Report to the Congress:

Adequacy of Federal Sentencing Guideline Penalties for Computer Fraud and Vandalism Offenses

(as directed by section 805 of Public Law 104-132)



United States Sentencing Commission
June 1996

Report to the Congress:
Adequacy of Federal Sentencing Guideline Penalties
for Computer Fraud and Vandalism Offenses

I. Introduction

A. The Statutory Directive

Congress has directed the Commission, pursuant to Section 805 of the Antiterrorism and Effective Death Penalty Act of 1996 (Antiterrorism Act)[1], to review the deterrent effect of existing guidelines as they apply to computer crimes set forth at 18 U.S.C. § 1030 (a)(4) and (5).[2] This report responds to that particular directive.

The computer crimes set forth at 18 U.S.C. §1030 (a)(4) and(5) prohibit unauthorized access of a federal government data base for the purpose of obtaining information to perpetrate a fraud (subsection (a)(4)) and the transmission of a program, information, code, or command to a computer system used in interstate commerce or communication for the purpose of damaging such a system or with reckless disregard for the possibility that such damage will occur (subsection (a)(5)).

The Commission is further instructed to amend its guidelines to the extent necessary to ensure that any individual subsequently convicted of violating 18 U.S.C. § 1030 (a)(4) or (5) will face a minimum term of imprisonment of six months. The Commission is currently considering alternative means of implementing this sentencing directive. The Commission is also considering other needed changes in the guidelines applicable to computer crimes. This work continues a cooperative effort with the Department of Justice begun several years ago and may result in the submission of guideline amendments to Congress within the next amendment cycle (*i.e.*, by May 1, 1997).

---

[1] Pub. L. No. 104-132, 110 Stat. 1214 (1996).

[2] Congress specifically directed that the Commission ". . . review the deterrent effect of existing guideline levels as they apply to paragraphs (4) and (5) of section 1030 (a) of title 18, United States Code."

B. Summary of Findings

The following findings [3] are based on the Commission's review of approximately 80 percent of guideline convictions (1988 to present) under 18 U.S.C. § 1030 (a)(4) and (5):

- Federal "computer crime" cases sentenced under the pertinent provisions of 18 U.S.C. § 1030 are relatively uncommon at present. An estimated 60 defendants have been successfully prosecuted and sentenced thereunder in the almost nine years since the guidelines came into existence.[4]

- Overall, federal district judges historically have sentenced a higher percentage of those convicted under 18 U.S.C. § 1030 (a)(4) or (5) within the guideline range than has been true of other "white collar" defendants or federal defendants generally.

- Computer crime defendants receive downward departures from guideline ranges more frequently than do other "white collar" defendants or federal defendants generally.

- To date no person sentenced under the guidelines whose primary offense of conviction was a computer crime under 18 U.S.C. § 1030 (a)(4) or (5) has received a sentence that departed upward from the guideline range.

- Defendants convicted under 18 U.S.C. §1030 (a)(4) or (5) tend to have more formal education than other "white collar" defendants and much more formal education than federal defendants generally.

- Individuals convicted under the pertinent statutes tend to have less serious criminal histories than other "white collar" criminals and much less serious criminal histories than federal defendants generally.

---

[3] The Commission's data base of sentences imposed under the guidelines contains 174 cases of computer crime convictions under 18 U.S.C. § 1030. Thirty-eight (38) of the most temporally remote of these files had not been received from outside storage at the time this report was prepared. Forty (40) cases have been identified in which computer crime pursuant to 18 U.S.C. § 1030 (a)(4) or (5) was the primary offense of conviction and in which sentences were established pursuant to the fraud guideline (USSG §2F1.1). Thus, even if all 38 of the files not yet reviewed are for convictions under the pertinent statutory provisions, an unlikely result, no more than 78 federal convictions under 18 U.S.C. § 1030 (a)(4) or (5) will have been obtained in a period of more than seven years. If the proportion of convictions under subsections (4) and (5) to total computer crime convictions for cases already reviewed remains constant in the files to be reviewed, the total result will be approximately 60 guideline sentences under subsections (4) and (5).

