FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1364189-0

Total Deleted Page(s) = 60
Page 7 ~ b3;
Page 8 ~ b3; b6; b7C;
Page 9 ~ b3; b6; b7C;
Page 10 ~ b3; b6; b7C;
Page 11 ~ b3; b6; b7C;
Page 12 ~ b3; b6; b7C;
Page 13 ~ b3; b6; b7C;
Page 14 ~ b3;
Page 15 ~ b3; b6; b7C;
Page 16 ~ b3; b6; b7C;
Page 17 ~ b3; b6; b7C;
Page 18 ~ b3; b6; b7C;
Page 19 ~ b3; b6; b7C;
Page 20 ~ b3; b6; b7C;
Page 21 ~ b3; b6; b7C;
Page 22 ~ b3; b6; b7C;
Page 23 ~ b3; b6; b7C;
Page 24 ~ b3; b6; b7C;
Page 25 ~ b3; b6; b7C;
Page 26 ~ b3; b6; b7C;
Page 27 ~ b3; b6; b7C;
Page 28 ~ b3; b6; b7C;
Page 29 ~ b3; b6; b7C;
Page 30 ~ b3; b6; b7C;
Page 31 ~ b3; b6; b7C;
Page 32 ~ b3; b6; b7C;
Page 33 ~ b3; b6; b7C;
Page 34 ~ b3; b6; b7C;
Page 35 ~ b3; b6; b7C;
Page 36 ~ b3; b6; b7C;
Page 37 ~ b3; b6; b7C;
Page 38 ~ b3; b6; b7C;
Page 39 ~ b3; b6; b7C;
Page 40 ~ b3; b6; b7C;
Page 41 ~ b3; b6; b7C;
Page 42 ~ b3; b6; b7C;
Page 43 ~ b3; b6; b7C;
Page 44 ~ b3; b6; b7C;
Page 45 ~ b3; b6; b7C;
Page 46 ~ b3; b6; b7C;
Page 47 ~ b3; b6; b7C;
Page 48 ~ b3; b6; b7C;
Page 49 ~ b3; b6; b7C;
Page 50 ~ b3; b6; b7C;
Page 51 ~ b3; b6; b7C;
Page 52 ~ b3; b6; b7C;
Page 53 ~ b3; b6; b7C;
Page 54 ~ b3; b6; b7C;

Page 56 ~ b3; b6; b7C;
Page 58 ~ b3; b6; b7C;
Page 59 ~ b3; b6; b7C;
Page 60 ~ b3; b6; b7C;
Page 70 ~ b6; b7C;
Page 85 ~ b3; b6; b7C;
Page 87 ~ b3; b6; b7C;
Page 88 ~ b3; b6; b7C;
Page 89 ~ b3; b6; b7C;
Page 102 ~ Duplicate;
Page 103 ~ b3; b6; b7C;
Page 148 ~ b3;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

Complaint Form
FD-71 (Rev. 8-29-74)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases	Character of case
BRUCE PAUL; NATIONAL CSS - VICTIM	FBW(A) - Computer Fraud
	Complainant [redacted]
	Complaint received ☐ Personal ☒ Telephonic Date ~~11/15/80~~ Time ~~7:30p.m.~~
Address of subject [redacted]	Complainant's address and telephone number [redacted]

Subject's Description						
	Race	Sex ☐ Male ☐ Female	Height	Hair	Build	Birth date and Birthplace
	Age		Weight	Eyes	Complexion	Social Security Number
	Scars, marks or other data					

Facts of complaint

Complainant telephonically contacted this office in regards to unauthorized possession of computer entry codes.

[redacted] National CSS, which has one of their offices on route 7, Wilton, Conn. National CSS is a computer sales and leasing company. They operate and have offices across the United States.

Complainant stated that some former employees of National CSS, set up their own business called Guild Inc., This company also does the same type of business as National CSS.

Complainant stated that both companies are in good standing with each other.

According to complainant, Guild Inc., rendered services to a firm in Calf., which later resulted in some disagreement. As a result of this disagreement, Guild Inc., changed the computer access codes for this firms data. Thus they were unable to retrieve their own data. This Calf. firm then hired National CSS to break the new code of Guild Inc., for the retrieval of this firms data. When they did succeed in breaking the new code, they also inadvertently discovered that Guild Inc., had access to computer entry codes that National CSS and the firms they represent had access to.

Duty Agent [redacted] of the New Haven office was advised at 7.40p.m. of this date. He then contacted comp[redacted] regards to thi[redacted]

SEARCHED INDEXED SERIALIZED FILED NOV 5 1980 FBI - NEW HAVEN

Action Recommended
O+A SPC Mark A. Foyil
(Agent) C. 196A-11/19/80
ORIGIN NH
SUPV DCS

196-397-1

FD-340a (Rev. 10-3-77)

(Title) _____

(File No.) 196-397-1A

Item	Date Filed	To be returned Yes	To be returned No		Disposition
1	12/30/8		X	[redacted] obtained by	b3 b6 b7C
				FGJ subpoena Rec'd 12/22/80 by	
				SA [redacted]	
2	4-3-81		✓	w/s RESA [redacted] Re: Summary of	b3
				[redacted] 2-11-81	b6 b7C
3	4-3-81		✓	Original notes re: Bruce Paul 12-16-80	
4	4-3-81		✓	" " " Physical description	
				of 590 Danbury Rd. Ridgefield, CT 12-16-80	
5	4-3-81		✓	Original notes re [redacted] 12-16-80	b6 b7C
6	4-3-81		✓	Original notes re interview of [redacted]	

See Sub 1

196-397-1A

SEARCHED INDEXED
SERIALIZED FILED

DEC 30 1980

FBI—NEW HAVEN

FD-340 REV. (6-14-77)

Field File No. _____

OO and File No. NH 196-397-1A-1

Date Received 12/22/80

From [redacted]

By _____
(NAME OF SPECIAL AGENT)

To Be Returned ☐ Yes Receipt Given ☐ Yes

☒ No

Description:

[redacted]

OBTAINED BY FGJ SUBPOENA

GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO RULE 6(e), Fed. R. Crim. P.

GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO RULE 6(e), Fed. R. Crim. P.

b3
b6
b7C

b3

FD-340 REV. (6-14-77)

Field File No.

CO and File No. 196A 397-1A-2

Date Received 2/11/81

From

(NAME OF CONTRIBUTOR)

(ADDRESS OF CONTRIBUTOR)

By

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Description:

W/S of SA

Re: Summary of

b6
b7C

b3
b6
b7C

FD-340 REV. (6-14-77)

Field File No. _____

CO and File No. NH 196A 347-1A-3

Date Received 12/16/80

From Bruce Paul
(NAME OF CONTRIBUTOR)

West View Trailer
(ADDRESS OF CONTRIBUTOR)

Redgefield, CT

By [redacted]
(NAME OF SPECIAL AGENT)

To Be Returned ☐ Yes ☒ No

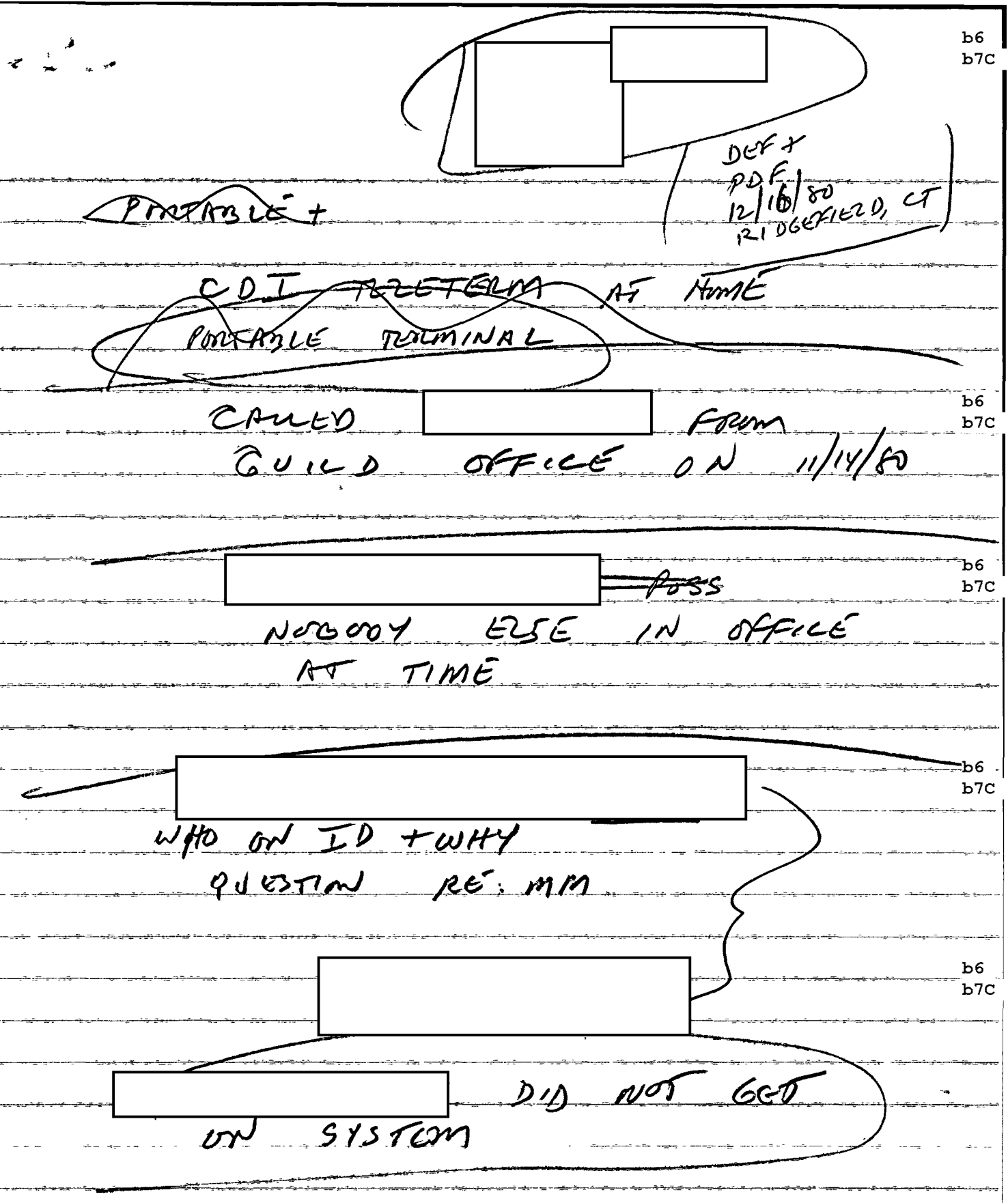
Receipt Given ☐ Yes ☒ No

Description:

Original notes of SA [redacted] Re Interview of Bruce Paul

b6
b7C

b6
b7C


b6
b7C
DEF x
PDF
12/16/80
121 DGEFIELD, CT
PROBABLE +
CDI TELETERM AT HOME
PORTABLE TERMINAL
b6
b7C
CALLED
FROM
GUILD OFFICE ON 11/14/80
b6
b7C
POSS
NOBODY ELSE IN OFFICE
AT TIME
b6
b7C
WHO ON ID + WHY
QUESTION RE: MM
b6
b7C
DID NOT GET
ON SYSTEM

[redacted] - SF OFFICE

b6
b7C

PASCALE COMPILER

NOMAD MODULE

DISK DUMP GUILD ID

AT NYSIS

MAG TAPE BROUGHT OUT

1ST CAROLE WEEKS OCT

29TH FLEW OUT 10/10/80 BACK

M.M.

GUILD RENTAL

NAME BRUCE IVAN PAUL

(AKA) BIPPER

SEX M RACE W

DOB 6/20/54 POB BROOKLYN, N.Y.

HEIGHT 6'1½" WEIGHT 230 BUILD HVY

HAIR BROWN EYES GREEN GLASSES NO

SCARS - RIGHT WRIST 3" LONG BELOW THUMB
- NECK LEFT SIDE APPROX 1"

HOME ADDRESS & TELEPHONE

746-2676
WESTVIEW TRAILS

OCCUPATION - MGR

EMPLOYER GUILD, INC
590 DANBURY, RD
RIDGEFIELD, CT

EDUCATION 1ST YR COLLEGE - ~~UNIV OF~~ EMPIRE STATE COLLEGE
MANHATTEN, NY

MARITAL STATUS MARRIED

[redacted] b6 b7C

SSAN OR CT LIC 123-38-5496

PRIOR ARREST
NO

ASSOCIATES

[redacted] b6 b7C

8-77 TO 7/79

10/79 THRU 4/80

NOMAD SUPPORT -

RELATIONAL DATA BASE MGT SYSTEM

EMPLOYEE SINCE 8/80

CONSULTING PRIOR

DENY MOVE DIRECTORY DATA FILES

ENCRIPTING

MOVE PASCRLE COMPILER OUT

NAMED MODULE OUT

431-0411
2
3
4

PHONE LINES IN DATA LINES
1-4

IN DIRECTORY NAME OF
GUILD

FD-340 REV. (6-14-77)

Field File No. _____

CO and File No. NH 196A 397-IA-4

Date Received 12/16/80

From _____
(NAME OF CONTRIBUTOR)

_____
(ADDRESS OF CONTRIBUTOR)

By [redacted]
(NAME OF SPECIAL AGENT)

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Description:

Original notes of SA [redacted] Re Physical Inspection of 590 Donlon Road Redgrind, CO.

b6
b7C

GUILD

DATA LINES

431 - 0641

438 - 5720

438 - 6688

438 - 2398

dy 12/16/80 PUBLICATIONS

FD-340 REV. (6-14-77)

Field File No. _____

CO and File No. NH 196A 397-1-A-5

Date Received 12/16/80

From [redacted]

By [redacted]

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☐ No

Description:

Original notes of SA [redacted] Re Auto of [redacted]

b6
b7C

(1)

UEF
PDF
12/16/80
RIDGEFIELD, CT

CONSULTANT 3 MONTH

EMPLOYEE APPROX OCT 1980

MEDIA METRICS

PREPARING MAJOR APPLICATIONS
INVOLVING NEWSPAPER ADVERTISING.

[redacted] b6 b7C

FREE USE OF SYSTEM DURING TIME THAT GOULD WAS WORKING ON THE PROGRAMS.

ASSUME SPECIFIC DISK STORAGE AREA b6 b7C

[redacted]

[redacted] HIRED

BAUER PAUL

EMPLOYED ON AN INFREQUENT BASIS

BAUER TOLD OTE PROBLEMS ON MONDAY EXCEPTION NOBODY AT GOULD

[redacted] b6 b7C

[redacted] PASS NO

NCSU

NCSS SYSTEMS DEVELOPMENT CREW

NO KNOWLEDGE OF WHAT NCSS DIRECTORY DATA ~~WERE~~ WAS OUT IN CARY.

