreet group of employees in entitlement programs who determine eligibility and the amount of the payments to be made to program beneficiaries. Most of these employees met directly with the public, but some made decisions based upon the case files. None were in supervisory positions. (See Table A).

The next most frequently held job type (28 percent) was that of computer support or technical personnel. These are both professional and support staff whose raison d'etre was the computer system itself. About half could best be characterized as data entry technicians, i.e., non-supervisory employees, who sat at video terminals and entered data into the system. More often than not they made no evaluation of or decision on the data; they just entered it. The remaining technicians were more involved with the overall operation of the computer. Three were computer professionals who either designed and wrote programs, or supervised the operation of large management information systems. The others were support personnel working in the data center doing such things as loading decks of cards, hanging tapes, or managing the hard copy output.

The third most common position (26 percent) was held by persons with clerical titles. This category included employees whose primary responsibility was to review and process paper, such as case files, payroll forms, or vouchers and bills for goods or services rendered to the agency. As a normal part of their job they were functional users of the computer, but they would not spend all of their time at a terminal.

Of the remaining five perpetrators, four were line managers heading up major management information systems or financial operations, and one was a health care provider.

TABLE A: PERPETRATOR JOBS

JOB	TOTAL #	% SUPERVISORS	% WITH DIRECT COMPUTER ACCESS
CASEWORKER	16	0%	12%
TECHNICIAN	13	38%	100%
CLERK	12	1%	67%
OTHER	5	100%	80%
TOTAL	46	24%	59%

Direct Computer Access Not Universal

In order to perform their jobs, all the perpetrators needed to modify data in the system or have access to the computer itself. However, not all actually sat at a terminal or worked on a computer. Just under half of the perpetrators performed their jobs through the creation of input documents away from the computer. (See Table A). These documents would occasionally be reviewed and then were submitted to technicians who would enter the data. This is particularly true for the caseworkers. Only 2 of the 16 caseworkers loaded data directly into the computer as a normal part of their job. However many caseworkers did have "query-only" access to the computer system to review the status of cases.

Typical of this are benefit program field offices where caseworkers have "query-only" computer terminals they can go to in order to review the status of specific cases. However, when they want to make a change in a case they must complete a form. That form is reviewed by one technician and submitted to another technician to be entered into the computer system.

Most Worked For Benefit Programs

Just over three-quarters of the perpetrators worked for benefit programs that issued funds, and were in a position to issue those funds. About half of these employees worked for federally administered entitlement programs such as Social Security or the Black Lung program. A third worked for State or locally administered grant programs such as Food Stamps or Unemployment Insurance. The remainder were employees of private companies managing financial transactions for the Medicaid or Medicare programs.

The remaining perpetrators worked in administrative or staff positions, most often in various parts of payroll operations.

III. How Were The Crimes Perpetrated?

> I brought the screen up with a phoney ID. I created a phoney beneficiary and a phoney claim using my mother's Social Security number. I just keyed it in. A PRIVATE AGENCY CLERK

Most Perpetrators Issued Funds

The 46 perpetrators interviewed for this study were involved in 39 different criminal cases. In four instances we interviewed two perpetrators per case and on one case we were able to reach four. Accordingly, the analysis of how the specific computer-related frauds were committed will be based upon 39 cases.

In 85 percent of the cases, the perpetrators caused negotiable financial instruments to be issued. Most frequently U.S. Treasury checks were issued, but checks were also caused to be issued against State agencies and private financial organizations. In addition to checks, a few cases involved Food Stamp coupon issuances. The Stamps were usually converted to cash at about 75 cents for a dollar's worth.

The cases that did not involve negotiable financial documents included:

1. restoration of annual leave;
2. modification of income tax deductions;
3. keeping funds returned to the agency;
4. sale of false ID cards; and
5. sale of information.

Virtually All Were "Data Diddlers"

"Data diddling" is a commonly used term to describe those computer crimes where an employee commits the crime by manipulating data before or during the input process, or during output from the computer system. Examples are: changing the name, address, or bank account of a beneficiary to that of the perpetrator or the perpetrator's co-conspirator; or erasing the history of a payment so that a duplicate check is issued.

Over 90 percent of the cases involved data diddling. This is consistent with the finding in the original study that most cases involved manipulation of data. Almost all the cases involved manipulating input to the data system, but a few involved the manipulation during both the input and output processes. These cases involved Food Stamp issuance, and output data manipulation was necessary to bypass controls, such as separation of duties, and to conceal the fact that illegal stamps were issued.

As noted earlier, not all of the perpetrators had direct access to the computer, nor did they require direct access to the computer system to commit their crimes. In fact, half of the cases of input manipulation were not committed with "hands on" access to a computer. In these instances the perpetrators, based upon their substantial knowledge of the system, were able to create documents that were later entered into the system by another person. When entered, they modified data in the system to cause the illegal transaction.