[4] *Id.*

- To date no person convicted of violating 18 U.S.C. § 1030 (a)(4) or (5) and sentenced under the fraud guideline has been sentenced for a subsequent federal crime.

- A review of the sentences imposed upon those who violated 18 U.S.C. § 1030 (a)(4) or (5) prior to the enactment of the Antiterrorism Act indicates that the guideline adjustments mandated by Congress generally will increase punishment for this class of defendant.

- Existing data do not permit the Commission to draw any firm conclusions regarding the deterrent effect of existing guideline penalties for these computer-related crimes.

II. Operation of Relevant Sentencing Guidelines, Computer Fraud Crimes

The sentencing guidelines contain multiple, related mechanisms designed to achieve appropriate punishment for fraud offenses, including frauds perpetrated with the aid of a computer.[5] These provisions include: (1) the fraud offense guideline (§2F1.1); (2) related commentary identifying atypical offense characteristics that may justify a sentence above the applicable guideline range (§5K2.0); (3) the vulnerable victim adjustment which provides enhanced sentences for those who choose their victims mindful of some characteristic (*e.g.*, youth, old age, mental infirmity, etc.) which makes them particularly susceptible to the crime (§3A1.1); and (4) the adjustment for abuse of a position of trust which provides for a two level enhancement to the offense score of a defendant who, because of his status as a trusted managerial employee, is subject to significantly less supervision than rank-and-file employees (§3B1.3).

A. Fraud Guideline

The Federal Criminal Code contains numerous fraud offenses which vary in their mode of perpetration (*e.g.*, mail, telephone, computer, etc.), affected victims, and penalty structure. The Sentencing Commission promulgated a single fraud guideline, §2F1.1, to govern sentencing of these myriad fraud offenses. The fraud guideline is designed to measure the seriousness of a given offense by requiring the district court to assess: (1) the amount of loss experienced by the victim or victims of the offense; (2) the sophistication of the offense in terms of planning; (3) whether the offender claimed to be a representative of a charity or other especially trusted institution; (4) whether the criminal conduct violated a previously imposed judicial or administrative order; (5) whether the serious bodily injury occurred or was risked; and (6) whether significant harm was suffered by a financial institution.

B. Departures

[5] Crimes pursuant to subsections (a)(4) and (5) are currently designated to the fraud guideline despite the fact that subsection (a)(5) violations are not true fraud offenses. The Commission is currently considering redesignating subsection (a)(5) violations to the trespass guideline or, potentially, other alternatives.

Guideline §5K2.0 (Grounds for Departure) is a policy statement explaining circumstances that may warrant a sentence outside the otherwise applicable guideline range. This departure authority reflects Congressional intent promulgated under 18 U.S.C. § 3553 (b), which provides, in pertinent part, that the district court may impose sentences outside the range established by the applicable guideline when it finds "that there exists an aggravating or mitigating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines that should result in a sentence different from that described."

The guidance afforded by §5K2.0 is augmented by the Commission's general approach to departures as stated in Chapter One of the Guidelines Manual.[6] Read together, these sections articulate the Commission's desire that applicable guideline provisions will result in sentences appropriate for typical ("heartland") cases of particular offense types and offender categories.[7]

C. Vulnerable Victim Adjustment

Where a defendant has exhibited predatory conduct which targeted victims because of their unusually high vulnerability to the crime, the Commission has provided a general, two-level enhancement (approximately a 25 percent increase in sentence length). This enhancement is promulgated at §3A1.1 (b) and can apply to a wide range of criminal behavior, including computer fraud. Section 3A1.1 (b) envisions an ad hoc determination by the district court focusing both on whether the victim was "unusually vulnerable" and on whether the defendant knew or should have appreciated that vulnerability.

D. Abuse of Position of Trust

Where a defendant has held a position characterized by substantial discretionary judgment and in which he has been subject to significantly less supervision than employees whose tasks are non-discretionary in nature, a violation of this trust can result in a two level enhancement and correspondingly harsher sentencing. This enhancement applies only when the position of trust contributed in some way to the commission or concealment of the offense.[8] This "abuse of trust" enhancement is applied to computer fraud defendants at a much higher rate than to other federal defendants. *See Table 2, post.*

III. Data Analysis

---

[6] *See* USSG Ch. 1, Pt. A 4(b).