NO CURRENT EMPLOYEES WITH EXCEPTION OF BRUCE

OTHER EMPLOYEES NOT NCSS PEOPLE

FD-340 REV. (6-14-77)

Field File No. _____

CO and File No. NH 196A 397-1A-4

Date Received 5/19/81

From [redacted]

By [redacted]
(NAME OF SPECIAL AGENT)

To Be Returned ☐ Yes ☒ No Receipt Given ☐ Yes ☒ No

Description:

Original notes re
Quote of [redacted]

b6
b7C

(1)

5/19/81
SHELTON, CT

b6
b7C

5/26/81

THE GUILD, INC

[redacted]

[redacted]

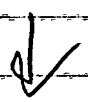
NOW

[redacted]

[redacted]

LEFT FIRM OFFICIALLY

b6
b7C



[redacted]

(2)

ID GUILD EVERYBODY

[redacted] b6 b7C

1½ YR AGO

INTR BY NCSS [redacted]

DESC [redacted]

SOFTWARE FOR USE OF MACHINE FOR DEVELOPMENT PURPOSES

DONE VERBALLY

PRIMARY [redacted] b6 b7C IN CHG.

AIME BRUCE PAUL

HOCKEY

[redacted] b6 b7C - NO BUSINESS RELATIONSHIP

4 PRIV CLASS A, B, C, D.

CLASS B - DEVOL PEOPLE

DIR PAINT

PASSWORD OF ID DIRECTORY

(3)

[redacted] b6 b7C

- CALL IN - THEY SUG CALL NCC WITH DIR DAOR.
ARBITRATE WITH NCC - PROBLEM

12/18/80

CAS

BRUCE

HOW TO GET PAST ELMO
DUNG. DRAGONS CAVE.

PASSWORD FOR DIRECTORY

[redacted] b6 b7C

LOG

DIRPRINT LOG

Bulky Exhibit - Inventory of Property Acquired as Evid
FD-192 (Rev. 4-27-79)

Date: 1-21-81

Title and Character of Case

BRUCE I. PAUL;
NATIONAL CSS, INC. - VICTIM
FBW (A) - COMPUTER CRIME

Date Property Acquired	Source From Which Property Acquired
1-21-81	[redacted] b6 b7C National CSS, Inc., 650 California St, Suite 1840, SF
Location of Property or Bulky Exhibit	Reason for Retention of Property and Efforts Made to Dispose of Same
	Original evidence
To Be Returned: [X] Yes [ ] No	Agent Submitting Property or Exhibit: SA [redacted] Oakland RA
	Agent Assigned Case: SA [redacted] Oakland RA

Description of Property or Exhibit

** NOTE: All items to be returned to National CSS, Inc., San Francisco, when no longer needed as evidence.

1. Memorex brand disk pack, serial #7008291, labeled "TMSPK1"
2. BASF brand magnetic tape #02 164 0 X304 A3 25, labeled "DIRECTORY/ BACKUP ØØØ 117 ENTIRE PACK"
3. BASF brand magnetic tape #12 276 0 A483 A2 07, labeled "TP DUMP GUILD" and "0918".

AND NOTHING ELSE

Seals on items 1, 2, 3 observed to be intact dlf 7/6/81

ITEMS 1B1 + 1B2 WERE RETURNED TO NCSS CORP HEADQUARTERS WILTON, CT PER REQUEST OF [redacted] b6 b7C NCSS, INC.

SEMIANNUAL INVENTORY CERTIFICATION TO JUSTIFY RETENTION OF PROPERTY (Initial and Date)

dlf 7/6/81

Returned to NCSS Wilton, CT dlf

Field File # SF 196A-195

OO: NH 196A-397

NH-397-1B1

SEARCHED INDEXED
SERIALIZED FILED
JUL 06 1981
FBI — NEW HAVEN

Bulky Exhibit - Inventory of Property Acquired as Evidence
FD-192 (Rev. 4-27-79)

Date: 1-7-81

Title and Character of Case

BRUCE I. PAUL;
NATIONAL CSS, INC. - VICTIM
FBW (A) - COMPUTER CRIME

Date Property Acquired	Source From Which Property Acquired
1-6-81	

b6
b7C

Location of Property or Bulky Exhibit	Reason for Retention of Property and Efforts Made to Dispose of Same
	Original evidence

To Be Returned	Agent Submitting Property or Exhibit	Agent Assigned Case
[XX] Yes [ ] No	SA [redacted] Oakland RA FBW	SA [redacted] Oakland RA

Description of Property or Exhibit

** NOTE: All items to be returned to National CSS, Inc., San Francisco, when no longer needed as evidence.

1. ✓ Terminal Log created by [redacted] for period 2:58 PM - 3:23 PM, 11-14-80. b6 b7C
2. ✓ Terminal Log for period 3:27 PM - 3:47 PM, 11-14-80, of activity between terminal using the Guild ID and Mediametrics computer.
3. ✓ Terminal Log for period 4:15 PM - 4:51 PM, 11-14-80, of activity between terminal using the Guild ID and Mediametrics computer.
4. ✓ Terminal Log for period 4:44 PM - 4:52 PM, 11-14-80, of activity between terminal using the Guild ID and Mediametrics computer.
5. ✓ Terminal Log for period 4:57 PM - 5:00 PM, 11-14-80, of activity between terminal using the Guild ID and Mediametrics computer.
6. ✓ Printout entitled "Inventory Guild" created 4:46 PM, 11-13-80.
7. ✓ Printout entitled "Inventory Guild" created 4:07 PM, 11-13-80.
8. ✓ Printout entitled "DIRDATA" created 5:26 PM, 11-20-80.
9. ✓ Printout entitled "DIRDATA" created 4:35 PM, 11-20-80.
10. ✓ Printout entitled "DIRDATA" created 5:35 PM, 11-20-80.
11. ✓ Terminal Log created starting 6:16 PM, 11-20-80, between terminal and National CSS computer SFR-1.
12. ✓ Two page portion of "DIRDATA" printout created 8:03 AM, 11-15-80.
13. ✓ One continuous printout containing (a) 95 page listing of NCSS IDs, passwords, and other data created at 5:35 PM, 11-13-80, (b) terminal log for period 4:54 PM - 5:39 PM, 11-13-80, of activity between terminal using the Guild ID and Mediametrics computer, and (c) terminal log for period 5:40 PM (no ending time), 11-13-80, for same activity.
14. ✓ Mediametrics system console logs for period 11:58 AM, 11-10-80 to 3:32 PM, 11-19-80.

SEMIANNUAL INVENTORY CERTIFICATION TO JUSTIFY RETENTION OF PROPERTY (Initial and Date)

Returned to NCSS Walton, CA 3/20/83 dlf

196-397-182

SEARCHED ___ INDEXED ___
SERIALIZED IC FILED IC
JUL 06 1981
FBI — NEW HAVEN

1 dlf

FBI/DOJ

Field File # SF 196A-795

OO: NH 196A-397

Bulky Exhibit - Inventory of Property Acquired as Evidence
FD-192 (Rev. 4-27-79)

Date: 5-26-81

Title and Character of Case

BRUCE IVAN PAUL;
NATIONAL CSS, INC. - VICT
FBW (A) - COMPUTER FRAUD

Date Property Acquired	Source From Which Property Acquired
5-26-81	Mediametrics, Inc., 1620 School St., Moraga, CA

b6
b7C

Location of Property or Bulky Exhibit	Reason for Retention of Property and Efforts Made to Dispose of Same
	Original Evidence

To Be Returned	Agent Submitting Property or Exhibit	Agent Assigned Case
[X] Yes [ ] No	SA [redacted] Oakland RA	SA [redacted] Oakland RA

Description of Property or Exhibit

1. One continuous printout representing Mediametrics system console log for period from 5:28 PM, 9-20-80, to 11:49 AM, 9-27-80.
AND NOTHING ELSE

Returned to SF via A/T dtd 3/23/83 dmj

SEMIANNUAL INVENTORY CERTIFICATION TO JUSTIFY RETENTION OF PROPERTY (Initial and Date)

Field File # SF 196A-795

OO: NH 196A-397

196-397-183

SEARCHED INDEXED
SERIALIZED FILED
JUL 06 1981
FBI — NEW HAVEN

Bulky Exhibit - Inventory of Property Acquired as Evidence
FD-192 (Rev. 4-27-79)

Date: 1-16-81

Title and Character of Case

BRUCE I. PAUL;
NATIONAL CSS, INC. - VICT
FBW (A) - COMPUTER FRAUD

Date Property Acquired	Source From Which Property Acquired
1-13-81	Mediametrics, Inc., 1620 School St., Moraga, CA

b6
b7C

Location of Property or Bulky Exhibit	Reason for Retention of Property and Efforts Made to Dispose of Same
	Original evidence

To Be Returned	Agent Submitting Property or Exhibit	Agent Assigned Case
[X] Yes [ ] No	SA Oakland RA	SA Oakland RA

Description of Property or Exhibit

1. One continuous printout from Mediametrics printer of 55 items starting at 17:33:26, 11-15-80 to approx 18:10:06, 11-15-80.
2. One continuous printout measuring approximately 4½" high from Mediametrics printer of 242 items starting at 18:05:45, 11-15-80 to 18:17:55, 11-15-80.

Returned to SF w/ii A/T dtd 3/23/83 dj

SEMIANNUAL INVENTORY CERTIFICATION TO JUSTIFY RETENTION OF PROPERTY (Initial and Date)

196-397-1B4

Field File # SF 196A-795

OO: NH 196A-397

SEARCHED ____ INDEXED ____
SERIALIZED ____ FILED ____
JUL 06 1981
FBI — NEW HAVEN

196-397-2

196-397-3

SEARCHED X INDEXED X
SERIALIZED X FILED X
DEC [illegible] 1960
FBI—NEW HAVEN

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:	PRECEDENCE:	CLASSIFICATION:
☑ Teletype	☐ Immediate	☐ TOP SECRET
☐ Facsimile	☐ Priority	☐ SECRET
☐ _____	☑ Routine	☐ CONFIDENTIAL
		☐ UNCLAS E F T O
		☑ UNCLAS

Date 12/3/80

FM NEW HAVEN (196A-~~3791~~) (P) 397 & Note Chang

TO SAN FRANCISCO ROUTINE

BT

UNCLAS

BRUCE I. PAUL; NATIONAL CSS, INC. - VICTIM; FBW (A) - COMPUTER FRAUD; OO: NH.

NATIONAL CSS, INC.(NCSS) IS AN INTERNATIONALLY KNOWN COMPUTER SERVICES FIRM WITH HEADQUARTERS LOCATED AT 187 DANBURY RD., WILTON, CONN. NCSS PROVIDES SALES AND SERVICE OF ITS OWN SOFTWARE, MAINFRAME AND PERIPHERAL EQUIPMENT, AS WELL AS ACCESS TO A NATIONAL TELECOMMUNICATIONS NETWORK WHICH LINKS TWO NCSS MAINFRAME COMPUTERS AT STAMFORD, CONN. TO AN NCSS MAINFRAME IN SUNNYVALE, CALIFORNIA.

NCSS MAINTAINS AND CREATES DAILY A HIGHLY SENSITIVE FILE CALLED "CDIR DATA" FOR USERS OF EACH MAINFRAME. THE CDIR DATA FILE FOR EACH LOCATION CONTAINS:

1) USER IDENTIFICATION NAMES; 2) LOG IN PASSWORDS; 3) ACCOUNT NUMBER; 4) LIST OF RESOURCES AVAILABLE; 5) READ PASSWORDS; 6) WRITE PASSWORDS.

196-397-6

1-NEW HAVEN

DEF/pen pen

VIA ENCIPHERED TELETYPE

b6
b7C

Approved: _____ Transmitted 002 21032 Per _____
(Number) (Time)

SEARCHED.....
SERIALIZED.....
INDEXED.....
FILED.....

FBI/DOJ

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:	PRECEDENCE:	CLASSIFICATION:
☐ Teletype	☐ Immediate	☐ TOP SECRET
☐ Facsimile	☐ Priority	☐ SECRET
☐ _____	☐ Routine	☐ CONFIDENTIAL
		☐ UNCLAS E F T O
		☐ UNCLAS

Date _____

IF THE CDIR DATA FILES FOR ALL THREE MAINFRAME LOCATIONS WERE COMBINED, ACCESS TO ANY BYTE OF INFORMATION STORED ON-LINE IN THE NETWORK COULD BE OBTAINED. NCSS CUSTOMERS INCLUDE SEVERAL MAJOR BANKS AND LARGE CORPORATIONS BASED IN THE UNITED STATES AND EUROPE. THE CODE NAME AND LOCATION FOR EACH NCSS MAINFRAME FOLLOWS:

CODE NAME:	LOCATION:
H-SYS	485 SUMMER ST. STAMFORD, CONN.
EAST	1351 WASHINGTON BOULEVARD STAMFORD, CONN.
SUNY	530 PASTORIA BOULEVARD SUNNYVALE, CALIFORNIA

ENTRY TO THE TELECOMMUNICATIONS NETWORK CAN BE GAINED ANYWHERE IN THE COUNTRY SIMPLY BY USING A PORTABLE TERMINAL WITH A TELEPHONE INTERFACE.

BRUCE I. PAUL WORKED FOR NCSS FROM AUG. 1977 TO APRIL 18, 1980, WITH ONE SHORT BREAK IN SERVICE. PAUL WAS A SYSTEM PROGRAMMER WHO HAD RESPONSIBILITY TO DEVELOP SOFTWARE TO CHECK

Approved: _____ Transmitted _____ (Number) _____ (Time) Per _____

FBI/DOJ

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:
- ☐ Teletype
- ☐ Facsimile
- ☐ _____

PRECEDENCE:
- ☐ Immediate
- ☐ Priority
- ☐ Routine

CLASSIFICATION:
- ☐ TOP SECRET
- ☐ SECRET
- ☐ CONFIDENTIAL
- ☐ UNCLAS E F T O
- ☐ UNCLAS

Date _____

THE VALIDITY AND INTEGRITY OF ALL ON-LINE DATA. THE JOB REQUIRED PAUL TO HAVE ACCESS TO ALL CUSTOMER DATA.

MOST RECENTLY PAUL WAS WORKING EITHER FOR OR WITH A SOFTWARE DEVELOPMENT GROUP KNOWN AS "THE GUILD INC." (GUILD). SEVERAL MONTHS AGO, THE GUILD SIGNED A CONTRACT WITH MEDIAMETRICS, INC. (MM), 1620 SCHOOL ST., MORAGA, CALIFORNIA, TO DEVELOP CERTAIN SOFTWARE PACKAGES. AS PART OF THE AGREEMENT, MM ALLOTTED CERTAIN DISK STORAGE SPACE TO GUILD TO AID IN THE SOFTWARE DEVELOPMENT. ACCESS TO THE DISK STORAGE SPACE CAN BE GAINED FROM ANYWHERE IN THE COUNTRY AS LONG AS THE MM SYSTEM IS ON-LINE WITH THE NCSS SUNY UNIT. THIS IS GENERALLY 7 A.M. TO 12 MIDNIGHT PACIFIC TIME.