The three cases that would not be described as data diddling were all committed by computer experts. In one instance, data from a criminal justice information computer system was sold. The two other cases were technical computer crimes often referred to as "Trojan Horses" which occur when a person with programing expertise places a small, illegal computer program within a larger normal operating program. The small program is difficult to detect and generates the illegal transactions when the larger program is run.

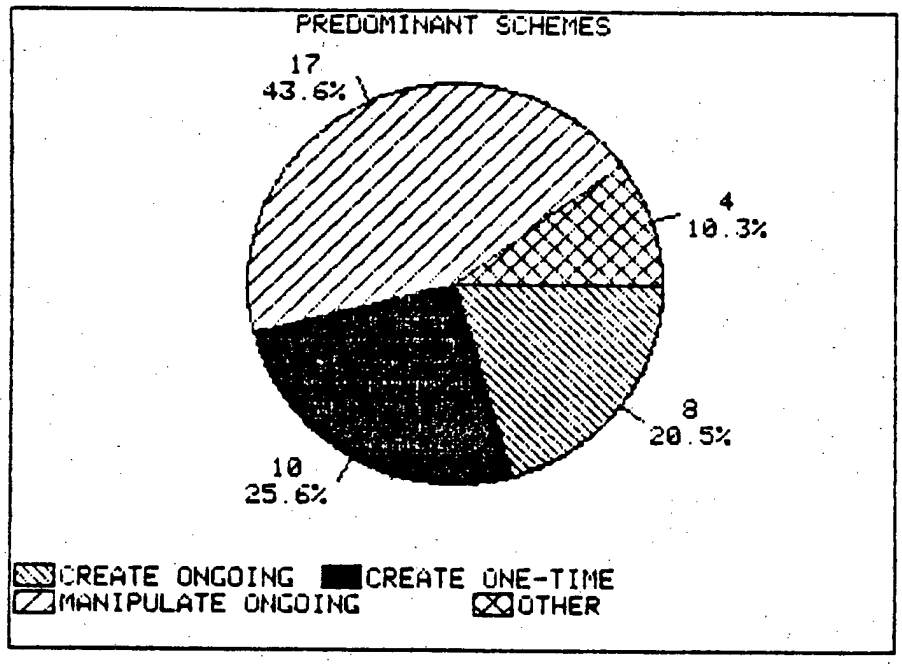
In one of these cases, the names and addresses of three friends of a Federal programmer were inserted in place of three employees in the agency's payroll. After the program was run, the sub-program was deleted so that the check went to the perpetrators' friends; but a review of the computer tape showed that checks were issued to the employees. The second "Trojan Horse" case was quite similar. A technical consultant from a private company working on a Federal benefit program caused his wife's name and address to be inserted in place of a beneficiary when the program to issue the entitlement check was run.

Three Schemes Predominate

The crimes committed by the perpetrators were dictated by the purpose of the computer system on which the perpetrator worked, and in virtually all cases involved the manipulation of data in either on-going payment systems or one-time payment systems. On-going payment schemes occur on benefit program systems where a person or family is eligible for a specific benefit such as Social Security, unemployment insurance, or a paycheck.

Once eligibility is established, funds are issued on a regular basis. One-time payment schemes occur on financial systems designed to issue funds to a vendor, provider, or beneficiary in response to a specific bill or voucher for goods or services. With regard to data in these payment systems, perpetrators had two options. They could either create unauthorized files or records, or manipulate existing files or records. This leads us to the three predominant schemes used by the perpetrators that account for 35 of the 39 cases. (See Chart I).

Chart I:



The most common scheme, accounting for almost half of the crimes, was the manipulation of data on existing cases in an on-going payment system. This type of crime occurred in such programs as Social Security or other entitlement programs. In such instances, the beneficiary already existed in the program data base as a valid case. Then, seizing upon an opportunity when the beneficiary died or lost eligibility for example, the perpetrator redirected the check to himself or a co-conspirator. In other instances, perpetrators have caused duplicate payments to be issued to relatives who are valid cases on the system. A third way of taking advantage of existing cases was to identify and reactivate dormant cases and to have the benefits sent to a co-conspirator. The following is a common example of this scheme.

> Bill, a caseworker, got a notification that a beneficiary had died. Instead of terminating that person's eligibility, he went to a bank and opened up an account in that beneficiary's name (and Social Security number). He then simply completed an input form that changed the address so that the check would be sent to his bank via direct deposit. Bill then periodically drew money out of that account. Bill didn't have to do very much modification to the case file in the computer. All he did was change the routing of the check.