[7] Along with the nature of the offense, guideline sentences are determined by criminal history scores which assess an offender's previous criminal record and provide incrementally greater punishment in relation to the frequency, seriousness, and temporal proximity of the offender's previous criminal behavior. *See* USSG Ch. 4, Pts. A and B.

[8] *See* USSG §3B1.3, App. Note 1.

A. General Approach

The Commission reviewed sentencing files of 136 of the 174 defendants who have been convicted of any crime under 18 U.S.C. § 1030 since the guidelines became effective in 1987. Only 51 of the 136 files reviewed involve convictions under subsections (a)(4) or (5).[9] Of these 51 cases, only 40 were cases in which either subsection was the primary offense of conviction. These 40 cases were coded for pertinent data. Using a variety of factors, discussed more fully *infra*, these computer crime cases have been compared to all federal convictions (1988-95) and to all "white collar" convictions (1988-95).[10] Unfortunately, this data affords a scant basis upon which to comment concerning the deterrent effect, specific or general, of the existing guidelines upon those who have committed or would otherwise have committed crimes as defined in 18 U.S.C. § 1030 (a)(4) or (5). For this reason, the Commission attempted to establish a "profile" of the typical offender under the pertinent statutes in the hope that this "profile," in combination with research on the "deterrability" of individuals sharing the characteristics of the "profile," would permit a reasoned assessment of the deterrent effect of the existing guidelines.

B. Methodology and Data Limitations

There are several reasons why the dataset available to the Commission is inadequate to evaluate the deterrent effect of existing guideline penalties for computer crime. Empirical assessment of the deterrent effect of the guidelines is inhibited by two important factors: 1) the absence of case information prior to the promulgation of the sentencing guidelines; and 2) the lack of information on important additional variables (*e.g.*, percentage of the public which knows the guidelines exist, percentage of the public which knows the extent of penalties provided by the guidelines, extent to which technological advances have increased the security of computer systems, allocation of law enforcement resources etc.) which could impact the rate of occurrence of computer crime. An assessment of the deterrent impact of the guidelines cannot be made without some knowledge of the rate of occurrence of computer crime prior to the enactment of the guidelines. Even could it be demonstrated that the rate of computer crime has decreased since implementation of the guidelines, this would not permit the conclusion that the guidelines were responsible for such a decrease. [11]

Even if all the unknown variables discussed above could be accounted for, the small population of computer crime defendants sentenced to date under the guidelines would be inadequate

---

[9] *See supra note 3.*

[10] In this context "white collar" crime means the aggregate number of federal convictions from 1988 through 1995 for the following types of offenses: fraud, embezzlement, forgery, counterfeiting, bribery, tax offenses and money laundering.

[11] Concomitantly, an increased rate of computer crime after implementation of the guidelines would not permit the conclusion that the guidelines were not providing deterrent effect. The increase could be attributable to a steeply increasing rate of opportunity for commission of computer crimes, economic conditions, etc.

to permit any statistically valid generalizations about the ability of the existing guidelines to provide specific deterrence (*i.e.*, deter those already convicted from engaging once again in this crime) or general deterrence (*i.e.*, the extent to which those who had the opportunity to commit such crimes refrained from such behavior as a result of their knowledge and fear of punishment as prescribed by the existing guidelines). Because only an estimated 60 persons have been convicted in the federal system of computer crime offenses under 18 U.S.C. § 1030 in a time when the number of computers and those with access to them has increased exponentially, one could hypothesize that the existing guidelines have afforded effective general deterrence. Yet, a number of pertinent questions remain unanswered. For example, how much criminal behavior that could have been successfully prosecuted under 18 U.S.C. § 1030 was prosecuted under other fraud statutes or under state law, or not prosecuted at all, at the election of individual prosecutors? How much of this conduct has simply gone undetected? The fact that the Commission does not have information to answer adequately these and possibly other relevant questions necessarily limits the validity of any conclusions it may draw concerning the general deterrence of the existing guidelines.