[redacted] OF MM, BECAME UNSATISFIED WITH THE GUILD'S PROGRAMMING EFFORTS APPROXIMATELY ONE MONTH AGO. [redacted] THEN ATTEMPTED TO FIND OUT EXACTLY WHAT GUILD WAS USING THE DISK STORAGE FOR. [redacted] THEN FOUND THAT HE WAS UNABLE TO GAIN ACCESS TO THE DISK STORAGE SPACE BECAUSE GUILD HAD APPLIED ADDITIONAL SECURITY MEASURES TO THE ACCESSING ROUTINE. [redacted] THEN HIRED NCSS PERSONNEL TO BREAK INTO THE DISK

b6
b7C

Approved: _____ Transmitted _____ (Number) _____ (Time) Per _____

FBI/DOJ

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:
- ☐ Teletype
- ☐ Facsimile
- ☐ _____

PRECEDENCE:
- ☐ Immediate
- ☐ Priority
- ☐ Routine

CLASSIFICATION:
- ☐ TOP SECRET
- ☐ SECRET
- ☐ CONFIDENTIAL
- ☐ UNCLAS E F T O
- ☐ UNCLAS

Date _____

397

PAGE FOUR NH 196A-379 UNCLAS

STORAGE SPACE ON THE MM SYSTEM ALLOTTED FOR THE GUILD'S WORK.

ON THE MORNING OF NOV. 14, 1980, NCSS EMPLOYEE [redacted] b6 b7C

[redacted] SUCCESSFULLY PENETRATED THE DISK STORAGE SPACE ALLOTTED TO THE GUILD. ELEMENTS OF THE THREE CDIR DATA FILES CONTAINING NCSS CUSTOMER DATA WAS FOUND IN THE STORAGE AREA. A PARTIAL HARD COPY PRINTOUT OF THE DATA WAS OBTAINED AT THE TIME. A SHORT TIME LATER, THE DATA IN THE STORAGE AREA WAS SCRAMBLED THROUGH COMMANDS WHILE THE MM SYSTEM WAS ON-LINE WITH NCSS SUNY.

ON APPROXIMATELY NOV. 15, 1980, NCSS NOTIFIED ALL OF ITS CUSTOMERS OF A PROBLEM INVOLVING A POTENTIAL COMPROMISE OF SYSTEM ACCESS SECURITY. NCSS THEN URGED ALL CUSTOMERS TO IMMEDIATELY CHANGE ALL PASSWORDS USED TO ACCESS THE NCSS NETWORK.

IT IS POSSIBLE THAT PAUL OR SOME OTHER FORMER NCSS EMPLOYEE OBTAINED THE DATA CONTAINED IN THE CDIR DATA FILE. THE INFORMATION COULD HAVE BEEN OBTAINED AND TRANSMITTED TO THE MM FACILITY IN THREE WAYS:

Approved: _____ Transmitted _____ (Number) _____ (Time) Per _____

FBI/DOJ

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:
☐ Teletype
☐ Facsimile
☐ _____

PRECEDENCE:
☐ Immediate
☐ Priority
☐ Routine

CLASSIFICATION:
☐ TOP SECRET
☐ SECRET
☐ CONFIDENTIAL
☐ UNCLAS E F T O
☐ UNCLAS

Date _____

PAGE FIVE NH 196A-~~379~~ 392 UNCLAS

ONE: PENETRATION AND TRANSFER THROUGH THE NETWORK.

TWO: OBTAINING THE DATA WHILE AN EMPLOYEE, THEN SENDING THE DATA BY MAIL (MAGNETIC TAPE) TO THE MM FACILITY.

THREE: OBTAINING THE DATA WHILE AN EMPLOYEE AND HAND CARRYING THE DATA (MAGNETIC TAPE) TO THE MM FACILITY.

SAN FRANCISCO IS REQUESTED TO ASSIGN THE FOLLOWING LEADS TO AN AGENT WHO HAS ATTENDED THE BUREAU COMPUTER FRAUD IN-SERVICE. IT IS REQUESTED THESE LEADS BE HANDLED EXPEDITIOUSLY.

SAN FRANCISCO, AT MORAGA, CALIF.: INTERVIEW [redacted] b6 b7C [redacted] MEDIAMETRICS, INC., 1620 SCHOOL ST., MORAGA, CALIF. AND ASCERTAIN THE FOLLOWING:

1) DETAILS OF AGREEMENT WITH GUILD, INC. FOR SOFTWARE DEVELOPMENT.

2) REASONS FOR HIRING NCSS TO PENETRATE SPACE ASSIGNED TO GUILD.

3) EXACT ADDRESS OF DISK STORAGE SPACE ASSIGNED TO GUILD.

AT SAN FRANCISCO, CALIF.: INTERVIEW [redacted] b6 b7C [redacted] AT NCSS OFFICE, 650 CALIFORNIA ST., SAN FRANCISCO, TELEPHONE [redacted] AND ASCERTAIN THE FOLLOWING:

Approved: _____ Transmitted _____ (Number) _____ (Time) Per _____

FBI/DOJ

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:
- ☐ Teletype
- ☐ Facsimile
- ☐ _____

PRECEDENCE:
- ☐ Immediate
- ☐ Priority
- ☐ Routine

CLASSIFICATION:
- ☐ TOP SECRET
- ☐ SECRET
- ☐ CONFIDENTIAL
- ☐ UNCLAS E F T O
- ☐ UNCLAS

Date _____

PAGE SIX NH 196A-379 UNCLAS

1) COMPLETE DETAILS OF MM SYSTEM, I.E. HARDWARE TYPE TERMINALS, ACCESS LINES TO NCSS SUNY MAINFRAME.

2) EXACT CIRCUMSTANCES THAT THEY WERE HIRED TO PENETRATE GUILD DISK SPACE.

3) OBTAIN ANY AND ALL EVIDENCE AVAILABLE (HARD COPY, MAGNETIC DISC, LOGS SHOWING ENTRY TO SYSTEMS).

4) ANY OTHER PERTINENT INFORMATION.

NEW HAVEN, AT WILTON, CONN.: INVESTIGATION CONTINUING AT WILTON, CONN.

BT

#

Approved: _____ Transmitted _____ (Number) _____ (Time) Per _____

FBI/DOJ

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription December 31, 1980

1.

[redacted] b6 b7C was advised of the official identity of the interviewing agents and the nature of the interview. He, thereafter, provided the following information:

He has employed Bruce Paul as an employee since approximately October 1980. Prior to that time he employed Paul on a consulting basis for about three months. Paul has been involved in preparing major application programs involving newspaper advertising for Mediametrics (MM) of Moraga, California.

He is not familiar with the exact details involving the agreement between The Guild and MM as the agreement was worked out by a [redacted] b6 b7C He was aware of the fact that The Guild has free use of the MM System during the time that the Guild was working on the application programs. He assumes that specific disk storage area was set aside for Guild use by MM. [redacted] the Guild, the operation was run by [redacted] initially hired Bruce Paul. At that time [redacted] was employed on an infrequent basis.

He was not aware of any problem involving MM until he was told about the problems by Paul on Monday, November 17, 1980.

It was his opinion that nobody employed at The Guild had the high level of knowledge regarding the National CSS System that Bruce Paul did. The only individuals who could match Paul's expertise would be someone from the NCSS Systems Development crew.

He had no knowledge of what NCSS Directory Data was maintained on The Guild storage space at MM.

Interviewed on 12/16/80 at Ridgefield, Connecticut File # NH 196A-397 - 8

by SA [redacted] SA [redacted] DEF / sab Date dictated 12/23/80 b6 b7C

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription December 31, 1980

1.

Bruce Ivan Paul, residence Westview Trails, New Fairfield, Connecticut, was interviewed at the place of his employment, The Guild, Inc., 590 Danbury Road, Ridgefield, Connecticut. He was advised of the identity of the interviewing agents and the nature of the interview. He, thereafter, provided the following information.

He was employed by National CSS, Inc. from August 1977 to July 1979 and October 1979 through April 1980. His last position with National CSS (NCSS) was that of a programmer in the Nomad Support Unit - Relational Data Base Management System. From April 1980 until August of 1980 he did consulting work in the Computer Field. He has been employed by The Guild, Inc. since August 1980, as a full time employee.

As it is necessary for him to use a computer terminal in his work he maintains a portable C.D.I. Teleterm Terminal at his home.

He is familiar with [redacted] Mediametrics (MM) of Moraga, California, as he has been involved in programming work for MM for several months. Between September 29 and October 10, 1980, he flew out to MM to resolve some programming problems. At that time he brought with him a magnetic tape containing a "Pascale Compiler" and a "Nomad" module. It was his impression that The Guild had a rental agreement with National CSS to use both the Pascale Compiler and the Nomad Module. He made several attempts to get the Nomad Module working on the MM System. He was, however, unable to do so and discontinued further efforts at implementing Nomad.

b6
b7C

On November 14, 1980, he was working late at The Guild Office on various MM problems. At the time there was no one else in The Guild Office. When he attempted to go on-line to the MM System through the NCSS Telecommunications Network he found that someone was already on the system using the Guild I. D. He then sent a message from terminal to terminal to the effect of "From Bipper/Guild: Who the hell is this!" After getting no response he called [redacted] at MM to find out who was on

b6
b7C

Interviewed on 12/16/80 at Ridgefield, Connecticut File # NH 196A-397 - 9

b6
b7C

by SA [redacted] DEF / sab Date dictated 12/23/80

the system. [redacted] did not answer his questions fully so he called [redacted] in NCSS San Francisco Office. [redacted] also could not answer his questions. He later found out that he could not enter the MM System because [redacted] discontinued Guild access. b6 b7C

He denied transferring or causing the transfer of four "CDIR Data" files to disk space allotted to The Guild on the MM System. He also denied encrypting all data stored by The Guild on the MM System on November 15, 1980.

He initially agreed to take a polygraph test regarding all information he had provided. He then indicated that he thought he was being set up, however, he did not want to accuse anyone else without proof. He indicated that [redacted] did have all access codes and could have provided them to anyone. He then indicated that he did not want to take a polygraph test. He decided that it might be best if he did not make any more statements until talking to an attorney. The interview was, thereafter, discontinued. b6 b7C

The following information was obtained by observation and interview.

Name:	Bruce Ivan Paul
AKA:	Bipper
Sex:	Male
Race:	White
Date of Birth:	June 20, 1954
Place of Birth:	Brooklyn, New York
Height:	6'½" tall
Weight:	230
Build:	Heavy
Hair:	Brown
Eyes:	Green
Scars:	Right wrist - 3" long below thumb left side neck approximately 1" long.
Home Address:	West View Trails New Fairfield, Connecticut
Telephone:	746-2676
Occupation:	Manager
Employer:	Guild, Inc. 590 Danbury Road Ridgefield, Connecticut
Education:	Empire State College Manhattan, New York - one year

[redacted] b6 b7C

SSAN: 123-38-5496
Prior Arrest: None admitted

[redacted] b6 b7C

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription December 31, 1980

1.

Physical inspection of the premises occupied by The Guild, Inc., 590 Danbury Road, Ridgefield, Connecticut, determined that the following telephonic data lines were being used:

1. 431-0641
2. 438-5720
3. 428-6688
4. 438-2398

Interviewed on 12/16/80 at Ridgefield, Connecticut File # NH 196A-397-10

by SA [redacted] DEF / sab Date dictated 12/23/80

b6
b7C

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription February 4, 1981

1.

[redacted] National CSS, Inc., 187 Danbury Road, Wilton, Connecticut, telephone number [redacted] was advised of the identity of the interviewing agent and the nature of the interview. He, thereafter, provided an event report as of January 21, 1981 08:45:30. A copy of the report is attached hereto.

b6
b7C

Interviewed on 1/21/81 at Wilton, Connecticut File # NH 196A-397-11

by SA [redacted] dsf / sab Date dictated 1/28/81

b6
b7C

EVENT REPORT AS OF 01/21/81 08:45:30

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 JAN 02	ID GUILD put up on HSYS.	[redacted] b6 b7C
1980 APR 15 16:55:39	Userid [redacted] LINKs to disk GUILD on HSYS. There are other instances of this in April 1980.	The Security log (SECSERV) from April 1980.
1980 APR 15 19:17:22	Userid [redacted] LINKs to disk VERIFY on HSYS.	Security log (SECSERV) from April 1980.
1980 APR 23 19:49:16	Userid [redacted] LINKs disk NOMCLECT on NCS1.	The Security log (SECSERV) from April 1980.
1980 APR 24	ID GUILD2 put up on HSYS.	[redacted] b6 b7C
1980 MAY 12 18:27:33	[redacted] on NCS1 got password of [redacted] on NCS1, giving reason as [redacted]	DIRPRINT log on NCS1. [redacted] says he never used DIRPRINT.
1980 MAY 12 18:30:40	[redacted] on NCS1 tried to use DIRPRINT but failed due to invalid arguments. Reason was [redacted] Arguments were "VERIFY PASSWORD". Userid being asked about was "ooooo£AS", where "o" probably is a control character.	DIRPRINT log on NCS1. [redacted] says he never used DIRPRINT.
1980 MAY 12 18:31:52	[redacted] on NCS1 got password for VERIFY on EAST, giving reason as [redacted]	DIRPRINT log from EAST. [redacted] says he never used DIRPRINT.
1980 JUN 12	ID GUILD3 put up on HSYS with 200 cyl. mountable mini.	[redacted] b6 b7C
1980 JUN 21	The directory information found on userid GUILD (AIMS) on 11/13 and 11/14 in file HSYS CRDATA are from 6/21 to 6/23/80 HSYS.	[redacted] determines these date by refering to customer records for userids created before, after, and during this time period.
1980 JUN 23 15:15:31	[redacted] on NCS1 got password for NOMCLECT on NCS1, giving reason as "etst".	DIRPRINT log on NCS1. [redacted] says he never used DIRPRINT.
1980 JUN 23 20:04:45	SUPPORTH logs into HSYS from NCS1 port 022, attaches BACKUP, VERIFY, and a TEMP20, uses Nomad, and logs out at 20:07:16.	HSYS billing data.
1980 JUN 24	The directory information in the EAST CRDATA files found on userid GUILD on AIMS are from 6/24/80 EAST system.	[redacted] determines this date by using the customer records for userids created before, after, and on this date. b6 b7C
1980 JUN 24 08:08:05	SUPPORTM logged in to EAST from port 022 on NCS1.	EAST billing records.
1980 JUN 24 08:09:12	SUPPORTM on EAST attached BACKUP as T-disk.	EAST billing records.

