U.S. Sentencing Commission

One Columbus Circle, NE
Suite 2-500, South Lobby
Washington, DC 20002-8002

REPORT SUMMARY

Summary of Findings

Computer Fraud Working Group

From 1984 to 1990, Congress established six new criminal computer offenses, codified at 18 U.S.C. § 1030 under the caption "Fraud and related activity in connection with computers." During the Commission's 1993 amendment cycle, the Department of Justice proposed a new sentencing guideline for cases involving computer fraud and abuse, one that would emphasize harms that cannot be adequately quantified by dollar loss (*e.g.*, intrusion into privacy interests and disruption of telecommunications systems). The Commission responded by organizing the Computer Fraud Working Group to study computer fraud offenses and to investigate whether the nature of these crimes was sufficiently distinct from fraud offenses to justify development of a separate sentencing guideline.[1]

Since their inception, the federal sentencing guidelines have punished criminal computer fraud offenses under the general fraud guideline. In 1993, a staff working group considered whether computer fraud offenses differed sufficiently from other more common fraud offenses to justify development of a separate computer fraud guideline. A summary of the working group's findings is provided in this first in a series of periodic reports that will highlight Sentencing Commission research activities. The full report is available through the Depository Libraries of the U.S. Government Printing Office, Superintendent of Documents.

Computer Fraud Defined

Reaching consensus on a definition of computer crime proved to be difficult. One early definition, advocated by John Taber, called it "a crime that, in fact, occurred and in which a computer was directly and significantly instrumental."[2] Taber's definition, while not universally accepted, initiated further discussion. Other scholars, seeking to narrow it, proposed alternative definitions of computer crime:

- any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution;[3]
- any traditional crime that has acquired a new dimension or order of magnitude through the

---

[1] The Working Group included members of the Commission's legal, research, and training staffs.

[2] J.K. Taber, "One Computer Crime," 1 Computer Law J. 517-543 (1979). *See also* J.K. Taber, "A Survey of Computer Crime Studies," 2 Computer Law J. 275-327 (1980).

[3] D. Parker, Computer Crime: Criminal Justice Resource Manual 2 (1989).

aid of a computer, and abuses that have come into being because of computers;[4]

- any financial dishonesty that takes place in a computer environment;[5] and

- any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.[6]

It could be argued that computer crime is not a unique offense but rather a novel means of committing a more traditional offense. Consequently, many computer crimes are prosecuted under such traditional criminal statutes as wire fraud and destruction of property.

While existing criminal statutes are sufficiently generic to prosecute many computer-related offenses, these statutes are incomplete. For example, some offenses – such as unauthorized access to a computer to permit "electronic browsing" – are unique to computers and difficult to prosecute under traditional criminal statutes. These offenses typically target the computer in which proprietary information is stored and generally can be accessed, altered, stolen, or sabotaged without the perpetrator being physically present or without resorting to the use of force.

Congress, responding to concerns that computers were being used as criminal instruments, enacted the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ("the Act"). In debating the need for this new criminal statute, Congress perceived the existing criminal justice system as ineffective against "unconventional computer operation."[7] Difficulties in prosecuting computer-related criminal activity arise because much of the property involved is intangible (in the form of magnetic impulses) and does not mesh well with traditional theft or larceny statutes. This problem was compounded by "the advent of . . . so-called 'hackers' who have been able to access (trespass into) both private and public computer systems, sometimes with potentially serious results."[8] Codified at 18 U.S.C. § 1030, the Act extended computer-related crime beyond the traditional notions of fraud to other "related activity in connection with computers" by establishing six new offenses:

- knowingly accessing a computer without authorization to obtain national security data *(subsection (a)(1))*;

- intentionally accessing a computer without authorization to obtain certain confidential financial information *(subsection (a)(2))*;

- intentionally accessing a government computer thereby "affect[ing] the use of the government's operation of such computer" *(subsection (a)(3))*;

- accessing a computer with intent to defraud and thereby obtaining anything of value *(subsection (a)(4))*;

- intentionally accessing a computer without authorization, among other things to alter information, thereby causing a loss of at least $1,000 *(subsection (a)(5))*; and

- trafficking in a password or similar information through which a computer can be accessed without authorization, knowingly and with intent to defraud *(subsection (a)(6))*.

---

[4] M.C. Gemignani, "What is Computer Crime and Why Should We Care?," 10 U. Ark. Little Rock L.J. 55, 56 (1987-88).

[5] M. Wasik, Crime and the Computer 1 (1991).

[6] *Id.* at 2 (quoting S.L. Mandell, Computer, Data Processing and the Law 155 (1984)).

[7] H. Rep. No. 98-894, 98th Cong., 2nd. Sess. 9 (1984).