With respect to specific deterrence, the data reviewed indicate that 40 defendants convicted under 18 U.S.C. § 1030 (a)(4) or (5) have received a guideline sentence[12] and, to date, none of these 40 individuals have been sentenced for other federal crimes.[13] This may seem to indicate that the existing guidelines provide adequate specific deterrence. However, most of the 40 individuals, 21 of whom have been subjected to some length of imprisonment, have been released from criminal justice control too recently to determine whether any of the 40 ultimately will recidivate.[14]

Because of the inadequacy of the available statistical information, standing alone, to permit any definitive response to Congress' deterrence question, the Commission compiled additional data

---

[12] As indicated previously, 51 defendants are known to have been convicted under 18 U.S.C. § 1030 (a)(4) or (5). However, the sentences of 11 of these defendants were determined primarily under guidelines other than the fraud guideline because of more serious related criminal conduct. The 40 whose sentences were determined under the fraud guideline are the analytically significant portion of this population. Of these 40, 21 were sentenced to some term of imprisonment. Thus, 47.5 percent (19 of 40) of the universe of offenders sentenced to date primarily for violations of 18 U.S.C. § 1030 (a)(4) or (5) drew sentences of probation. It may readily be inferred that Congress' direction to provide for six months imprisonment for these crimes will dramatically affect sentencing practices in this context.

[13] A name and social security number check of the Commission's files was conducted to verify that each of these 40 persons has been sentenced only once under the guidelines.

[14] Also, the cases thus far examined indicate that 77.5 percent of those convicted under the pertinent statutory provisions committed their crimes in the workplace. Their criminal records may well have precluded them from the occupations they formerly performed and deprived them of the opportunity to repeat their crimes. Thus, their post-sentence conduct may be more attributable to the fact that these individuals no longer function in an environment where repetition of their crimes is possible than to the deterrent effect of the guidelines.

(Tables 1, 2, 3 and 4 attached) from which a profile of a "typical offender" has been drawn.[15] It was hoped that this profile, in combination with the research social scientists have produced on the question of the "deterrability" of "white collar" crime, could be used to draw tentative conclusions about the deterrent effect of the existing guidelines. The data presented in Tables 1, 2, 3 and 4 provide a convenient reference for looking at the characteristics of the "typical" computer crime case.

C. Findings

Table 1 compares all federal convictions, "white collar" convictions, and all convictions under the pertinent statutory provisions from 1988 through 1996 for various "defendant characteristics" including citizenship, gender, race and level of education. For the most part, the comparisons are unremarkable; however, with respect to educational level, the data indicate that the typical computer crime defendant is better educated than other "white collar" defendants and much better educated than federal defendants generally. Specifically, 26.3 percent of computer crime defendants are college graduates as opposed to 17.1 percent for "white collar" defendants and only 7.5 percent for all federal defendants.

Table 2 illustrates the application of various guideline factors to the groups being compared. In terms of average base offense levels, mode of conviction, and frequency of receipt of a downward adjustment for acceptance of responsibility (USSG §3E1.1), the data in Table 2 is unremarkable. Perhaps significantly, the typical computer crime defendant has no criminal history. Eighty (80) percent had no criminal history score (vis-a-vis 65.7 percent in "white collar" defendants and 50.6 percent in all federal defendants). Thus, from the sample the Commission could examine, it appears that computer crime defendants have less significant criminal histories than other federal defendants. It should be noted also that computer crime defendants receive enhanced sentences for "abuse of position" pursuant to §3B1.3 more frequently than "white collar" defendants (32.5 percent for the former; 8.8 percent for the latter) and much more frequently than the class of all federal defendants (32.5 percent vis-à-vis 3.0 percent).