EVENT REPORT AS OF 01/21/81 08:47:37

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 JUN 24 08:09:24	SUPPORTM on EAST attached VERIFY as U-disk.	EAST billing records.
1980 JUN 24 08:09:34	SUPPORTM on EAST attached TEMP20 as P-disk.	EAST billing records.
1980 JUN 24 08:11:05	Spool file 24081105 produced by SUPPORTM on EAST.	EAST billing records. L-type records show this file at 08:14:36.
1980 JUN 24 08:11:29	SUPPORTM logged off EAST, selio=X'388', mpxio=X'891'.	EAST billing records.
1980 JUN 24 08:14:36	Spool file 24081105 transfered to GUILD on HSYS. Number of cards is X'891'=2193.	EAST billing records.
1980 JUN 26	ID GUILD3 taken down on HSYS.	[redacted] b6 b7C
1980 JUN 27	The directory information found in the file SUNY CRDATA on userid GUILD on AIMS are from this day 6/27/80 SUNY.	[redacted] determines this date by using customer records for userids create before, after, an on this date.
1980 JUN 27 08:35:47	VERIFY logged in to SUNY from port 024 on NCS1.	SUNY billing records. (Time is SUNY time.)
1980 JUN 27 08:38:20	Spool file 27083820 produced by VERIFY on SUNY.	SUNY billing records. L-type records show this file at 08:41:26.
1980 JUN 27 08:38:50	VERIFY logged off SUNY, selio=X'1FF', mpxio=X'463'.	SUNY billing records.
1980 JUN 27 08:41:26	Spool file 27083820 transfered to GUILD on HSYS. Number of cards is X'463'=1123.	SUNY billing records.
1980 JUN 29	Backup tape made on this day contains a backup of userid VERIFY, formerly used by Bruce Paul. There is a file on this disk called BIPUSER CRDATA and it contains the same format file found on the userid GUILD on AIMS. The data is not the same.	Backup tape 6H007 from HSYS created on 6/29/80. Supplied by [redacted] b6 b7C
1980 JUL 08	Port numbers for the Danbury area are changed to: 36B, 359, 357, 352, 364, 363. They all are connected to NCS1. Prior to this day, the port numbers are: 022 thru 027, inclusive and all are connected to NCS1.	Data Communications Dept. [redacted]
1980 JUL 10	ID GUILD3 put up on HSYS with 1 cyl online.	[redacted] b6 b7C
1980 JUL 15	Three spool files shipped from HSYS to AIMS machine: The spool file names are: 10125448,	Information from [redacted] In file folder.

EVENT REPORT AS OF 01/21/81 08:49:46

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 JUL 15	10125526, 10125552	
1980 JUL 16 11:48:40	Userid VERIFY LINKs userid BACKMC P disk.	Security log (SECSERV) from July 1980.
1980 JUL 18	Two spool files from HSYS to AIMS machine: spool file names are: 18100827, 18123459.	Information from [redacted] In file folder. b6 b7C
1980 JUL 21	4 spool files went from HSYS to AIMS on this day. 3 of them were created this day from userid GUILD on HSYS. They are: 21145941, 21145951, & 21150002. The 4 th file was created on 7/18/80 and is 18123459.	Detail billing records from tape of 7/21/80 HSYS data. [redacted] supplied this information.
1980 JUL 21 14:59:41	Spool file 21145941 sent by GUILD on HSYS to GUILD on AIMS, apparently containing HSYS directory information.	Billing records provided by [redacted] show this file being transmitted at 18:32:45. The size is X'75B'=1883 cards, which corresponds to the size of HSYS CRDATA found on AIMS (4996 30-byte records -> 188 blocks).
1980 JUL 21 14:59:51	Spool file 21145951 sent by GUILD on HSYS to GUILD on AIMS, apparently containing the EAST directory information.	Billing records provided by [redacted] show this file being transmitted at 18:54:44. The size is X'891'=2193 cards, which corresponds to the EAST CRDATA file found on AIMS (5819 30-byte records -> 219 blocks).
1980 JUL 21 15:00:02	Spool file 21150002 sent by GUILD on HSYS to GUILD on AIMS, apparently containing the SUNY directory information.	Billing records provided by [redacted] show this file being transmitted at 19:00:06. The size is X'463'=1123 cards, which corresponds to the size of the SUNY CRDATA found on AIMS (2984 30-byte records -> 112 blocks).
1980 JUL 23	ID EAGLE put up on HSYS.	[redacted]
1980 JUL 23 13:13:28	[redacted] on NCS1 got password of [redacted] on NCS1, giving reason as "debugging".	DIRPRINT log on NCS1. b6 b7C
1980 JUL 23 13:15:23	[redacted] on NCS1 got password of [redacted] on NCS1. Reason was "debugging a problem".	DIRPRINT log on NCS1.
1980 JUL 23 13:21:25	[redacted] on NCS1 got password of VERIFY on HSYS, giving reason as ".".	DIRPRINT log of HSYS. [redacted] says he never used DIRPRINT.
1980 JUL 23 13:22:38	[redacted] on HSYS got password of BACKUPTA on NCS1, giving reason as ";".	DIRPRINT log on NCS1.
1980 JUL 24	Three spool files from HSYS to AIMS machine: Spool file names: 21150002, 2145941, 21145951	Information from [redacted] In file folder. b6 b7C

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 JUL 31	IDs GUILD2 and GUILD3 taken down on HSYS.	[redacted]
1980 AUG 07 14:41:55	[redacted] on NCS1 got password of [redacted] on NCS1, giving reason as "+".	DIRPRINT log on NCS1.
1980 AUG 07 15:10:42	[redacted] on NCS1 got password of BACKUPTA on NCS1, giving reason as "+".	DIRPRINT log on NCS1.
1980 AUG 26	Userid [redacted] LINKs userid BACKUP on SUNY 8 times. Access is made to the P T V disks.	Security log (SECSERV) from August 1980.
1980 AUG 26 11:21:43	[redacted] on NCS1 got password of [redacted] on NCS1, giving reason as ".".	DIRPRINT log on NCS1.
1980 AUG 26 11:22:36	[redacted] on NCS1 got password of BACKUPT9 on NCS1, giving reason as ".".	DIRPRINT log on NCS1.
1980 AUG 26 11:23:05	[redacted] on NCS1 got password of BACKUPT9 on NCS1, giving reason as ".".	DIRPRINT log on NCS1.
1980 SEP 18	LINKs from userid [redacted] to: BACKUP P disk on HSYS; HSL on HSYS; VERIFY P, T, U disks on EAST.	Security log (SECSERV) from September 1980.
1980 SEP 18 16:14:09	[redacted] on NCS1 got password of BACKUPMA on EAST, giving reason of ".".	DIRPRINT log from EAST. According to DMG, CSSPFR should not have been in use at this time.
1980 SEP 18 16:15:16	[redacted] on NCS1 got password of BACKUPTA on NCS1, giving reason as "/".	DIRPRINT log on NCS1.
1980 SEP 24	ID GUILD taken down on HSYS.	[redacted]
1980 OCT 10	Shadow [redacted] of userid [redacted] LINKs userid BACKUP P disk.	security log (SECSERV) from October 1980.
1980 OCT 10 16:39:04	Someone with LOGONID of [redacted] on NCS1 tried to get password of [redacted] on EAST, giving reason of "../.", but failed due to insufficient privilege ([redacted] is not a class B userid).	DIRPRINT log from EAST.
1980 OCT 10 16:41:46	Someone with LOGONID of [redacted] on NCS1 asked for password of [redacted] on NCS1, but failed due to insufficient privilege (there is no class B ID called [redacted].	DIRPRINT log on NCS1.

b6
b7C

b6
b7C

EVENT REPORT AS OF 01/21/81 08:54:28

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 OCT 15	Shadow [ ] of userid [ ] LINKs to userid [ ] and [ ]	Security log (SECSERV) from October 1980
1980 OCT 15 14:50:09	[ ] on NCS1 got password of [ ] on NCS1, giving reason as "dtm retrieval".	DIRPRINT log on NCS1.
1980 OCT 16 10:44:58	[ ] on EAST got password for BACKUPBD on EAST, giving reason as "aaaaaa".	DIRPRINT log on EAST.
1980 OCT 22	Shadow [ ] of userid [ ] on NCS1 LINKs userid [ ] 6 times within a minute or two.	Security log (SECSERV) from October 1980.
1980 NOV 11 07:32:47	Someone with LOGONID of [ ] logged in to NCS1 from port 36B for about five minutes.	NCS1 ALTOP log.
1980 NOV 11 07:37:32	Eight seconds after logoff of [ ] login from port 36B to VPSYSMGR on MML1, for 17 minutes.	NCS1 ALTOP log shows port. MML1 ALTOP log (checked by [ ] shows login on MML1 at 4:37:49 (time difference 17 seconds). MML1 ALTOP log also shows a SNAP "NMSPKTRD" for VPSYSMGR.
1980 NOV 11 07:54:24	Fifteen seconds after logout from MML1, port 36B used to login with LOGONID [ ] on NCS1, for 11 minutes.	NCS1 ALTOP log.
1980 NOV 11 08:04:26	Someone with LOGONID of [ ] on NCS1 tried to get password of [ ] on NCS1, giving reason as "vvv". Failed because [ ] is not a class B ID.	DIRPRINT log on NCS1.
1980 NOV 11 08:05:29	Eight seconds after logoff of [ ] login of [ ] on NCS1 from port 36B, for one minute.	NCS1 ALTOP log.
1980 NOV 11 08:06:06	[ ] on NCS1 got password of BACKMC on NCS1, giving reason as ".".	DIRPRINT log on NCS1.
1980 NOV 11 08:06:29	Ten seconds after logoff of [ ] login of [ ] on HSYS from port 36B, for four minutes.	NCS1 ALTOP log shows port being used. HSYS ALTOP log shows login at 8:07:17 (time difference 48 seconds).
1980 NOV 11 08:10:48	Eight seconds after use with HSYS, port 36B used to login or attempt login on SUNY, total time 24 seconds.	NCS1 ALTOP log.
1980 NOV 11 08:11:23	Eleven seconds after previous use, port 36B used to login or attempt login on SUNY, total time 1 minute 31 seconds.	NCS1 ALTOP log.
1980 NOV 11 08:13:02	Eight seconds after previous use, port 36B used to login on SUNY, total time 21 minutes.	NCS1 ALTOP log.

b6
b7C

EVENT REPORT AS OF 01/21/81 08:57:00

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 NOV 11 08:34:47	Nine seconds after previous use, port 36B used to login to EAGLE on HSYS.	NCS1 ALTOP log shows port used to access HSYS. HSYS ALTOP log shows login by EAGLE at 8:35:35 (time difference 48 seconds).
1980 NOV 13 12	Time approximate. [redacted] (AIMS) calls [redacted] stating he has trouble with GUILD and wants to get out of contract. [redacted] needs passwords and asks [redacted] for them. [redacted] used DPRINT to get password of userid GUILD on AIMS and gives password to [redacted] tried to ATTACH the GUILD disk but got logged off by PROTECT EXEC. [redacted] then tells [redacted] to use LINK command, and explains its use.	Conversation with [redacted] on 11/24/80 and [redacted] b6 b7C
1980 NOV 13 13	Time approximate (not really known by us now). [redacted] logs onto userid GUILD in order to review general contents. Notices file with filetype CRDATA and looks at them. To him they appear to be a list of userids and passwords. Before logging out he adds a SET TLOG command to the PROFILE EXEC on the userid GUILD. This will allow a hardcopy to be made of future login attempts.	Conversation with [redacted] on 11/24/80 with [redacted]
1980 NOV 14 13:00:00	[redacted] (AIMS) calls [redacted] and says "What would you give for the directory?" [redacted] says he found directory on userid GUILD and tested validity of passwords by attempting to log into some of them successfully on HSYS.	Conversation with [redacted] on 11/24/80 with [redacted]
1980 NOV 14 14:58:33	[redacted] logs into userid GUILD on AIMS through SF2 using A/C INFO:BIPXBIPX++++++++. While logged on she gets message from userid BIPPER(shadow of GUILD) saying "Who the hell is this?" [redacted] notices files with filetype: CRDATA and prints some of it out. The file is HSYS CRDATA. The files are readable, not encrypted.	Coversation on 11/24/80 with [redacted] [redacted] AIMS OPERATOR log. Hardcopy of terminal session of [redacted] b6 b7C
1980 NOV 14 14:58:44	Userid shadow BIPPER of userid GUILD logs onto AIMS machine through port 36B on NCS1.	AIMS OPERATOR log. 11/14//80
1980 NOV 14 15:01:00	Message received on userid GUILD [redacted] currently on) from BIPPER/GUILD saying "Who the hell is this!!!!"	Hardcopy of [redacted] terminal session.
1980 NOV 14 15:02:50	Userid shadow BIPPER of userid GUILD logs off AIMS.	AIMS OPERATOR log (11/14/80).
1980 NOV 14 15:03:38	Userid GUILD [redacted] is forced logged off AIMS.	Hardcopy of [redacted] terminal session & AIMS

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 NOV 14 15:03:38	OPERATOR log shows time as 15:03:07 and 15:03:40.	OPERATOR log (11/14/80).
1980 NOV 14 15:11:22	Userid GUILD logs on to AIMS. The user is [redacted] See looks at more CRDATA files and lists the database PWS. The database description matches the CRDATA files containing the directory information. She also runs a small report to verify the database structure.	Hardcopy terminal log of [redacted] AIMS OPERATOR log.
1980 NOV 14 15:15:00	Time approximate. [redacted] says he got phone call from Bruce Paul (probably verifiable with SNET) asking who was userid GUILD that day. [redacted] plays dumb.	Conversation with [redacted] with [redacted]
1980 NOV 14 15:24:42	Userid GUILD [redacted] is foreced off the system by the KILL command.	Hardcopy terminal log of [redacted] AIMS OPERATOR log.
1980 NOV 14 15:27:08	Userid shadow BIPPER of userid GUILD logs onto AIMS from port 36B on NCS1. Attempts to see virtual machine configuration of userid GUILD (who is in the process of being KILLed.	The TLOG log created by the PROFILE EXEC. Original on file in SFR1 office. Copy in [redacted] file. AIMS OPERATOR log (11/14/80).
1980 NOV 14 15:36:58	Userid GUILD gets logged off of AIMS.	AIMS OPERATOR log.
1980 NOV 14 15:41:00	Userid BIPPER/GUILD is still logged into AIMS and lists all files with a last access date of 11/24/80. At 15:43 the user repeats the list of all files using the TIME option. User logs off at 15:47:29.	The TLOG log.
1980 NOV 14 15:47:32	Userid BIPPER/GUILD logs off.	AIMS OPERATOR log. Hardcopy of TLOG. (15:47:29).
1980 NOV 14 16:15:05	Userid GUILD logs on as shadow called BIPPER from port 36B (from NCS1). The user immediately encrypts files: HSYS CRDATA, EAST CRDATA, BIPUSER CRDATA, and SUNY CRDATA. The user then erases the unencrypted files. The user then checks for the configuration of userid [redacted] The user then changes his READ, WRITE, BATCH and LOGIN passwords. The user then changes PROFILE EXEC to ask for more passwords. User apparently does not notice the SET TLOG (put there by [redacted] in the PROFILE EXEC. The user logs out at 16:37:18 on 14NOV80.	The TLOG log. AIMS OPERATOR log (11/14/80) 16:14:39.
1980 NOV 14 16:44:57	User logs in as shadow BIPPER of userid GUILD through port 36B on NCS1. User looks for some files then logs off at 16:52:30 on 14NOV80.	The TLOG log. AIMS OPERATOR log (11/14//80) 16:44:16.
1980 NOV 14 16:57:28	User logs Into shadow BIPPER of userid GUILD through port 36B on NCS1. User edits PROFILE	The TLOG log. AIMS OPERATOR log (11/14/80) 16:56:38.