With the second scheme, the perpetrators created false claims in a one-time payment systems and had the payments go to co-conspirators. This accounted for about a quarter of the cases. Most frequently they authorized a payment to a co-conspirator for bogus bills such as would be received on a purchase order or for reimbursement to beneficiaries for medical services. For example:

> Tom was a voucher examiner. His job was to review bills for completeness and then give them to data entry technicians to be loaded into the system so that a payment could be made. One day Tom started submitting bogus bills to the technicians. They were just like real bills from doctors and physical therapists because there was MD or PT after every name. That was one of the edits in the system. However, the names and addresses were not real medical professionals, they were Tom's friends. Over 18 months they stole $250,000.

In the third common scheme, false records were created and added to files in on-going payment programs. This was more difficult to accomplish than other schemes because of the documentation required to establish eligibility. In some of these cases the perpetrator used the identity of co-conspirators, while others went through the process of creating false identities.

> Some employees used both versions of this scheme with a food stamp program. First they had friends come to the office and apply for food stamps. They needed real Social Security numbers and matching names because that was a control in the system. Once they had the real name and number, they put false income data on the application and their friends become eligible for benefits.
>
> Then when the Cuban and Haitian boat lift people began arriving, the eligibility system broke down. The newcomers become eligible for benefits but didn't have Social Security numbers. In order to by-pass the Social Security number control, the program officials adopted a system of pseudo-Social Security numbers, that could be issued in each office. The perpetrators didn't need their friends' names or numbers now; they could just create false beneficiaries with pseudo-numbers. And they did.

In the schemes that involved on-going payment systems, it was not uncommon for the perpetrator to periodically terminate their illegal cases or claims. This was done to prevent detection. For example, cases were terminated to avoid a quality control audit of cases or a programmatic requirement for a periodic, face-to-face recertification of the case. Other perpetrators, would keep a bogus case going for only a specific number of months - usually 3 to 6.

It was also common, when creating or modifying a case in an entitlement program, for the perpetrator to initiate the periodic payments with a large payment. These payments are typical of adjustment in benefits caused by retroactive eligibility or accounting for previous underpayments. This was often not a separate act but was done by the perpetrator at the time the case was initially modified or created.

Most Took Steps To Cover Up Their Crime

As would be expected with a white collar crime, most of the perpetrators took specific steps to cover up their crime. In almost half of the cases the perpetrators destroyed the hardcopy evidence of their crime. This occurred most often when the perpetrator, such as a caseworker, did not have direct access to the computer. In such cases they would destroy the input document they had given to the input technician. But some perpetrators also had to destroy computer output evidence of their crime, such as printouts or alerts produced when their crime was picked up by a screen or edit in the system. A perpetrator who had worked for a Federal agency said, "At first I was really nervous. I had to put the case file in my brief case and walk out of the building. When I got home I burned it. When I did it and realized how easy it was, I knew how bad the system was."

A few perpetrators reported that they did not have to worry about destroying evidence of their crime. Instead they relied on virtually nonexistent filing systems or on routine, periodic destruction of hardcopy to cover up their crime for them. Some perpetrators also used the computer to cover up their crime. For example, they reported that they were able to delete the record of their illegal transaction from the system, or they relied on routine purging of transactions from the system to cover up the crime.

Most Used Co-conspirators

In the original study, the survey data indicated that most of the perpetrators (75 percent) acted alone. However, based upon interviews with the perpetrators we found that three-quarters of the computer-related fraud cases involved co-conspirators. Beyond the psychological value of providing moral support, co-conspirators served other specific needs. Most frequently the perpetrators used co-conspirators who were outside the agency. These persons were often used to provide a false ID and address and/or receive and cash checks. In some cases, fellow employees conspired in the crime. In such cases, this was usually necessary to bypass controls such as separation of duties. In only a few cases, did a perpetrator use both internal and external co-conspirators.

Most of those who did not use co-conspirators felt very strongly that this was the only way that they could commit the crime. One senior level manager summed it up for this group when he said, "I couldn't have done it if I had had to involve someone else." These perpetrators were generally older employees, and interestingly, 60 percent of those who had acted alone had received awards, compared to only 20 percent of those who used co-conspirators. All but one of the perpetrators with a former criminal record used co-conspirators.

Only a Few Had To Bypass ID and Password Controls

Almost half of the perpetrators told us that the computer systems did not require them to use an identification number and/or password to get data into the system to commit their crime. This occurred for two reasons. First, as already noted, many perpetrators didn't need direct access to the computer system to commit their crime. (However, some of these perpetrators did have to forge a supervisor's signature on the data entry document.) Secondly, some perpetrators worked on systems that simply did not require ID or password controls for each user. This situation would typically occur where a bank of terminals would be brought on line at the beginning of the day and shut down in the evening. During the day any number of staff would have access to the system.