[8] *Id.*

Empirical Study of Defendants Convicted Under 18 U.S.C. § 1030

Methodology

The Computer Fraud Working Group studied defendants sentenced under the federal sentencing guidelines whose criminal conduct involved computer fraud and abuse. The Department of Justice confirmed the contention in the literature that the prosecution of certain cases involving computer fraud and abuse continued under traditional criminal statutes like wire fraud rather than under the computer fraud and abuse statute, 18 U.S.C. § 1030. Indeed, the Working Group found that computer fraud cases could be charged under approximately 40 different federal statutes. In the end, the Working Group limited its study to cases in which the defendant was convicted of at least one count of section 1030.

Commission data for the period January 19, 1989, through April 30, 1993, include 76 cases in which the statutes of conviction included 18 U.S.C. § 1030. Of these 76 cases, 50 were available for inspection.[9] The Working Group examined these cases to determine the incidence of significant sentencing factors identified by the Department of Justice in their proposed computer fraud amendment.

Results

In its examination of the 50 cases in which the defendant was charged under section 1030, the Working Group found that the conduct frequently involved general fraud offenses. Table I and Figure I present the distribution of cases by the section 1030 subsection charged. Table I indicates that the majority (54%, n=27) of the defendants were charged and convicted of section 1030 (a)(4) – general fraud. In these cases, the Working Group found that the pecuniary loss was readily quantifiable and that the existing fraud guideline, §2F1.1, adequately addressed the offense conduct.

TABLE I
DISTRIBUTION OF CASES CONVICTED
UNDER 18 U.S.C. § 1030
BY SUBSECTION CHARGED

Subsection	Nature of Offense	Number	Percent[1]
(a)(1)	Effect on National Security	0	0
(a)(2)	Access to Financial Information	12	24
(a)(3)	Affect Government Use of Computer	5	10
(a)(4)	General Fraud	27	54
(a)(5)	Alteration of Information	1	2
(a)(6)	Trafficking in Passwords	6	12

[1] Percentages total more than 100 because one defendant was charged under both subsections (a)(2) and (a)(4).

In addition to the fraud offenses, 24 percent (n=12) of the defendants were convicted of subsection (a)(2) – improperly accessing financial information. While these cases invoke the privacy provisions of section 1030, the Working Group found that the defendant's motivation typically was to commit a fraud. Review of the case documents indicates that ten cases involved credit card fraud or altering credit histories to obtain bank loans improperly. The remaining two cases involved the theft/embezzlement of monies from a financial institution. Again, because the pecuniary loss in these cases was readily quantifiable, the Working Group found that the existing fraud guideline adequately addressed the offense conduct.

Of the remaining 12 defendants, five were convicted of accessing a government computer

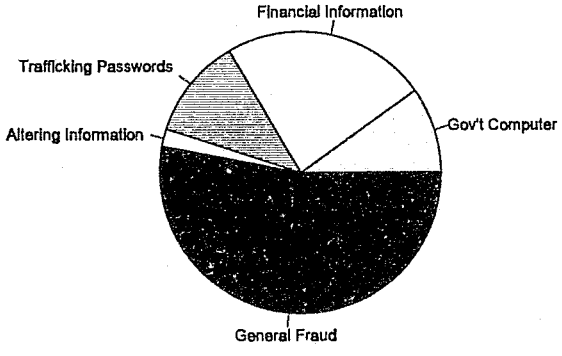
[9] The remaining 26 cases were older and had been archived off-site.

and affecting its use (subsection (a)(3)) by committing the following offenses:

- improperly accessing a computer to obtain criminal history information from the National Criminal Information Center (NCIC) system for re-sale;[10]
- improperly accessing a computer to monitor an ongoing criminal investigation;
- improperly accessing a computer to use e-mail; and
- programming a computer to delete personal information upon a defendant's resignation from an organization.

One defendant was convicted of altering government computer information to browse the system, a violation of subsection (a)(5), and six defendants were convicted of trafficking stolen telephone access passwords, a violation of subsection (a)(6). Of these latter defendants, the Working Group found that the existing fraud guideline adequately covered the offense conduct because the loss caused by the use of the stolen telephone access passwords was readily quantifiable.

FIGURE I
DISTRIBUTION OF CASES CONVICTED UNDER 18 U.S.C. § 1030 BY SUBSECTION CHARGED



In most convictions under section 1030, the Working Group found that the courts generally were able to quantify the pecuniary loss (*see* Table II and Figure II). Table II indicates that

TABLE II
DISTRIBUTION OF CASES CONVICTED UNDER 18 U.S.C. § 1030 BY PECUNIARY LOSS

Pecuniary Loss	No.[1]	Percent	Cumulative Percent
$2,000 or less	10	21.7	21.7
More than $2,000	6	13.0	34.7
More than $5,000	6	13.0	47.7
More than $10,000	4	8.7	56.4
More than $20,000	6	13.0	69.4
More than $40,000	4	8.7	78.1
More than $70,000	3	6.5	84.6
More than $120,000	1	2.2	86.8
More than $200,000	2	4.4	91.2
More than $350,000	2	4.4	95.6
More than $500,000	0	0.0	95.6
More than $800,000	2	4.4	100.0

[1] Four cases were excluded due to missing information describing the pecuniary loss to the victim.

the median loss amount was between $10,000 and $20,000; more than 78.3 percent of the cases involved losses to the victim of less than $70,000.