b6
b7C

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 NOV 14 16:57:28	EXEC, makes minor bug correction and looks to see configuration of userid [redacted] User then logs off at 17:00:47 on 14NOV80.	
1980 NOV 14 17:00:00	[redacted] agree to remove AIMS from NCSS network until Tues. 11/18.	Conversation with [redacted] b6 b7C
1980 NOV 15	[redacted] copied the disk pack on which the userid GUILD resided. She brought the disk pack to the SFR1 office along with the copied tape before the encryption. This tape was created by [redacted] when he was looking around and noticed the files. She also brought back the TLOG logs and the printout created by [redacted] containing the CRDATA files.	The disk and tapes and printouts are in the SFR1 office.
1980 NOV 17 06:15:51	Login from port 36B using LOGONID [redacted] on NCS1, for three minutes.	NCS1 ALTOP log.
1980 NOV 17 06:18:37	Seven seconds after previous use (by [redacted], port 36B used to attempt login as VPSYSMGR on SFR1.	NCS1 ALTOP log shows use of port 36B to access SFR1. SFR1 ALTOP log (according to [redacted] shows "LOGOFF VPSYSMGR" at 03:19:14 (time difference 37 seconds).
1980 NOV 17 06:22:28	Six attempts from port 36B to login to EAGLE on HSYS. First attempt at 06:22:28, last at 06:39:00.	NCS1 and HSYS ALTOP logs.
1980 NOV 17 06:46:18	Port 36B used to login to some ID on SUNY, for about six minutes.	NCS1 ALTOP log.
1980 NOV 17 06:58:09	Login of [redacted] on NCS1 from port 36B, for about one minute.	NCS1 ALTOP log.
1980 NOV 17 06:59:01	[redacted] on NCS1 got password for EAGLE on HSYS, giving reason as ".".	DIRPRINT log from HSYS. [redacted] says he never used DIRPRINT. b6 b7C
1980 NOV 17 06:59:31	Seven seconds after logout of [redacted] login to EAGLE on HSYS from port 36B. Session lasted about 8 minutes.	NCS1 and HSYS ALTOP logs. Time on NCS1 was 6:58:56.
1980 NOV 19	[redacted] removed userid GUILD from the AIMS machine. Attempted login to the AIMS machine. Logged onto userid VPSYSMGR twice, once for 1 minute, then for 30 minutes. This occurred around 0400 hrs on 11/19 (pst).	Conversation with [redacted] and [redacted] b6 b7C
1980 NOV 21 16:25:00	Conversation with [redacted]	Conversation With [redacted] nd files currently on

EVENT REPORT AS OF 01/21/81 09:04:30

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 NOV 21 16:25:00	After inspecting the copied files from GUILD on AIMS (files now on SFR1), [redacted] notes that: 1. BIPUSER CRDATA and HSYS CRDATA are identical files. 2. There is a program (EXEC) that could have been used for file transfers between systems. It uses INTERCOM to receive files.	SFR1. b6 b7C
1980 NOV 22	[redacted] inspects copy of GUILD userid both before and after encryption. On the copy created by [redacted] (before encryption), SJM notices the following: 1. The 4 CRDATA files. Notices that hisown userid CSSMADI only exists on the EAST CRDATA file. 2. Notices a copy of NOMAD module (later [redacted] will confirm it to be NOMAD2, unauthorized). 3. Notice a copy of the PASCAL compiler. 4. [redacted] prints out the contents of ALL files.	Terminal log in [redacted] office. File copies are on the SFR1 machine. b6 b7C
1980 NOV 25 17:10:00	Conversation with [redacted] Detailed billing records show that shadow [redacted] (login on 11/11/80 at 07:54) is userid [redacted] Records also show that shadow [redacted] (login on 11/11/80 at 07:32) is userid [redacted]	Billing records from 11/11/80 cupplied by Al [redacted]
1980 NOV 26 17:45:00	Conversation with [redacted] 1. His group does log into userid VPSYSMGR occassionally to fix problems on 3200s. They do this at request of Marketing/customer. 2. [redacted] not aware of login attempts on 11/17/80 (06:18) to SFR1 or to MML1 on 11/"1/80 (04:37 pst) 3. In general, noone logs in that earlyin the morning. [redacted] sees no reason for anyone logging into SFR1. 4. Userid [redacted] (belonged to [redacted] was used by [redacted] for NOMAD work. The FINAL group may also know the password to [redacted]	Conversation with [redacted] on11/26/80 and [redacted] b6 b7C
1980 DEC 01	[redacted] submits two listings: List from userid GUILD on AIMS showing file PSW SIT. SLIST command is displayed.	Hardcopy from [redacted] On file with [redacted] b6 b7C

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 DEC 01	List from the NCSS Backup system in use today. Slist command is displayed.	
1980 DEC 02 15:15:00	Conversation with [redacted] [redacted] uses shadow [redacted] of userid [redacted] on occassion. He never logs into any 3200. Occassionally logs in early morning to do regular work, and uses Danbury exchange.	Conversation with [redacted] b6 b7C
1980 DEC 02 15:20:00	Conversation with [redacted] He frequently uses shadow [redacted] for userid [redacted] He never logs in from Danbury. He logs in early sometimes, usually from Stamford. He last used userid [redacted] in April 1980 to fix NOMAD6 bugs. Did not use shadows then. Logs into CSS1 as [redacted] an occassion but NEVER logs into any other 3200. [redacted] said that [redacted] used the userid [redacted] also.	Conversation with [redacted] on 12/2/80.
1980 DEC 02 15:25:00	Conversation with [redacted] Last used userid [redacted] in 3/80-4/80. She never logs into any 3200.	Conversation with [redacted]
1980 DEC 02 17:00:00	Conversation with [redacted] [redacted] NEVER used DIRPRINT.	Conversation with [redacted]
1980 DEC 04 14:09:12	Investigate backup files for userid VERIFY on HSYS for end of June, 1980. Actual date of backup is 6/29/80. Observe file: BIPUSER CRDATA on the disk. This file is exact same format as the files found on AIMS. The number of items is 3878 and the actual data is from a different time. Also on tape is program called SPINOFF NOMAD, SETUP NOMAD, PWORD ASSEMBLE, and PWORD TEXT. SPINOFF reads database BACKTAPE and produces BIPUSER CRDATA using SETUP and PWORD. Also notice that ADDRESS MEMO is for [redacted] b6 b7C	HSYS backup tape No. 6H007 from end of June, 1980.
1980 DEC 05	Conversation with [redacted] The name of the database used by the NCSS Backup system is BACKTAPE. It is a control file used	Conversation with [redacted] 12/5/80.

DATE AND TIME	DESCRIPTION	EVIDENCE
1980 DEC 05	during the backup process. See 12/1/80, Conversation with [redacted] The file resides on the P disk of the userid BACKUP. Also, the Backup system creates the control file containing only userids which have disks. Userids without disks are not in the file.	b6 b7C
1980 DEC 08 21:02:56	Investigate backup tape for end-of-June 1980 (actual date = 6/29/80). Userid GUILD2 (which belongs to the GUILD) on HSYS is restored to disk. Two files seem interesting: TRNSFR EXEC seems to have capability for transmitting data between userids on different hosts using INTERCOM. The second file: PWHOST NOMAD is a NOMAD procedure to ....?????	HSYS backup tape No. 6H159 for end of June 1980.
1980 DEC 17 13:12:00	[redacted] reviews files from GUILD on AIMS (before encryption). Notice file called TEMP FILE which appears to contain entire Directory of AIMS machine.	File copies on SFR1 on userid [redacted] b6 b7C

x AIRTEL

2/24/81

TO: SAC, SAN FRANCISCO (196A-795)

FROM: SAC, NEW HAVEN (196A-397) (P)

SUBJECT: CHANGED
BRUCE IVAN PAUL
NATIONAL CSS, INC., - VICTIM
FBW (A) - COMPUTER FRAUD
(OO: NEW HAVEN)

Title marked changed to include full middle name Ivan. Title previously carried only middle initial "I".

RE: New Haven tel to San Francisco, 12/3/80.

Enclosed for San Francisco are the following items:

[redacted] b3

[redacted] b3 b6 b7C

[redacted] b6 b7C

2 - San Francisco (Encs. 4)
2 - New Haven
DEF/sab
(4)

GRAND JURY MATERIAL - DISSEMINATE ONLY
PURSUANT TO RULE 6(e), Fed. R. Crim. P.

SEARCHED
SERIALIZED
INDEXED
FILED

196A-397-12

LEADS:

NEW HAVEN
At Wilton, Conn.

Investigation continuing.

b6
b7C

TIME 09:20 DATE 11/19/80 PAGE 1
TERMINAL P900

PAUL BRUCE I WEST VIEW TRAILS NEW FAIRFLD CONN 06/20/54
01 UV9881 EXP 12/80 72 FORD LT CO SQ ST WAG GRN 2E76S207658

****
P/N PRESS ENTER FOR NEXT PAGE

TIME 09:20 DATE 11/19/80 PAGE 2
TERMINAL P900

PAUL BRUCE 4 WESTVIEW TRAILS NEW FAIRFLD CONN 06/20/54
01 YJ9426 EXP 12/80 74 CHEV VEGA 2D SED GRY 1U77R4U110507

END OF REQUEST *_*

196-A-397-13

TIME 09:18 DATE 11/19/80
TERMINAL P900 PAGE 1

b6
b7C

[redacted]

TIME 09:18 DATE 11/19/80
TERMINAL P900 PAGE 2

PAUL,BRUCE,I WESTVIEW TRAILS NEW FAIRFIELD CONN
DRIG ISS 12/21/78
EXP 06/82 OPNO 184156260 FEE $18.50
DOB 06/20/54 TYPE 103 HGT 6 01 SEX M
DUPS
END INQUIRY * *

196-A-397-14

Firm Avoids Security Breach With Customer Cooperation

By Rita Shoor
CW Staff

WILTON, Conn. — What can be done to prevent a security breach when an employee with access to sensitive information voluntarily leaves the company? National CSS, Inc. (NCSS) here chose to let all of its time-sharing customers in on things when faced with such a potential security problem.

The firm, which markets software and interactive computer services, discovered that "customers can be very understanding," according to David Fehr, president.

The situation arose when an employee whose job included knowledge of NCSS security procedures left the firm with the information locked away in his head. Although "there is no evidence that any [NCSS] customer files were accessed [invalidly] or that their [customer] IDs were used in any way," the potential for a security breach existed, Fehr said.

He pointed out the difference between this occurrence and one in which documents are taken or someone breaks a system security code through a remote terminal.

Change the Locks

The employer "can't shoot former employees," he noted. "But it can keep changing the locks" on private files and data bases.

NCSS, therefore, urged all customers to change log-in and read/write passwords in order "to maintain its commitment to maintain absolute security" in a memo dated Nov. 20.

Most of the firm's customers have been very cooperative about the password change, and there has been a "lack of negativism" within NCSS' customer base, according to Fehr.

This is especially gratifying in view of the fact that the firm could not give the customers a detailed explanation since "the matter is still under investigation for potential criminal action."

FROM COMPUTERWORLD
DATE UNKNOWN

196A397-15

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:	PRECEDENCE:	CLASSIFICATION:
☐ Teletype	☐ Immediate	☐ TOP SECRET
☐ Facsimile	☐ Priority	☐ SECRET
☒ AIRTEL	☐ Routine	☐ CONFIDENTIAL
		☐ UNCLAS E F T O
		☐ UNCLAS

Date 4/27/81

TO: SAC, SAN FRANCISCO (196A-795)

FROM: SAC, NEW HAVEN (196A-397)

SUBJECT: BRUCE IVAN PAUL;
NATIONAL CSS, INC. - VICTIM;
FBW (A) - COMPUTER FRAUD
(OO: NEW HAVEN)

During the course of captioned investigation, a FGJ subpoena was issued to obtain [redacted]

[redacted]

b3
b6
b7C

2 - San Francisco (194A-795)
2 - New York
(2) - New Haven
DEF/sab
(6)

Searched
Serialized
Indexed
Filed

[redacted]

b6
b7C

196A397-16

Approved: _____ Transmitted _____ (Number) _____ (Time) Per _____

NH 196A-397

New Haven at New Haven

Investigation continuing at Wilton, Conn.

Memorandum

To : SAC, NEW HAVEN (196A-397) Date 4/29/81

From : SECRETARY [redacted] b6 b7C

Subject : BRUCE IVAN PAUL
NATIONAL CSS, INC. - VICTIM
FBW (A)
(OO: NEW HAVEN)

[redacted] b6 b7C b7D

The attached data cannot be made public except upon the issuance of a subpoena duces tecum directed to

[redacted] b6 b7C b7D

On 4/29/81, check of the New Haven Offices Indices proved negative regarding [redacted] b7D

(2) - New Haven
/sab
(2)

196A397-17
SEARCHED ____ INDEXED ____
SERIALIZED ____ FILED ____
APR 29 1980
FBI — NEW HAVEN

FBI/DOJ

NH 196A-397
/sab
1.

On April 28, 1981, investigation conducted at New Haven, Connecticut, determined the following information:

[redacted]

b6
b7C
b7D

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/26/81

[redacted] b6 b7C

was advised of the official identity of the interviewing agent and the nature of the interview. He thereafter provided the following information:

Approximately one year ago he was affiliated with the Guild Incorporated [redacted] b6 b7C [redacted] The Guild had been established by them approximately one year prior for the purpose of developing complex computer software programming.