In the remaining cases, nine perpetrators used their own ID and/or password to commit the crime, while only eleven had to make up or steal an ID number. Usually when perpetrators used their own ID/password it was on systems that did not record the users identification number with the transactions, so there was no permanent record of who made the data entry.

Those who needed another ID/password identification to commit their crime didn't seem to have too much difficulty getting it. Some just sat at the terminal during their free time and made up possible identifying combinations until they found a valid one. In two cases any three alpha characters would serve as an identifier and all the employees knew it. So it wasn't very difficult to get into the system in that office. In three other offices, the ID number was simply an employee's initials. In these cases the perpetrator just stole another worker's ID.

Frequency, Duration, and Loss Varied Greatly

The number of times the perpetrators committed their criminal act ranged from one to 200. This was dictated in part by the type of scheme they used. For example, if the perpetrator created or manipulated data in an entitlement program, that one criminal act would yield a monthly check as long as the perpetrator kept that case active. However, if the perpetrator created false bills in a voucher payment system that crime would usually yield only one check. To illustrate this fact, one perpetrator only made four unauthorized entries into a benefit program computer and got over $100,000. Another entered 55 false bills into a state bill payment system and only got $1,000. The median frequency for committing the criminal act was only eight times, which serves to demonstrate the potential efficiency of using a computer to commit a crime and how infrequently the perpetrators needed to exploit the vulnerabilities in the system.

The duration of the crime also affected the number of times the illegal act was committed. The time from when the first illegal act was committed until the perpetrator was caught, or voluntarily stopped prior to being caught, ranged from one month to 72 months. The median duration of the crimes was six months.

The reported amount of direct financial loss to the government agency ranged from no loss to $350,000. The average loss per case was $45,000. Eighteen percent of the cases involved losses greater than $100,000, which is somewhat higher than the 7 percent reported in the original study. There were two cases of no dollar loss. One was selling of information and the other was issuing false ID for immigration purposes. Although none of the perpetrators admitted to stealing more than had been identified in their case as submitted to the court, some implied during the interview that more was stolen.

IV. Why Did They Commit The Crime?

> I had personal problems because I was $20,000 in debt. But I had also worked my butt off for them and they passed me over for a promotion. I was good and deserved more. I decided to get back at them. A FEDERAL PROGRAM MANAGER

Perpetrators Stole Under Stress

Because eight perpetrators refused to admit committing a crime, we were not able to discuss their motives during the interview. Consequently, analysis of motives is based upon 38 discussions. Three-quarters of the perpetrators reported that they were responding to or were influenced by a specific situational stress when they committed their crime. Most of these perpetrators stole money because of a specific family problem such as medical bills, potential eviction or loss of a home, or loss of spousal income. Others reported that specific debts caused them to steal, and a few said they stole to support a drug habit.

Still others in this group reported that their primary reason for committing their crime was because they were disgruntled. Some were mad at the organization, while others were seeking revenge on an immediate supervisor. A systems analyst for a private company confided: "I had given my soul to that company and I got burned. That company ended up being my life and I got caught in the stigma of this lousy contract with the government. They wouldn't transfer me out. I had to show them." Furthermore, a third of those who stole because of a specific personal problem noted that they were also unhappy employees and that fact made it easier for them to commit their crime.

Although most perpetrators started stealing to meet a specific need or in response to other stresses, few voluntarily stopped once that need was met. Only one in six of the perpetrators voluntarily stopped.

Temptation and Boredom Influenced Others

A quarter of the perpetrators reported committing their crime because an opportunity presented itself rather than because of some driving problem. In some cases it was a specific event such as funds being returned to the office, or the accidental discovery of a vulnerable procedure in the system. However, for others it was the result of boredom or free time. In such instances the perpetrator, often sitting at a terminal, would play with the system or play "beat the system" in idle time until they won the game. For example:

> Connie, a terminal operator for a state program, enjoyed exploring the system. She worked in the reimbursement section and found out that there was an emergency payment program with no screens for payment under $1,000. "When it started I was playing with the terminal on a break. I typed in my friend's name and then I hit return; it was processed. I could have cancelled it, but I didn't."

Only Some Feared Being Caught

Perpetrators reported that a factor that significantly contributed to their committing a crime was that they didn't fear being caught or punished. Over half said that they didn't even think about the consequences of their actions. They reported that they acted on impulse, or that they just didn't care. One programmer said, "the drugs were in control. I didn't even think about being caught."

Most of the other perpetrators who said that they realized that they might lose their job, go to jail, or be forced to pay restitution, felt that the chances of being caught were minimal. The primary factor here was that most felt that management was not sensitive to crime from the inside, so they weren't being watched.