Table 3 illustrates sentencing statistics for the groups being compared. Table 3 provides illustrative information with respect to departure rates and guideline ranges. Computer crime defendants were sentenced within guideline ranges at a rate of 86.1 percent; "white collar" defendants at a rate of 80.4 percent; and the class of all federal defendants at 76.6 percent. Computer crime defendants received downward departures from guideline ranges more frequently than members of the other two groups, and no computer fraud defendant has ever been subjected to an upward departure. The data tends to suggest that sentencing judges are generally satisfied that guideline sentences for computer crime defendants are realistically constructed to mirror the seriousness of these offenses.

---

[15] This "typical offender" has been delineated on the basis of those 40 individuals whose sentences were calculated under the fraud guideline and who were convicted under 18 U.S.C. § 1030 (a)(4) or (5).

Table 4 includes information on computer crime defendants only. The Commission reviewed each available computer crime case file and collected information on the level of computer expertise of these defendants, the motivation for their crimes, the way in which a computer was used in the crimes perpetrated and the environment where the crimes were committed. Data in Table 4 indicate that the typical computer crime defendant has only a pedestrian level of computer expertise (76.9 percent were neither computer professionals nor highly skilled "hackers"), is motivated to commit his/her crime for financial reasons (87.5 percent of the time), and usually commits his/her crime through the use of a computer he/she is authorized to use in his/her workplace (77.5 percent of the time). These findings tend to dispel the popular notion that the typical computer crime defendant is a highly skilled computer "hacker" invading classified data bases with intent to sabotage or extort. Yet, it must again be stated that the population examined is very small, and one cannot measure the frequency or extent of criminal conduct which may go undetected or is detected without means of identifying the offender. The Commission's data obviously are the outcome of a process that is contingent upon the detection, federal prosecution and conviction of computer crime offenders. The limited data which the Commission does possess indicate that the typical computer crime defendant commits his crime in the workplace, has only functional computer skills, and is motivated by hope of illicit profit.

An additional, perhaps significant, fact is that none of the 40 computer crime defendants who have been sentenced under the guidelines as a result of convictions under 18 U.S.C. § 1030 (a)(4) or (5) have been subsequently convicted of another federal crime. While this fact would tend to support the proposition that the existing guidelines provide adequate specific deterrent effect, other considerations preclude such a definitive conclusion. For example, these offenders all have completed their sentences fairly recently and, as such, some may very well yet recidivate. Moreover, it is possible that some have already been arrested for subsequent federal crimes which are not yet ripe for disposition. It is possible, too, that some have committed subsequent offenses which will generally not appear in the Commission's data base (*e.g.*, offenses under state law). These factors, plus the small size of the population being examined, militate against drawing any strong conclusions as to the deterrent effect of the existing guidelines.

IV. Deterrence Studies

In addition to compiling the aforementioned data contained in Tables 1-4, the Commission has conducted a limited review of scholarship on the subject of general deterrence and the factors that specifically deter "white collar" criminals from repeating their offenses.[16] Based on this limited review, it appears generally that researchers who have studied general deterrence have found that it is very difficult to say with certainty the extent to which a given criminal sanction discourages criminal conduct. However, some researchers who have studied deterrence believe that (1) there is inherent deterrent effect in criminalizing a behavior, and (2) that the deterrent effect increases where the perception exists that punishment will be certain, swift and severe. Conversely, to the extent that any of these perceptions is lacking, deterrent effect diminishes.[17]

V. Conclusion

The limited empirical data available to the Commission and other factors preclude a definitive assessment of the deterrent effect of existing guidelines for computer fraud and computer vandalism.[18] The relatively few convictions under these provisions are insufficient to permit generalized conclusions about their deterrent effect. As convictions increase, the Commission, in cooperation with the Department of Justice, will continue to analyze the operation of the guidelines in the computer crime context and expects to consider additional modifications in the current, 1996-97, amendment cycle to improve their operation and effectiveness.

---

[16] The Commission's review of existing scholarship on the specific subject of factors which would deter an individual from committing computer crime found no such studies in the criminal justice literature.

[17] *See, e.g.,* Jack P. Gibbs, Crime, Punishment and Deterrence, 5-11 (1975).

[18] Moreover, the "profile" of the typical computer crime defendant, when correlated to existing scholarship on deterrence, still did not enable the Commission to conduct a definitive analysis.