Approximately one and a half years ago he was introduced to [redacted] of Mediametrics (MM) of Moraga, California, by a National CSS (NCSS) employee by the name of [redacted] b6 b7C Some time prior to the introduction by [redacted] MM had purchased a computer and a software package from NCSS to adapt the MM operation to a computer based system. The software package which MM had purchased from NCSS was not however living up to expectations as previously described by NCSS employees. In an effort to make the NCSS computer and software perform more efficiently, [redacted] introduced [redacted] hoping that the Guild could improve upon the software packages provided by NCSS. After meeting with [redacted] and discussing the situation, it was agreed by the partners of the Guild, on a verbal basis, that they would agree to develop software to be used on the MM NCSS machine in exchange for machine time which could be used by the Guild for other developmental purposes. [redacted] the software development for MM. [redacted] with the approval of all the other Guild partners hired Bruce Ivan Paul to work on the software programming packages. Several months thereafter on approximately July 18, 1980, he and [redacted] severed their relationship with the Guild for numerous personal and financial reasons. After that point in time, they had very little contact with [redacted] at MM.

[redacted] b6 b7C

Investigation on 5/19/81 at Shelton, Connecticut File # 196A-397-18

by SA [redacted] dej/DEF/lmf Date dictated 5/26/81 b6 b7C

During sometime in November, 1980, he was called by [redacted] of MM who described to him data which [redacted] found in the computer space being used by the Guild. Both he and [redacted] recognized the information to be directory data and suggested that [redacted] immediately call NCSS to tell them what he had found. Within a week thereafter, [redacted] was successful in keeping the Guild off of his machine located at MM. [redacted] then asked he and [redacted] to develop software programs to get the MM business operation back on line. They accepted the offer and provided [redacted] with a much more steamlined operation, which was completely installed just a short time ago. b6 b7C

He recalled receiving a phone call from Bruce Paul some time during the middle of November, 1980. During the phone conversation, Paul identified himself and then asked how do you get past [redacted] He was very puzzled as to this question and then remembered that he had recently received a copy of a Dungeons and Dragons type computer game from another software programmer just a short time ago. He then suggested to Paul that Paul contact the developer of the program directly. He has not heard from Bruce Paul since that time. b6 b7C

He indicated that he did not gather together and transport the directory data from NCSS main frames which was found on the MM computer space used by the Guild. He further indicated that he would be willing to take a polygraph in regard to this matter.

He noted that NCSS had four privilege classes for access to computer information on the NCSS time sharing system. The class B privilege class was reserved for those individuals in the developmental section at NCSS. All of those individuals would have access to a command called DIRPRINT. With access to the DIRPRINT command the passwords on the I-D directory could be obtained relatively easily. He suggested that it might be possible to obtain a log which was maintained on all of the use of the DIRPRINT command. The log could probably be obtained from [redacted] at NCSS. b6 b7C

He also suggested that an [redacted] contacted in regard to this matter. [redacted] had apparently done an extensive investigation for a magazine called [redacted] When [redacted] was ready to release his report on NCSS security, the report was apparently held in obeyance because NCSS did not want anyone to find out about their security problems. b6 b7C

It was his opinion that the gathering of the directory data and the transporting of it to an area on the MM computer was not really done with criminal intent. He referred to the term "hackery" which is known in the business as an attempt by

someone to break the system. It was his opinion that hackery would continue in the computer business as long as security for programs and computer information had loop holes in the design.

He indicated that he would be willing to provide any other assistance which may become necessary during the course of the investigation.

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/26/81

[redacted] b6 b7C

was advised of the official identity of the interviewing agent and the nature of the interview. Also present during the interview were [redacted] He thereafter provided the following information:

[redacted] b6 b7C

[redacted] The Guild had been established by them approximately one year prior for the purpose of developing complex computer software programming.

Approximately [redacted] he was introduced to [redacted] of Mediametrics (MM) of Moraga, California, by a National CSS (NCSS) employee by the name of [redacted] b6 b7C Some time prior to the introduction by [redacted] MM had purchased a computer and a software package from NCSS to adapt the MM operation to a computer based system. The software package which MM had purchased from NCSS was not however living up to expectations as previously described by NCSS employees. In an effort to make the NCSS computer and software perform more efficiently, [redacted] introduced [redacted] hoping that the Guild could improve upon the software packages provided by NCSS. After meeting with [redacted] and discussing the situation, it was agreed by the partners of the Guild, on a verbal basis, that they would agree to develop software to be used on the MM NCSS machine in exchange for machine time which could be used by the Guild for other developmental purposes. [redacted] with the [redacted] hired Bruce Ivan Paul to work on the software programming packages. Several months [redacted]. After that point in time, they had very little contact with [redacted] at MM.

[redacted] b6 b7C

Investigation on 5/19/81 at Shelton, Connecticut File # 196A-397-19

by SA [redacted] DEF/lmf Date dictated 5/26/81 b6 b7C

NH 196A-397

During sometime in November, 1980, he was called by [redacted] of MM who described to him data which [redacted] found in the computer space being used by the Guild. Both [redacted] recognized the information to be directory data and suggested that [redacted] immediately call NCSS to tell them what he had found. Within a week thereater, [redacted] was successful in keeping the Guild off of his machine located at MM. [redacted] then asked he [redacted] to develop software programs to get the MM business operation back on line. They accepted the offer and provided [redacted] with a much more steamlined operation, which was completely installed just a short time ago.

b6
b7C

He indicated that he did not gather together and transport the directory data from NCSS main frames which was found on the MM computer space used by the Guild. He further indicated that he would be willing to take a polygraph in regard to this matter.

He indicated that he would be willing to provide any other assistance which may become necessary during the course of the investigation.

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:	PRECEDENCE:	CLASSIFICATION:
☐ Teletype	☐ Immediate	☐ TOP SECRET
☐ Facsimile	☐ Priority	☐ SECRET
☒ AIRTEL	☐ Routine	☐ CONFIDENTIAL
		☐ UNCLAS E F T O
		☐ UNCLAS

Date 6/30/81

TO: SAC, NEW HAVEN (196A-397)

FROM: ADIC, NEW YORK (196-1697) (RUC) (M-12)

SUBJECT: BRUCE IVAN PAUL;
NATIONAL CSS, INC - VICTIM;
FBW (A) - COMPUTER FRAUD
(OO: NH)

ReNHairtel dated 4/27/81.

b3
b6
b7C

(2) - New Haven
1 - New York

GMO:tll
(3)

196-397-20

SEARCHED 1 INDEXED
SERIALIZED 13 FILED JD
JUL 4 1981
NEW HAVEN

b6
b7C

Approved: [signature] Transmitted _____ Per _____
(Number) (Time)

☆ U.S. GOVERNMENT PRINTING OFFICE: 1980-305-750/5402

Memorandum

To : SAC, NEW HAVEN (196A-397) (P) Date 6/18/81

From : SA [redacted] b6 b7C

Subject : BRUCE IVAN PAUL,
NATIONAL CSS INCORPORATED -
VICTIM
FBW - (A) - COMPUTER FRAUD

On 6/9/81, the writer contacted [redacted] b6 b7C to determine where [redacted] was living and working in the Boston area so that he could be contacted and interviewed by a Boston Division Agent regarding captioned matter. [redacted] advised that at [redacted] he would feel very uncomfortable being interviewed on a formal basis by an FBI Agent.

[redacted] did feel that an interview over the phone could be productive for both himself and the writer as a type of information exchange. He then indicated that he had begun his investigation into attempts at unauthorized access to directory information stored on the NCSS On Line Time Sharing System. During the course of his investigation, he interviewed numerous individuals who were past and present employees of NCSS which is based in Wilton, CT. In addition, he has talked to several other sources involving Computer Fraud on a national and regional basis throughout the United States. His investigation in this [redacted]

(2) New Haven
DEF:lmf
(2)

196-397-21

SEARCHED INDEXED
SERIALIZED FILED
JUL 02 1981
FBI — NEW HAVEN

[redacted] b6 b7C indicated that he had interviewed an individual by the name of [redacted] had been working out of the Cleveland area attempting to make sneak attacks against the security systems installed in the NCSS Time Sharing System. [redacted] was apparently very successful and is a kind of folk hero to the programmers currently working at NCSS. [redacted] also discovered that a [redacted] during approximately 1978 had sent a letter to [redacted] Since that time, other operations individuals at NCSS had apparently been attempting to brake the system as successfully as [redacted] had in the past.

[redacted] then talked of various other computer fraud b6 b7C cases with which he was very familiar including the FBI case involving [redacted] which was worked out of the Los Angeles area. [redacted] also indicated that he had [redacted] also stated that he believes the current Computer Fraud case involving Bruce Paul appeared to be very significant as he was told that two (2) Senate investigating committees would be sending up their own investigators to determine how serious the security breach had been, and what safeguards were currently being taken to insure that further system failures would not reoccur.

[redacted] was told by the writer that at the current b3 b6 b7C time [redacted] had been subpoenaed by Federal Grand Jury at [redacted] also that a criminal investigation involving the Bruce Paul incident was currently continuing. The writer also told [redacted] that the case would not be presented to the US Attorneys Office until a complete investigation was compiled.

196-397-22

SEARCHED ____ INDEXED ____
SERIALIZED ____ FILED ____
JUL 6 1981
AVEN

b6
b7C

CHRONOLOGY OF SIGNIFICANT EVENTS - PM OF 11-14-80, FRIDAY (TIMES ARE PST)

NM FILE 196A-397 (00) - SF FILE 196A-795 (A0) - PREPARED ON 06-03-81

12:00:+- - [redacted] NOTIFIES [redacted] OF CDIR FILES ON GUILD ID ON MM COMPUTER. b3 b6 b7C

02:30+- - [redacted] INFORMS [redacted] OF PROBLEM UPON HIS RETURN TO OFFICE AND [redacted] IS INSTRUCTED TO VERIFY THAT CDIR FILES ARE ON MM COMPUTER.

02:58:+- - [redacted] CALLS [redacted] SAYING SHE WANTS TO GET INTO CDIR FILES.

02:58:27 - [redacted] LOGS ONTO GUILD ID ON MM COMPUTER FROM NCSS.

03:00:+- - [redacted] RECEIVES CALL FROM PAUL ASKING WHO COULD BE ON GUILD ID..

03:01: - MESSAGE ON [redacted] TERMINAL FROM [redacted] GUILD: WHO THE HELL IS THIS!

03:03:38 - [redacted] KILLED FROM GUILD ID.

[redacted]

03:11:22 - [redacted] LOGS BACK ONTO MM COMPUTER FROM NCSS.

[redacted]

03:23:52 - [redacted] LOGS OFF MM COMPUTER.

03:27:31 - SOMEONE VIA NCSS NETWORK LOGS ONTO GUILD ID ON MM COMPUTER.

03:28: - USER ID GUILD ATTEMPTS TO GET HARD COPY LIST OF WHICH TERMINALS HAD BEEN USING THEIR ID.

[redacted] b3

03:43: - USER ID GUILD LISTS ALL THEIR FILES ACCESSED ON 11-14-80.

03:47:29 - USER ID GUILD LOGS OFF MM COMPUTER.

04:15:05 - SOMEONE VIA NCSS NETWORK LOGS ONTO GUILD ID ON MM COMPUTER.

04:15: - USER ID GUILD ENCRYPTS CRDATA FILE 'HSYS'.

04:19: - USER ID GUILD ENCRYPTS CRDATA FILE 'EAST'.

04:23: - USER ID GUILD ENCRYPTS CRDATA FILE 'BIPUSER'.

04:27: - USER ID GUILD ENCRYPTS CRDATA FILE 'SUNY'.

04:29: - USER ID GUILD CHECKS TO SEE WHO WAS THEN LOGGED ONTO MM COMPUTER.

04:29: - USER ID GUILD ATTEMPTS TO SEE WHAT USER [redacted] b6 b7C [redacted] WAS DOING ON THE MM SYSTEM AT THE TIME.

04:30: - USER ID GUILD CHECKS TO SEE ALL WORK ON MM SYSTEM AWAITING PRINTING.

04:30 - USER ID GUILD CHECKS TO SEE IF THERE IS AN ADDRESS FOR CUSTOMER NAMED [redacted] WITH NEGATIVE RESULTS. b6 b7C

04:31: - USER ID GUILD CHANGES THEIR PASSWORDS TO MM COMPUTER.

04:31: - USER ID GUILD LOADS SECURITY FILE '11144734' & PRINTS OUT CONTENTS.

04:34: - USER ID GUILD MODIFIES THEIR PROFILE EXEC.

04:37:18 - USER ID GUILD LOGS OFF MM COMPUTER.

04:44:57 - SOMEONE VIA NCSS NETWORK LOGS ONTO GUILD ID ON MM COMPUTER.

04:45: - USER ID GUILD CHECKS TO SEE ALL WORK ON MM SYSTEM AWAITING PRINTING.

04:46: - USER ID GUILD CHECKS TO SEE IF ANY FILE BEING DIRECTED TO THEIR AREA OF DISK BUT NOT YET WRITTEN THERE.

04:47: - USER ID GUILD CHECKS TO SEE WHO WAS THEN ON MM SYSTEM.

04:48: - USER ID GUILD ATTEMPTS TO LOCATE FILE 'SER*EXEC' UNSUCCESSFULLY.

04:50: - USER ID GUILD ATTEMPTS TO RUN PROGRAM 'SERVER' UNSUCCESSFULLY.

[redacted] b3 b6 b7C

04:51: - USER ID GUILD CHECKS TO SEE IF USER ID [redacted] IS ON MM SYSTEM.

04:52:30 - USER ID GUILD LOGS OFF MM COMPUTER.

[redacted] b3 b6 b7C

04:57:28 - SOMEONE VIA NCSS NETWORK LOGS ONTO GUILD ID ON MM COMPUTER.

04:58: - USER ID GUILD MODIFIES THEIR PROFILE EXEC.

04:59: - USER ID GUILD CHECKS TO SEE WHO WAS THEN ON MM SYSTEM.

04:59: - USER ID GUILD ATTEMPTS TO SEE WHAT USER ID 'HSL' WAS DOING ON MM'S SYSTEM AT THAT TIME.

05:00:47 - USER ID GUILD LOGS OFF MM COMPUTER.

[redacted] b3 b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/18/81

[redacted] b6 b7C
[redacted] National CSS, Inc., 650 California Street, Suite 1840, San Francisco, California, telephone [redacted] was interviewed and related the following information:

As requested by SA [redacted] attempted b6 b7C to locate the original console log for National CSS's San Francisco branch computer known as "SFR-1" for November, 1980, that contained evidence of an attempted unauthorized access to the computer. [redacted] advised that he was unable to locate any original logs for this period and, as best as he could determine, all of them have been destroyed as part of their normal practice. [redacted] was not aware of any other copies of these console logs, and he provided no additional pertinent information.