V. What Was The Work Environment?

> Everyone had an ID number and there was a password to bring the system up. But the codes and ID numbers were on the wall, so everyone and anyone could see them. No one cared. A STATE CLAIMS EXAMINER

Controls Seen As Weak

Not suprisingly, most perpetrators rated computer security and internal controls in their offices as weak and not a significant barrier to their crime. While over 80 percent of the perpetrators were able to identify specific examples of computer security, three-quarters of these said it was weak.

The most common examples of security noted by the perpetrators were various types of access controls. Most systems required personal ID codes and/or passwords. However, as mentioned earlier, perpetrators easily found ways to bypass the ID and password controls, or did not need direct access to the system. Usually however, the access code gave the user full access to the system. In only a few cases was the user limited to specific files or types of transactions.

Other common controls noted by the perpetrators were screens, edits, or alerts that were built into the system. Generally these features would limit the amount of checks that could be issued or would send a hardcopy message back to the office that a specific, atypical transaction had been initiated. A third form of control noted by the perpetrators was separation of duties. In such instances people who made eligibility or payment decisions were not permitted to do data entry.

While access controls, screens, and separation of duties were designed into most computer systems, poor implementation at the user level often undermined their intent. Access controls were often simplistic, or were bypassed in daily practice in the interest of productivity. For example, it was not uncommon for ID numbers to be the users' initials or any 3 digits. Also, passwords and operating codes were often issued in memos or manuals. Terminals, once brought on-line by an authorized operator, were often left on when the operator left the terminal. Edits and screens in the system were well known to all system users and the perpetrators usually just steered clear of them. A few perpetrators reported that it was not uncommon, when a backlog or special event arose, for managers to lift the edits or screens to speed-up the input process.

The security intent of separation duties would be breached when, due to staffing changes, a person was trained in both input and output duties or simply when terminals were left unattended after being brought on-line. For example, some offices have separate terminals for query-only and input. A number of caseworker perpetrators, who had query-only authority, said it was easy to just walk in and sit down at an input terminal under the guise of doing only a query and then to enter an illegal transaction.

Perpetrators Were Aware Of Other Crimes

Another factor that influenced the perpetrators was their perception that the system was vulnerable. Two-thirds of them reported that they were aware of other crimes "like theirs." Half of these said they knew of specific crimes, while the others said they had heard of such crimes. In the wake of a computer crime, it was common for the modus operandi of the perpetrator to be spread by rumor. In a few instances the crime seemed to pervade the office. This was particularly true when supervisors were part of the scheme. For instance, a supervisor in one food stamp office recruited workers to be part of a crime by showing them how to commit the crime. We were able to interview four perpetrators from one case, but it was estimated by one that as many as 30 people were involved. In another office, the number was estimated at 14.

Perpetrators Said Supervision Was Weak

The perpetrators frequently volunteered that, "no one was watching me," when discussing how and why their crime was committed. These reports of weak supervision fell into two categories.

First were weaknesses associated with more traditional forms of supervision. Perpetrators reported that supervisors didn't review their work either because they were a trusted employee, because their supervisor was too overloaded to review everything, or simply because work generally wasn't reviewed. If and when work was reviewed, it was reviewed for productivity and for errors. Employee crime appeared to be a low priority at best.

The second form of weak supervision was of a more technical nature. Some perpetrators reported that their supervisor knew what their job was, but did not know how they did their job at the computer terminal. This is because supervisors often came up through the program when the job was done manually and had never learned how the job is done on the automated system. Accordingly, perpetrators were able to take advantage of such supervisory naivete. One perpetrator told us, "One of the largest problems you have is that managers have no knowledge of the systems. I finished my project 3 months ahead of time and my supervisor didn't know." Another perpetrator who was paying bogus bills to friends said, "My supervisor didn't know anything about the system. Those old ladies watched me all day and never caught me."

VI. How Would Perpetrators Strengthen The Systems?

> I would impress people with the idea of computer security or any security. We knew no one was watching. A FEDERAL CASEWORKER

During the discussions with the perpetrators we asked what could have prevented them from committing their crime or how they would eliminate the vulnerabilities in the computer system they had exploited. What follows are their more commonly cited recommendations.

Random Case Validation

Perpetrators who modified existing cases or created false cases said they exploited the fact that cases weren't verified. They said that when case files were reviewed, it was just a paper review. No one actually spoke to the beneficiary. In fact, one of the major problems perpetrators had in concealing their crimes was dealing with periodic case recertifications. It was common for a perpetrator to have to terminate a false case when a recertification notice went out. Perpetrators recommend that supervisors randomly, openly, and on an ad hoc basis contact beneficiaries to verify their existence and the status of their case. It appears that a very small sample, with only a telephone inquiry, would have raised the risk of detection sufficiently to preclude some of the crimes.