Finally, the Working Group found that the penalty imposed generally was proportional to the type of offense committed. Table III describes the distribution of sentences imposed according to the defendant's motivation. While the average sentence imposed was 6.8 months imprisonment, the data indicate that defendants who committed the least serious offenses (*i.e.*, browsing computer systems, demonstrating computer prowess, or committing minor vandalism) were placed on probation; defendants who committed fraud, theft, or embezzlement were sentenced to an average of seven months imprisonment; and defendants who affected the administration of justice or committed industrial espionage were sentenced, on average, to 17.3 months imprisonment.

[10] Two defendants were convicted of this offense.

Overall, the Working Group found that most of the cases sentenced pursuant to the guidelines involved economic harms and correlates of the kind addressed by §2F1.1 (*e.g.*, pecuniary loss and planning) and infrequently involved other harms identified by the Department of Justice as important (*e.g.*, invasion of privacy).

Recommendation

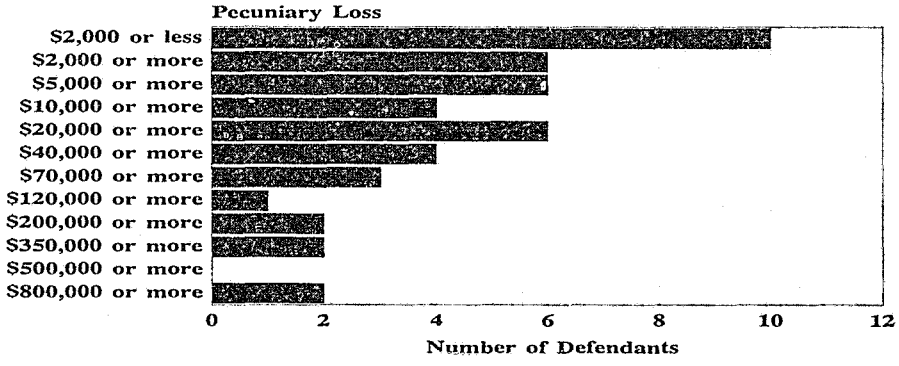
The Working Group concluded that the Commission should not create a separate guideline to govern computer fraud and abuse offenses. This recommendation was based on: (1) the difficulty in defining and measuring the harms that may flow from computer misconduct; (2) the charging decisions that could lead to application of different guidelines, with different sentencing outcomes, for similar computer crimes; and (3) the lack of empirical support for the creation of a separate guideline. The Working Group's review of the existing literature indicated no consensus on a definition of computer crime. The review of Sentencing Commission case files demonstrated that prosecutors can choose from numerous statutes to charge conduct that arises from computer fraud and abuse. Further, the review indicated that these cases typically

TABLE III
DISTRIBUTION OF SENTENCES IMPOSED
BY DEFENDANT'S MOTIVATION

Defendant's Motivation	Number[1]	Mean Sentence
Total	50	6.8
All Forms of Fraud, Theft, or Embezzlement	42	7.0
Obtain Free Use of a Communications Facility	6	0.2
Obtain Free Use of a Computer	3	0.3
Other Fraud, Theft, or Embezzlement	33	8.9
Browsing Computer Systems	2	0.0
Demonstrate Computer Prowess	1	0.0
Vandalism	1	0.0
Industrial Espionage	1	18.0
Interference with the Administration of Justice	5	17.2
Other	4	5.0

[1] Number of cases total more than 50 because some defendants were coded as having more than one motivation.

FIGURE II
DISTRIBUTION OF CASES
CONVICTED UNDER 18 U.S.C. § 1030
BY PECUNIARY LOSS[1]



[1] Four cases were excluded due to missing information describing the pecuniary loss to the victim.

involved the types of harms regularly processed under the theft, larceny, and fraud guidelines. Harms described by the Department of Justice as inadequately measured by the fraud guideline's loss table occur very infrequently.

In lieu of creating a separate computer fraud guideline, the Working Group recommended that: (1) the existing commentary in §2F1.1 be expanded to include the consequential damages of computer crimes; and (2) the Statutory Index be expanded to include references to other existing guidelines (*e.g.*, §2B2.3 (Trespass)) that might address better than the fraud guideline the harms occurring under some subsections of 18 U.S.C. § 1030. Such changes to the existing commentary offer certain advantages over the creation of a new guideline:

- definitional problems could be dealt with more easily using commentary (*e.g.*, the commentary generally could describe harms difficult to define – such as privacy interests – and note that where such harms occur to a significant degree, the court should consider a departure); and

- supplementing the loss commentary in the fraud guideline to include the relevance of consequential loss in computer fraud cases would conform to the current guideline structure that includes commentary explaining the relevance of consequential loss in product substitution and procurement cases.[11]

[11] *See* USSG §2F1.1, comment. (n. 7(c)).