196-391-23

Investigation on 6/15/81 at San Francisco, California File # SF 196A-795

by SA [redacted] cea Date dictated 6/16/81 b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 6/18/81

[redacted] b6 b7C

[redacted] was interviewed concerning his recollection of sending the contents of a backup tape over the telecommunications network during the week of November 17, 1980, while he was employed by National CSS, San Francisco.

[redacted] was informed that [redacted] of National CSS b6 b7C had stated during his interview that during the week of November 17, 1980, he [redacted] gave an original backup tape to [redacted] and requested that [redacted] send the contents of the tape over the National CSS network to [redacted] National CSS Headquarters, and that this backup tape contained CDIR file data that had been obtained from Mediametrics of Moraga, California. [redacted] advised that he had a vague recollection of [redacted] asking him to do several things in connection with the unauthorized possession of CDIR file information found at Mediametrics, but he could not specifically recall having sent the contents of a particular magnetic tape over the network to National CSS Headquarters. However, [redacted] advised that this would have been a reasonable and routine request and that, if [redacted] made such a request, [redacted] would have complied with it. He continued that there are standard procedures and utility programs that are used to make this routine transfer of information from a magnetic tape over the network and that such a process would in no way alter or destroy the data on the original magnetic tape. The magnetic tape would be in it's same condition after the procedure as it was at the beginning and [redacted] opined that he would have returned the original tape to [redacted] when he was finished with it. [redacted] explained that he could not recall further details because it occurred quite sometime ago and due to the very routine nature of [redacted] request. He provided no additional pertinent information.

196-397-24

Investigation on 6/15/81 at Santa Clara, Calif. File # SF 196A-795

by SA [redacted] / sdc Date dictated 6/15/81 b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/16/81

[redacted] b6 b7C

[redacted] was interviewed at his place of employment concerning his knowledge of the unauthorized possession of passwords and customer account numbers belonging to National CSS and found on a computer disc pack located in the computer room of Mediametrics (MM) of Moraga, California. [redacted] voluntarily related the following information:

[redacted] b6 b7C

connection with his duties he was knowledgeable of, and somewhat involved in, the software modifications that were being made to MM's operating system by a company known as "The Guild" located in Connecticut. In connection with The Guild's work, he had occasion to come into contact with an employee of that firm named Bruce Ivan Paul. Prior to Paul's becoming involved in the modification for The Guild, [redacted] had no prior contact with or knowledge of him. He understood from Paul that he had been employed as a Systems Programmer for National CSS prior to going to work for The Guild. All of [redacted] contact with Paul was telephonic or by computer terminal except for one occasion when Paul visited MM's facilities.

This visit occurred sometime in September of 1980 and was approximately one week in duration. Paul had come to MM in order to do some work on the project and [redacted] b6 b7C . Paul had brought with him one old magnetic tape that he said contained a number of utilities and other such routines that a programmer finds useful and it was [redacted] impression that the contents of this tape had been collected by Paul during his employment at National CSS. [redacted] was present in the computer room when Paul attempted to load this tape on one of MM's tape drives but they were unsuccessful in this effort because the density was different than could be handled by MM's tape drives. [redacted] believed that they were able to print out the label on the tape but that they could not load in any other data from it.

196-390-25

Investigation on 6/2/81 at San Francisco, Calif. File # SF 196A-795

by FW SA [redacted] / sdc Date dictated 6/5/81 b6 b7C

As far as [redacted] knew, this was the only tape that Paul brought with him. He recalled that during the same visit, Paul updated NOMAD on MM's system by use of an update tape supplied by National CSS but that, instead of using the regular time consuming procedure to run this update, Paul used a National CSS utility that he had stored on that section of the disc pack that MM had assigned for use by The Guild. [redacted] believed that this utility routine was named "SETSYS" and, although not available to the public, was not particularly valuable except to facilitate running update tapes received from National CSS. It was [redacted] understanding that this utility is not made available to customers because it does require somewhat more of a technical background in order to run it successfully than is possessed by normal customer representatives. b6 b7C

Over a period of time prior to November 13, 1980, MM detected that very little work was being done on the modification project by The Guild but that The Guild was using considerable system resources for their own projects. This became a source of concern to MM management and they undertook steps to correct this problem. This included attempts to discuss the matter with representatives of The Guild and these efforts were essentially unproductive. MM also tried changing passwords of The Guild but The Guild was able to get into MM's computer using a system ID and learn what their new passwords were.

This difficulty prompted MM's [redacted] to start developing an inventory routine that would permit MM to print out the contents of files being stored on any ID within MM's system so that they could determine what was being done. As part of this effort [redacted] discovered some files under The Guild ID that, because of their names and size, he suspected contained information proprietary to National CSS and something that The Guild should not possess. [redacted] to attempt to go into these particular files so that they could be listed on a printer. b6 b7C

As [redacted] recalled there were four such files; three of which had names that were the same as the regional host computers of National CSS called "HSYS", "EAST", and "SUNY". The fourth file was named something like, "BIPUSER" or a similar name that included the initials of Paul. b6 b7C

Through experimentation, [redacted] was able to print out the contents of one of these files and it appeared to him to be a list of all the passwords and customer account numbers which, b6 b7C

because of the names, [redacted] assumed belonged to National CSS. b6 b7C

[redacted] then printed out the entire contents of one of these files, which he believed was named "EAST". He discovered that it was inadvertently sent over the National CSS network via spooling to the "HSYS" node and he was unable to cancel this spooling before it was completed. Therefore, a full printout of this file was made on a printer in Connecticut and part of the "HSYS" host computer. As a normal procedure, the printouts contain the name and address to whom they should be delivered to and, in this case, it automatically showed The Guild's name and address since it was one of their files that was printed out. [redacted] did not know whether this printout was either delivered to The Guild or picked up by them, or what happened to it. As best as he recalled, this spooling activity occurred between 5:00 p.m. and 7:00 p.m. PST on November 13, 1980, and was the only spooling traffic from Ames to the "HSYS" node via the National CSS network. b6 b7C

After discovering that the printout had been erroneously sent, he then changed the necessary instructions and printed out one full copy of this file on the printer located in MM's computer room. As he recalled, it was approximately 1-2 inches high and some 100 pages in length. He gave this printout to [redacted] who said that he would put it away for safe keeping. b6 b7C

The next day (Friday, November 14, 1980), [redacted] informed National CSS at San Francisco of the discovery of what they thought were their passwords and other customer information and, during that afternoon, one of National CSS' technical people logged onto The Guild ID. They were attempting to determine if the passwords were live data and, while logged on, someone broke in on their terminal and demanded to know who it was. When National CSS did not respond, whoever it was that had initiated the message then automatically disconnected National CSS from the MM computer. It was [redacted] understanding that such a "kill" procedure is not part of the documentation that National CSS provides to it's customers but it is an in-house procedure known to National CSS personnel. b6 b7C

[redacted] has had no contact at all with Paul since this incident, nor did he have any other information, either direct or hearsay, as to who was responsible for storing these four sensitive files on MM's disc pack or why it was done. Although he emphasized that he had no facts on which to support his belief, he opined that if Paul in fact was responsible for copying and keeping these files without authorization, that Paul did not have any sinister motive in doing this. Rather, [redacted] felt that Paul was the type of b6 b7C

individual like most programmers that collect and keep various things that may be useful to them in the future in doing a particular job. [redacted] knew of no other information that would be of assistance in this investigation but agreed to notify SA [redacted] should he recall anything pertinent in the future. b6 b7C

[redacted]

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/2/81

[redacted] b6 b7C

Mediametrics, Inc. (MM), 1620 School Street, Moraga, California, telephone [redacted] was interviewed on a number of occasions between December 11, 1980 and May 26, 1981, pertaining to his knowledge of the unauthorized possession of passwords and customer account information belonging to National CSS and found on a computer disc pack located in the computer room of MM. [redacted] voluntarily related various information which has been incorporated into one results of interview for clarity.

MM is a computerized information service primarily subscribed to by various newspapers throughout the country. They have been in business for approximately 4½ - 5 years and they were known as Television Media Service (TMS) before they changed their name to MM. To support the service that they provided, they purchased a National CSS 3200 Series, Rev 5, mini-computer in September 1979 from National CSS. They had been doing business with National CSS since April 1978 by using their time sharing system, communications network, and software products.

During 1980, MM's computer system was on-line 24 hours a day, except for routine and unexpected down time, and it could be accessed via the National CSS network whenever it was on-line. MM's facilities are not staffed 24 hours a day and employees are usually only on site during the regular day time hours.

On December 9, 1979, while doing business as TMS, they entered into a verbal agreement with a firm called, "The Guild", which is a computer consultant group in the State of Connecticut. The agreement was made between [redacted] The Guild and [redacted] MM, and it called for The Guild to do software modifications to MM's computer system in exchange for free use of MM's system and certain disc storage space. The modifications were to be done by mid October 1980, and work on the job started within about one week of the agreement. b6 b7C

As far as [redacted] knows, The Guild consists of [redacted] b6 b7C

[redacted] are former National CSS employees and [redacted] is currently part of

196-391-26

Investigation on 12/11/80-5/26/81 at Moraga, Calif. File # SF 196A-795

by SA [redacted] / sdc Date dictated 5/29/81 b6 b7C

[redacted] were the only ones at The Guild that worked on MM's project originally and all of the work was done at The Guild Office in Ridgefield, Connecticut, via the National CSS network and remote computer terminal. This work continued until around May of 1980. b6 b7C

At that time, Bruce Ivan Paul was hired by The Guild by [redacted] was gradually phased into the MM project. Paul eventually took over the work exclusively after a phase-in period. It was [redacted] understanding that Paul was a systems programmer at National CSS at the time that he was hired by The Guild. Neither [redacted] nor MM had any contact or knowledge about Paul prior to this time, and all contact with him after he was hired by The Guild was either over the telephone or a computer terminal until Paul visited MM's facilities in September of 1980. b6 b7C

Around [redacted] severed their relationship with The Guild and [redacted] and sought out business as private computer consultants. Neither [redacted] nor [redacted] had anything to do with MM's modification project once they left The Guild. b6 b7C

Starting about September 25, 1980, Paul was on site at MM for approximately a one week period in connection with the software modification. This was the first and only time that [redacted] met Paul or that Paul was at MM's facilities. On the same day that he arrived he went into MM's computer room and loaded a NOMAD update from a tape that had been received from National CSS. [redacted] (who then worked for MM) were in the computer room at the time. While doing this, Paul said that he was going to see if he could load another tape that he had brought with him as it had some "neat things" on it that he could use in connection with his work at MM. Paul said that he made some modifications to various utilities that he used at National CSS and that he had taken them with him when he left National CSS. He told [redacted] more precisely what was on the tape, but [redacted] could not recall what it was other than some utility programs and procedures that a programmer would use. [redacted] was certain that no mention was made that any CDIR files or data was on the tape. b6 b7C

Paul gave [redacted] the tape, who then mounted it on the tape drive. Paul then typed in the commands at the console in an attempt to load it. [redacted] observed that this tape was not a new product tape but appeared to be a well used magnetic tape with many labels over one another as if it was for personal use b6 b7C

by someone rather than a part of a library or standard product. Several attempts were made to load the tape unsuccessfully and [redacted] believes this was due to a different density format (probably 6250 bpi) than the MM system tape drives could handle. As far as he knew, Paul took the tape back with him after this one effort to load it. b6 b7C

[redacted] had no knowledge if Paul had made other attempts to load this same tape or any other tapes that he may have brought with him. Paul had the complete run of the MM computer system during the entire time that he was on site and he could have done anything he wanted to do during that time. b6 b7C

In mid October 1980, MM started to notice very little work being done on the modification project by The Guild and that all of their work on MM's system was not related to the modification project. By November 6, 1980, all of Paul's activities on the MM system had ceased and all computer time was being used by [redacted] who had a similar experience and knowledge level as Paul. MM made repeated efforts prior to this time to contact Paul without success and MM was given various excuses by Guild employees as to why Paul would not return messages that MM had left for him. b6 b7C

On November 7, 1980, the MM system crashed while The Guild was logged on and it was [redacted] opinion that it was caused by excessive work being done by The Guild. [redacted] was notified by [redacted] during the a.m. hours of November 7, 1980, via a terminal message that MM's system was no longer available for use by The Guild until further notice. During the afternoon of that same date, [redacted] called [redacted] on the telephone and [redacted] repeated this notification to him. [redacted] did not object and [redacted] assumed that there would be no more use by The Guild until the problems were resolved with Paul or higher authority within The Guild. b6 b7C

Within 1½ or 2 hours of this telephonic contact, The Guild ID logged onto MM's system and moved several files stored on The Guild ID at MM over the National CSS network to the user ID EAGLE and stored on National CSS' host computer HSYS. [redacted] determined this by the console log and the spooling traffic shown b6 b7C

thereon. When [redacted] was informed of this on the same day that it occurred, he told [redacted] to change The Guild passwords so that they could not log onto the MM system. It was [redacted] intention to keep The Guild off until talking to Paul and others at The Guild in order to resolve the problems. b6 b7C

On November 10, 1980, calls were made to The Guild but they were unsuccessful in contacting either [redacted] b6 b7C

Either late on that same day or early on the following day, November 11, 1980, [redacted] learned that The Guild had been back on MM's system again. This meant that they had gotten into MM's system via the VPSYSMGR ID and obtained the new password that [redacted] had assigned to them. [redacted] tried to call The Guild again without success so he told [redacted] to terminate The Guild connection to MM's system and to take the entire MM system off of the National CSS network so that there would be no way that The Guild or anyone else could get into MM's computer. This was done, and within several minutes, [redacted] received a telephone call from [redacted] of The Guild. [redacted] told him that MM intended to sever their relationship with The Guild because of a lack of effort by The Guild on MM's modification project, and the inordinate amount of network and system resources being used by [redacted] on non-MM business. [redacted] agreed with [redacted] and stated that he would reorder The Guild's priorities and that they would complete the modification project as soon as possible (which [redacted] estimated to be November 14, 1981). Feeling that the situation had been resolved, [redacted] then told [redacted] to allow The Guild access to MM's system again. b6 b7C

Ever since September 20, 1980, The Guild has been assigned tracks 3770 to 4320, cylenders 342 to 392 (50 cylenders deep), on disc pack "TMSPK1". The Guild had previously been assigned 50 cylenders at a different address on the same disc pack ever since the original agreement. There was no other disc space assigned to The Guild on MM's system.