Rotate Caseload

Some perpetrators were able to conceal their crime and control their bogus cases because they were permanently assigned a specific caseload. Case assignments are often based on alphabetical order or the end digit in the beneficiary's ID number. Perpetrators recommended rotating caseloads to assure that one person doesn't have permanent control of a case.

Identify Workers With Their Transactions In The Database

Perpetrators noted that they were able to anonymously enter bogus data into the system. Most systems which the perpetrators worked on did not identify the input technician and/or caseworker with the transaction. Consequently, the perpetrators felt that the system "wasn't being watched." The perpetrators recommended that the system identify the persons who authorizes and/or inputs each transaction.

Limit Access Within The System

Perpetrators noted that they were often able to commit or cover-up their crime by using override or force codes in the system. Such codes give the perpetrator the opportunity to delete data from the system or to bypass edits and screens. Perpetrators recommended that system users' access be limited to only the codes or types of transactions they need to do their job and suggest that this be controlled by each user's ID and password.

Enforce Security Features

Some perpetrators were able to commit their crimes despite computer security features specifically designed to prevent such crimes. Sometimes computer controls were bypassed to promote office efficiencies, while in other situations they were not in effect because of benign neglect. Perpetrators recommend that the purpose and value of computer system controls be stressed to first line managers and that persons in charge of computer security periodically evaluate the implementation of specific controls.

CONCLUSIONS AND RECOMMENDATIONS

Investigations of computer-related fraud cases are generally limited to the facts necessary to prosecute the alleged perpetrator. The findings from interviews with perpetrators described in this report add to earlier findings reported by Inspectors General which were based on data in their files. For example, interviews reported the involvement of co-conspirators in many more cases than IG files suggested. Similarly, interviews provided more descriptive information on how the crimes were perpetrated and the effectiveness of system controls.

Debrief Perpetrators Routinely

Law enforcement officials and criminologists often interview persons convicted of economic crimes to identify the characteristics of a subset of perpetrators. Because computer fraud is a relatively new area of economic crime, we believe that interviewing these perpetrators will add to the growing body of knowledge in this area; and that findings from interviews can be used by management and Inspectors General to prevent additional fraud cases. We recommend, therefore, that:

- Inspectors General routinely debrief perpetrators of computer fraud to identify the specific vulnerabilities in their computer systems;

- Inspectors General provide feedback to management on the findings from perpetrator interviews and assure that controls are instituted to correct vulnerabilities; and

- Inspectors General, program managers, and systems security officers include perpetrator case histories in training on computer crime and computer security, both to heighten awareness and to act as a deterrent.

Strengthen Automated System Controls

Perpetrators reported that the existing controls in the victimized systems were weak and easily bypassed. IDs and passwords were simplistic and/or public knowledge and gave the user access to the whole system, rather than only the applications or transactions necessary for the user's job. A number of the victimized systems did not identify or maintain a record of the specific individual who authorized or input the data, creating the atmosphere of anonymity and severely hampered later review or investigation. Screens and edits were easily circumvented by users or lifted by management in the interest of productivity. These findings suggest the need to implement additional controls to strengthen the integrity of automated systems and prevent the perception that "no one is watching." We therefore recommend that:

- All payment systems be capable of enforcing personal accountability, by including such features as personal identification and authentication, and audit trails;

- Access controls in such systems limit user access to only the programs, records, or transactions required by the user's job responsibility; and

- Management periodically review the adequacy and implementation of all automated systems controls and security features, as required by OMB Circulars A-71 (TM-1) and A-123.

Guidance to State, Local, and Private Agencies

Federal agencies have a substantial investment in State, local, and private computer systems, both because the Federal government finances most of the development and maintenance costs of such systems, and because those systems control the allocation of Federal funds. Yet these systems appear to be vulnerable. About half of the perpetrators worked for State, local, or private agencies that were administering Federal programs. It is recommended that:

- Federal agencies re-evaluate their guidance to State, local, and private administering agencies regarding computer security and controls; and

- Vulnerabilities in State, local, or private agencies computer system be addressed with the same vigor as those in Federal systems.

Training and Awareness of Line Managers

The original study observed IG investigators were not fully aware of internal control procedures for automated systems. Nor were they aware of specific vulnerabilities in their agency's computer systems. Training in these areas was recommended. It appears that a similar lack of sensitivity to controls and potential vulnerabilities exist among line program managers. The potential for employee crime has not been stressed and some managers see system controls more as impediments to productivity than necessary security features. It is recommended that:

- IGs and/or system security officers provide training and awareness programs targeted to line program managers; and

- Procedures be established for "advertising" the existence of internal and system controls to indicate that "someone is indeed watching."