Table 1

DEFENDANT CHARACTERISTICS FOR ALL CASES, WHITE COLLAR CASES, AND COMPUTER FRAUD CASES

	All Cases[1]		White Collar Cases[2]		Computer Fraud Cases[3]	
DEFENDANT CHARACTERISTICS	Number	Percent	Number	Percent	Number	Percent
CITIZENSHIP STATUS						
U.S. Citizen	148,499	77.4	37,266	86.5	36	94.7
Non-U.S. Citizen	43,472	22.6	5,828	13.5	2	5.3
CRIMINAL HISTORY POINTS						
No Points	117,191	50.6	28,166	65.7	32	80.0
One or More Points	114,324	49.4	14,702	34.3	8	20.0
GENDER						
Male	166,391	84.3	32,040	73.0	27	71.1
Female	31,041	15.7	11,838	27.0	11	28.9
RACE						
White	83,779	42.9	26,026	59.7	27	71.1
Black	56,454	28.9	11,052	25.4	8	21.1
Hispanic	47,596	24.4	4,504	10.3	2	5.3
Other	7,402	3.8	1,979	4.5	1	2.6
EDUCATION						
Less than High School	75,553	39.9	8,885	20.8	2	5.3
H.S. Graduate	63,196	33.3	14,246	33.4	12	31.6
Some College	36,517	19.3	12,271	28.7	14	36.8
College Graduate	14,244	7.5	7,284	17.1	10	26.3

[1]Of the 248,896 cases, the total for each characteristic may add up to less than the overall total due to missing information for all demographic variables prior to 1990.
[2]White collar offenses encompass the following offense types: fraud, embezzlement, forgery/counterfeiting, bribery, tax offenses, and money laundering. The total for each characteristic may add up to less than the overall total due to missing information for all demographic variables prior to 1990.
[3]Of the 174 cases sentenced under §18:1030 from Monitoring's Ongoing Production Files, 51 were convicted under §§18:1030(a)(4) and 18:1030(a)(5). Of those 51, 40 were sentenced under §2F1.1 as the highest guideline. The total for each characteristic may add up to less than the overall total due to missing information for that variable.

SOURCE: U.S. Sentencing Commission, Ongoing Production Files, 1988 - 1996.

Table 2

GUIDELINE FACTORS FOR ALL CASES, WHITE COLLAR CASES, AND COMPUTER CRIME CASES

GUIDELINE FACTORS	All Cases[1]		White Collar Cases[2]		Computer Crime Cases[3]	
	Number	Percent	Number	Percent	Number	Percent
ABUSE OF POSITION						
Received Adjustment	6,890	3.0	3,776	8.8	13	32.5
No Adjustment	225,010	97.0	39,128	91.2	27	67.5
ACCEPTANCE OF RESPONSIBILITY						
Received Adjustment	189,728	81.8	37,545	87.5	38	95.0
No Adjustment	42,169	18.2	5,361	12.5	2	5.0
CRIMINAL HISTORY						
No Points	117,191	50.5	28,166	65.6	32	80.0
One or More Points	114,324	49.3	14,702	34.3	8	20.0
MODE OF CONVICTION						
Plea	203,610	88.3	40,694	92.9	38	97.4
Trial	27,031	11.7	3,118	7.1	1	2.6
AVERAGE SENTENCE RANGE[4]						
Mean Sentence Range (Months)	41 - 51		6 - 12		0 - 6	
Median Sentence Range (Months)	27 - 33		0 - 6		0 - 6	

[1]Of the 248,896 cases, the total for each characteristic may add up to less than the overall total due to missing information for abuse of position and acceptance of responsibility prior to 1990.

[2]White collar offenses encompass the following offense types: fraud, embezzlement, forgery/counterfeiting, bribery, tax offenses, and money laundering. The total for each characteristic may add up to less than the overall total due to missing information for abuse of position and acceptance of responsibility prior to 1990.

[3]Of the 174 cases sentenced under §18:1030 from Monitoring's Ongoing Production Files, 51 were convicted under §§18:1030(a)(4) and 18:1030(a)(5). Of those 51, 40 were sentenced under §2F1.1 as the highest guideline. The total for each characteristic may add up to less than the overall total due to missing information for that variable.

[4]Sentence ranges are derived from average base offense level and Criminal History Category I.

SOURCE: U.S. Sentencing Commission, Ongoing Production Files, 1988 - 1996.

Table 3

SENTENCING FACTORS FOR ALL CASES, WHITE COLLAR CASES, AND COMPUTER FRAUD CASES

SENTENCING FACTORS	All Cases[1]		White Collar Cases[2]		Computer Fraud Cases[3]	
	Number	Percent	Number	Percent	Number	Percent
DEPARTURE STATUS						
Within Range	169,259	76.6	33,147	80.4	31	86.1
Upward Departure	3,072	1.4	409	1.0	0	0.0
Downward Departure	14,989	6.8	2,813	6.8	4	11.1
Substantial Assistance Departure	33,608	15.2	4,884	11.8	1	2.8
WITHIN-GUIDELINE RANGES[4]						
First Quartile	80,732	63.8	18,798	66.6	17	73.9
Second Quartile	19,415	15.3	4,275	15.1	4	17.4
Third Quartile	7,124	5.6	1,410	5.0	1	4.3
Fourth Quartile	19,307	15.3	3,750	13.3	1	4.3
SENTENCE IMPOSED						
Prison Only	181,104	73.8	21,061	48.5	11	28.2
Prison + Confinement	8,888	3.6	3,577	8.2	5	12.8
Probation + Confinement	19,546	8.0	8,065	18.6	9	23.1
Probation Only	35,944	14.6	10,725	24.7	14	35.9
MEAN PRISON SENTENCE[5]						
Mean	63.2		19.3		13.1	
Median	33.0		12.0		9.0	

[1]Of the 248,896 cases, the total for each characteristic may add up to less than the overall total due to missing information on mandatory minimums prior to 1992.
[2]White collar offenses encompass the following offense types: fraud, embezzlement, forgery/counterfeiting, bribery, tax offenses, and money laundering. The total for each characteristic may add up to less than the overall total due to missing information for that variable.
[3]Of the 174 cases sentenced under §18:1030 from Monitoring's Ongoing Production Files, 51 were convicted under §§18:1030(a)(4) and 18:1030(a)(5). Of those 51, 40 were sentenced under §2F1.1 as the highest guideline. The total for each characteristic may add up to less than the overall total due to missing information for that variable.
[4]Only cases sentenced within the guideline ranges are included. Additionally, cases were excluded due to missing sentencing variables or various logical criteria.
[5]Cases with zero months prison or conditions of confinement only (as defined in USSG §5C1.1) were excluded.

SOURCE: U.S. Sentencing Commission, Ongoing Production Files, 1988-1996.

Table 4

CHARACTERISTICS FOR 1989-1996 COMPUTER FRAUD CASES [1]

COMPUTER FRAUD CHARACTERISTICS	Computer Fraud Cases	
	Number	Percent
LEVEL OF COMPUTER EXPERTISE		
Professional	2	5.1
Hacker	7	17.9
Work Related/School	30	76.9
None	0	0.0
INTENT OF OFFENSE		
Profit	35	87.5
Maliciousness	3	7.5
Other	2	5.0
ROLE OF COMPUTER IN OFFENSE		
Input New Data	6	15.0
Change Existing Data	23	57.5
Access Secured Data/Services (No changes made)	10	25.0
Other	1	2.5
SETTING		
Office	31	77.5
Home	7	17.5
Other	2	5.0

[3]Of the 174 cases sentenced under §18:1030 from Monitoring's Ongoing Production Files, 51 were convicted of §§18:1030(a)(4) and 18:1030(a)(5). Of those 51, 40 were sentenced under §2F1.1 as the highest guideline. The total for each characteristic may add up to less than the overall total due to missing information for that variable.

SOURCE: U.S. Sentencing Commission, 1995 Datafile, MONFY95 and Ongoing Production Files.