Review Personnel Security Procedures

In the course of locating the perpetrators we learned that 1 in 5 had a prior criminal record. Some were hired by the agencies under special placement programs for ex-felons. In light of our findings it is recommended that:

- Inspectors General and management re-evaluate agency personnel security policies and clearance practices for persons in positions of trust, including all positions with access to payroll, benefit records, and other payment data.

Appendix A

A Perpetrator Tells His Own Story

As a follow-up to our discussion with one of the perpetrators, he wrote down his own views of how and why he committed his crime. He has given us permission to include it in the report in the hope that it may help prevent other individuals and agencies from finding themselves in similar situations.

I am 44 years old and married. I am a formerly admitted lawyer and former claims examiner in a benefit program in a Federal regional office.

From June of 1980 to November 1981, while employed as a GS-11, I manipulated financial disbursement computers in such a way as to cause the computers to issue about 40 checks totalling about $54,000 to recently deceased beneficiaries. I had the checks mailed to my home. I forged the beneficiary's signatures and then deposited the checks in my personal checking account.

A more alert personnel security system, coupled with improved computer security would have made my crimes more difficult to perpetrate. However, the personnel security system was not designed to detect or flag likely violators. As for computer security procedures, they were virtually nonexistent. Password controls were lax. Audit trails were not examined by officials with any eye to detecting crime. The computers were not safeguarded adequately and, as a consequence, any number of us who had access to the ADP systems could have initiated the same crimes that I initiated.

The scheme I used was basically foolproof. I could have gone on with it indefinitely. In fact, 18 months went by from the time I quit my job until the Government, capitalizing on a simple and stupid mistake that I had made, detected my crimes and caught up with me.

Before recounting the details of my experience as a Federal employee, I would like to provide background of my own past. In a very real sense, my past played an important role in what I did. I grew up in a middle class home. A reasonably good student, I attended Penn State for two years and then transferred to the University of Pittsburgh where I completed my studies and graduated with a Bachelor of Science degree in Psychology. In 1969, I enrolled in law school, graduating in May of 1973 and being admitted to the Bar in May of 1974. It took me a total of 10 years to graduate because I worked to finance my own way.

It is also noteworthy that somewhere in my high school and college career I developed a serious drinking problem. I would continue to drink excessively and regularly until, at the age of 35, I brought my habit under control.

My alcoholism did not prevent me from obtaining a security clearance when I was in the Air National Guard, where I served from 1966 to 1971, including the period of May of 1968 until December of 1968, when as a result of the Pueblo incident, my unit was activated.

While still in law school, I started a private investigations business, in a small town, near a major eastern city. Most of my business involved injury claims due to product malfunction and car accidents and law enforcement related cases in which defense lawyers retained me on behalf of their clients. I had the investigative business from 1971 until 1975.

In the mid-1970's, I began to suffer from frequent bouts of depression stemming, I believe, from too much studies, too much outside work, and too much alcohol. In addition, my family was suffering because we were constantly short of cash. And I had another family problem. It was my mother, who, like me, had a drinking habit of equally self-destructive proportions. Eventually, she literally drank herself to death. I tried to encourage her to give up drinking and failed in my efforts, leaving me emotionally drained from seeing someone destroying herself, while caught up in the same trap that I was in.

My investigative work also had become a source of emotional difficulty for me. I was retained on one particularly grisly murder case that endangered my physical well-being and that ultimately led me to decide that I wanted to get into a more conventional pursuit. It was that decision that caused me to apply for a Federal job. That was in 1974.

I made another important decision in the year 1975 and I quit drinking.

I was somewhat idealistic about my government job. I felt I could do some good for my program beneficiaries and their families. At the same time, I hoped that change of scenery and pace would be good for myself and my family.

Unfortunately, I was soon to be discouraged with government service. I had been promoted a couple of times and had outstanding ratings on my performance. However, when a promotion that I wanted and felt that I clearly deserved was denied me, I became an enraged, disgruntled employee.

As I look back, I realize that I grossly overreacted to the lost promotion. I was in a rage -- over what I will leave to psychiatrists to explain. It was one thing to be angry over what I perceived to be an unjust personnel action. It was quite another to experience the rage that I experienced.

For a time, I was able to channel my rage, by involving myself in union work. I became president of a local union for Federal employees representing employees in four agencies. I also served as a substitute for a national representative, when there was no such representative in my area for a time.

I found the union work to be very satisfying. I didn't get paid for it, but I felt that I was able to help people to get a fairer shake than they were getting.

However, the emotional problems that I mentioned still remained within me and I made a scapegoat out of my agency. By now my family was living better than I ever lived. My wife and I were both bringing home good salaries. So we didn't really need more money. Yet for reasons to this day that I am unsure of I began to devise a scheme to steal through my agency's computer system.

Having grown up with traditional middle class values, I had never stolen anything before in my life. Also, as the product of a middle class environment, I had always been astonished at the criminals I had known in my investigative business because of their lack of fear of getting into trouble. Yet now, for the first time in my life, I found myself plotting a crime -- and, if that wasn't unpredictable enough, I found myself not fearing getting caught or getting incarcerated. I know from my own experiences that career criminals do not feel humiliation when they are apprehended. They, in most cases, don't seem to be deterred by the prospect of going to prison. For about a year and a half, I was in that frame of mind myself. For lack of a better term, I would describe myself, during the time period in question as burnt out. I was obsessed with one objective -- and that was to beat my agency illegally and to get away with it.

My scheme went like this:

I would note the death of a beneficiary who had been receiving a monthly entitlement check. I would be alerted to the death because I would receive a computer message that a check had been returned with this notation, "Possible Death of Payee."

Next, the office would send out a letter to the beneficiary's address asking for information as to the beneficiary's status. We would receive a response confirming the death. I would then ascertain that there were no other possible claimants. I would then proceed with my scheme.

First, I would remove the entire case file from the office. I took it home and destroyed it.

Second, I would enter into the computer a message that the beneficiary had undergone a change in financial circumstance -- a large number of medical bills, for example. I would make a retroactive benefit totalling less than $5,000. Anything under $5,000 I was authorized to process without another section's participation. In theory, two persons' computer access cards were necessary to create the benefit checks that I created by myself. However, there was no security regarding those cards, as the cards of other employees who may have been absent from the office, were just left lying around, totally unsecured. Additionally, each employee had a personal ID number to be used to log on to the computer when the access card was put in the terminal. I was able to steal another employee's ID number by standing behind them as they logged on. I simply watched their fingers as they typed their ID number.

Third, I would alter the beneficiary's address. Instead of sending the check to the beneficiary's home, I directed it to my address. However, because you needed two employees to complete such a transaction, I first used my own access card and ID to initiate the change and then I used another employee's card and ID to confirm the change. It was easy.

Fourth, I would terminate the beneficiary's case on the computer a month later. In six months, I knew the computer would erase all memory of the case and its history. That is why I call this a fool-proof scheme.

The checks would come to my house. I would sign the beneficiary's name, then endorse it myself and then deposit it in my personal account. I quit committing the crimes in November of 1981. Four months later I resigned, and about a year and a half later, the crimes were detected.

The mistake I made was that around the first of the year, I inadvertantly misdated the date of a beneficiary's death. This, when caught in a computer match led auditors to make a routine inquiry and they discovered several checks going to one address. It wasn't long before they realized that a violation may have occurred. The Secret Service was called in. My checking account was subpoenaed. Further inquiry established that the beneficiaries had all died earlier than I had listed them. The authorities put together a solid case against me.

I was indicted on many counts of mail fraud and forgery in April of 1984. I plead guilty and was sentenced to one month in a half way house, two three-year suspended sentences and five years of probation and ordered to make restitution of the $54,000. I was also fined $2,000. I was also suspended from the practice of law.

It was not money that motivated me in my crimes, it was irrational rage caused by emotional exhaustion, the sources of which were my long time excessive drinking, my overwork, disappointment with government service and the anguish of watching, but being unable to help, as my mother drank herself to death.

I made as much and more money than I earned with the government. All these factors are evidence that money or greed was not my primary motivation.

I have asked myself many times if my agency could have done anything to predict that I, and people like me, would initiate fraud against its computer. The answer is, yes.

The computers capable of disbursing dollar instruments were not properly protected against abuse. They were like unlocked bank vaults waiting to be invaded. Security around these machines was almost nonexistent. So the first thing I would say is that plant security must be considered an essential function of personnel security. If the bank vault has money in it and if nobody is watching, somebody, for whatever reason, is likely to steal from it.

The problem is also one of attitude. For example, one of the jobs that I had before was as a claims examiner for a private insurance company. There was a totally different approach to money there. Security was important to the managers. Conversely, this attitude seemed to be lacking at the Federal agency.

Along with improved physical security, I would point out that a more alert personnel security system might have flagged me or someone like me for two or three reasons.

I was a practicing alcoholic. I had a twenty-year history of heavy drinking.

My anger and rage at the agency -- most of which was unwarranted and irrational, was not something I tried to conceal. If a trained investigator would have interviewed me, I would have revealed my feelings, thereby calling attention to the possibility that I was a risk.