On November 12, 1980, [redacted] noticed from the console logs that on November 10, 1980, there were 47 files moved from The Guild ID on the MM system over the National CSS network and stored on their host computer HSYS under the ID of EAGLE. Someone at The Guild, possibly [redacted] were used for the shado ID, tried to log on the MM system and, after failing, logged onto the VPSYSMGR ID. Spooling traffic on the log shows that 47 files were moved but the names and contents of these files are not known. b6 b7C

When [redacted] heard about this on November 12, 1980, he started to devise an inventory procedure to identify all files resident on each of the system IDs as he was fearful that MM proprietary data had been removed by The Guild. This inventory procedure was started on internal user IDs and it was discovered that The Guild had changed their passwords again without notifying MM. b6 b7C

On November 13, 1980, [redacted] called [redacted] National CSS, San Francisco, and explained to her the problems that he was having in regards to The Guild. [redacted] asked her to help in getting access to The Guild's new passwords and she complied. She did this by remote terminal from her office at National CSS. After [redacted] got the new password, [redacted] was unable to log onto that ID because there had been some modifications made to the security procedures for that ID. When [redacted] informed [redacted] of this, she was able to overcome these changes in the profile exec for [redacted] was then able to successfully log onto The Guild ID. b6 b7C

During the PM of November 13, 1980, [redacted] did an inventory procedure on The Guild ID and also printed out the contents of some of the files thereon that looked suspicious to him. During the morning of the next day, [redacted] examined these printouts of The Guild files and he was of the opinion that it contained some highly sensitive information as well as software products that were proprietary to National CSS. In particular, he noticed four files of significance: HSYS, EAST, SUNY, and BIPUSER. He went into these four files and examined their contents and was then of the opinion that all four of them were CDIR files containing user IDs, passwords and other data on customers of National CSS. b6 b7C

Between 9:00 and 10:00 a.m., on November 14, 1980, [redacted] logged onto three of the IDs from one of the CDIR files in order to see if the passwords were still active. He found that each of them were still valid and he did this from line 046 to National CSS host computer HSYS. [redacted] could not recall which of the passwords he logged onto nor which of the files he accessed but he did recall that one of them was a demo file on National CSS script language on an ID of a company in either Boston or Cambridge, Massachusetts. b6 b7C

On either November 13, 1980 or early on November 14, 1980, [redacted] had The Guild ID profile exec modified so that it would create a Terminal Log in the MM computer of all activities on that ID. He also had [redacted] make special back-up tapes of b6 b7C

all of The Guild files.

Around noon on November 14, 1980, [redacted] called [redacted] at National CSS and explained to her about finding the CDIR files. She said that [redacted] was out to lunch but that she would advise him as soon as he returned. b6 b7C

Several hours later, [redacted] called [redacted] and said that she wanted to get into The Guild ID in order to check the CDIR files herself. She did this by remote computer terminal from her office in National CSS and, simultaneously, continued to talk with [redacted] was examining the contents of the CDIR files while on The Guild ID [redacted] received word for an MM employee that Paul was on another line wanting to talk with him. [redacted] hung up from [redacted] and got on the line with Paul. Paul asked him, "Who could be on The Guild ID logged in from SF1?" [redacted] pretending that he didn't know anything about it, told Paul that it was probably someone from National CSS Professional Software looking at the modifications that The Guild was making to the MM system. Paul seemed very curious and said that he knew someone in National CSS and that he was going to call that person to see if the person could find out who was using The Guild ID. This call lasted no longer than three minutes and Paul hung up. b6 b7C

Within minutes thereafter, [redacted] called [redacted] back and said that she had just been killed (i.e. involuntarily logged off of the MM computer system) after getting a message on her terminal asking her, "Who the hell is this!!!!" [redacted] then told [redacted] about receiving the telephone call from Paul. b6 b7C

Several hours later, at approximately 4:30 p.m., Paul called [redacted] again. There was the sound of a child crying in the background and this caused [redacted] to believe Paul was calling from his home. Paul said that he had called [redacted] at National CSS to find out who was on The Guild ID since there was not anyone at Professional Software that he could talk to. Paul said that [redacted] told him that there was no way of finding out the information that he wanted. Paul did not seem too concerned about the matter and he then talked to [redacted] about other topics related to MM's modification project. This call lasted about 15 minutes in total and Paul did not talk anymore about the user on The Guild ID. b6 b7C

[redacted] received a telephone call from [redacted] later that same day and [redacted] was requested to take the MM system off of the National CSS network until such time that National CSS could meet with him and pick up the original disc pack containing the CDIR files. Arrangements were made for [redacted] to meet b6 b7C

with [redacted] at MM the following morning for this purpose, and [redacted] agreed to take MM's system off line until that time. b6 b7C

At approximately 8:00 a.m. on November 15, 1980, [redacted] met with [redacted] at MM and [redacted] gave [redacted] the terminal logs, inventories of Guild files, and various printouts that had been made of data on The Guild ID. [redacted] also gave [redacted] two magnetic tapes: one being the latest version of the regular back-up made of data on the disc pack containing The Guild ID, and the other being a special back-up that [redacted] had [redacted] make of only The Guild ID data. b6 b7C

[redacted] made a copy of the disc pack onto another disc pack that he had brought with him and [redacted] released the original disc pack to [redacted] in exchange for the other one containing the copy of the data. [redacted] signed a receipt for all of these items and nothing further occurred at this time. b6 b7C

Later that same day, [redacted] was completing the inventory of The Guild files using the copied disc pack and he discovered that the four CDIR files had been encrypted. Since [redacted] was able to see the data within the CDIR files in unencrypted form during the afternoon of November 14, 1980, [redacted] opined that the encryption must have occurred after [redacted] was killed and before [redacted] took the MM system off of the National CSS network later that afternoon at [redacted] request. [redacted] called [redacted] during the evening of November 15, 1980, and informed her of this development. b6 b7C

MM's system continued to remain off of the National CSS network and, following the advice received from National CSS, MM changed all of their user and system IDs during the evening of November 17, 1980, and the daytime of November 18, 1980, in order to prevent future unauthorized access to MM's system by The Guild. National CSS had said that this procedure was all that was necessary to completely lock out The Guild. MM then brought their system back onto the network on November 18, 1980.

Between 3:00 a.m. and 7:00 a.m. on November 19, 1980, while MM was not staffed, there were several attempts by The Guild to log onto the MM computer system without success. Attempts were made to log onto the system using an ID that didn't print out on the console log and then whoever it was logged onto the VPSYSMGR ID. [redacted] determined this from the MM console logs but he was unable to ascertain what was done after the person logged onto the VPSYSMGR ID. b6 b7C

This was the only unauthorized access since November 15, 1980, that [redacted] was aware of and he had no information or knowledge of any other unauthorized entries of any computer systems as a result of using data from the purloined CDIR files. b6 b7C

[redacted] advised that MM does not use any other "value added" data communications network except National CSS but they do use the Southern Pacific Communication Network for voice communications. b6 b7C

[redacted] made some notes on MM's computer system on November 17, 1980, of the events that had occurred prior to that time and he also made some typewritten notes of activities that occurred thereafter. [redacted] reviewed these notes at various times during the various interviews in order to refresh his memory. After talking over these points and the sequence of events, [redacted] agreed that the chronology of events and details as told to SA [redacted] and recorded by him in his notes represented [redacted] best current recollection of what happened, and that he had been mistaken if any points in his notes conflict with his FBI interview. b6 b7C

[redacted] made available to SA [redacted] the original printouts described hereafter after he and SA [redacted] had initialed them for identification purposes: b6 b7C

1. One continuous printout from MM printer of 55 items starting at 5:33 p.m. November 15, 1980 to approximately 6:10 p.m. on November 15, 1980.

2. One continuous printout measuring approximately 4¼" high from MM printer of 242 items starting at 6:05 p.m. November 15, 1980 to 6:17 p.m. November 15, 1980.

3. One continuous printout representing MM system console log for the period from 5:28 p.m. September 20, 1980, to 11:49 a.m. on September 27, 1980.

In addition, [redacted] made available copies of his computerized and typewritten notes that he made, and he will retain his original notes for possible future use. The above items are being retained by the FBI as evidence. b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 6/3/81

[redacted] b6 b7C

National CSS, San Francisco, was contacted relative to his knowledge of the use of telephone number (415) 989-3930 during the period August through December 1980.

[redacted] stated that the telephone number was the main published number for that part of National CSS in San Francisco in which he worked. He stated that a person desiring to talk to him or to a person in his branch would call that number; however, that number was also used for reaching a wide variety of persons and other activities within National CSS. He continued that all calls to this number went to a PBX switchboard and that the calls were then routed to the particular person or section by use of internal extensions. [redacted] stated that neither he nor his branch had any direct telephone number and that all calls came through this published number. He provided no additional pertinent information. b6 b7C

196-397-27

Investigation on 5/27/81 at Oakland, Calif. File # SF 196A-795

by SA [redacted] / sdc Date dictated 5/29/81 b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 6/3/81

[redacted] b6 b7C

[redacted] National CSS, Inc., 650 California Street, Suite 1840, San Francisco, telephone [redacted], was interviewed concerning his knowledge of telephone number (415) 989-3930 during the period of August through December 1980.

[redacted] advised that the telephone number was the published number for the Remote Computer Service Division of National CSS, which was then the time sharing part of the company. [redacted] continued that this telephone number went into a PBX switchboard and was then routed to a particular person or unit within the division. He stated that no record was made of calls received and processed through the PBX and that there was no way of tracing a call made to that number at a particular time. He provided no additional pertinent information.

b6 b7C

196-397-28

Investigation on 5/26/81 at San Francisco, Calif. File # SF 196A-795

by JJW SA [redacted] / sdc Date dictated 5/29/81

b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/13/81

[redacted] Marsh & McLennan, 13th Floor, #3 Embarcadero Center, San Francisco, telephone [redacted] was interviewed at his place of employment concerning his knowledge of the unauthorized access to Marsh & McLennan's (MM) computer on November 11, 1980. He voluntarily related the following information: b6 b7C

Several months ago, they were informed by the San Francisco Branch of National CSS that they had reason to believe that the National CSS Network had been used by someone on the East Coast who possibly gained unauthorized access into MM's computer at 4:37 a.m. on November 11, 1980. [redacted] explained that MM had acquired a National CSS 3200 Series mini-computer system on or about November 2, 1980, and that the system was still undergoing acceptance testing at the time when this alleged unauthorized access occurred. MM did not take final delivery of the system until November 27, 1980, and it was [redacted] understanding that there were 31 other similar systems that National CSS had installed and were operational in that same configuration. b6 b7C

Following receipt of this information, MM undertook an extensive project of reviewing the system console logs for November 1980 and they found several entries of a suspicious nature. The first entry was at 4:37 a.m. on November 11, 1980, and a user utilizing the ID of "VPSYSMGR" logged onto MM's computer via the National CSS Network port "NCS 1", which [redacted] understood to be located in the State of Connecticut. The next entry on the log was at 4:54 a.m. and the person using the same ID logged off MM's system. Immediately following that, MM's computer system (which had been up and running some work at the time in background mode) then attempted to take a "snapshot dump" prior to the system crashing, but this dump attempt was aborted due to the lack of an available dump slot. The log indicated that the user ID of "VPSYSMGR" was responsible for whatever happened to cause the attempt to take a snapshot dump and for the system to crash. b6 b7C

Due to the configuration of MM's system, they were unable to tell what it was that the user ID "VPSYSMGR" was doing during the seventeen minutes that he was logged onto the MM system, nor could they tell what it was that caused the crash. Since "VPSYSMGR" is the highest level of user ID on the 3200 Series National CSS system,

196-397-29

Investigation on 5/11/81 at San Francisco, Calif. File # SF 196A-795

by SA [redacted] / sdc Date dictated 5/12/81 b6 b7C

whoever was using that ID had the highest level of access into MM's computer. Since virtually all of MM's computerized data is simultaneously on line in disc pack form, this user would have been able to literally do anything he wanted with MM's data, including reading the files, writing to them, or having them print out on a remote terminal via the National CSS Network.

Since being notified of the apparent unauthorized access, MM has done considerable research of the data and other non-computerized support records and they are 99 per cent sure that the unauthorized user did not change any of the files as all things balanced out after the entry. Further, MM changed all of their ID and passwords and they are now satisfied that no one can gain unauthorized access. National CSS sent over technicians, including the person who authored "NOMAD", a software package offered by National CSS, and these persons tried for some four hours to make unauthorized penetration into MM's system without success.

MM's [redacted] personally reviewed the console logs and did the other research, but they were unable to determine what it was the unauthorized user was doing and they were unable to discover anything that had been altered or damaged in any way. MM is confidant that the person entering via the National CSS port "NCS 1" was, in fact, an unauthorized user since MM always goes through the "SUNY" port. b6 b7C

Prior to being notified of this incident, MM was not aware that certain standard passwords were uniformly set up by National CSS whenever they delivered a particular system, and they have since notified National CSS that customers should be notified that these passwords are the same for all other similar series systems and that they should be immediately changed when a customer takes final acceptance of the computer. [redacted] was not aware if National CSS has notified the other 31 users of the National CSS 3200 Series system, nor was he aware if any of them had experienced any instances of unauthorized access. b6 b7C

Based on what National CSS told him, [redacted] was of the opinion that the unauthorized user was a disgruntled former National CSS employee and that he was probably trying to get into the operating system within MM's computer in order to cause National CSS some problems, and that this effort either caused the system to abort and crash or for some other reason he was unsuccessful in these efforts. b6 b7C

He had no independent information to substantiate this view and it was pure conjecture on his part.

At the conclusion of the interview, [redacted] provided SA [redacted] with the original sheet of MM's console log covering the period from 7:42 p.m. and 11 seconds, November 10, 1980, through 4:54 a.m. and 25 seconds, November 11, 1980. He and SA [redacted] initialed this document for identification purposes and it is being retained as evidence by the FBI. [redacted] advised that the document would be destroyed in one year anyway and that it was not necessary to return it when no longer needed for investigative purposes. b6 b7C

He provided no additional pertinent information and agreed to notify SA [redacted] should he come across any additional information or instances of other unauthorized access to MM's computer system. b6 b7C

FD-302 (Rev. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/20/81

[redacted] b6 b7C
[redacted] National CSS, Inc., 430 South Pastoria Avenue, Sunnyvale, telephone [redacted] was interviewed at his place of employment concerning the receipt of a phone call on or about November 14, 1980, either by himself or his department. [redacted] voluntarily related the following information:

He was working in his capacity on November 14, 1980, but had no recollection of receiving any telephone call during the afternoon hours from either Bruce I. Paul or anyone from a company called "The Guild". Prior to his interview, he had no contact or knowledge of either Paul or The Guild nor was he aware of anything pertaining to the unauthorized possession of National CSS proprietary information on a disc pack located on a computer owned by Mediametrics of Moraga, California.

[redacted] was acquainted with [redacted] when the latter worked for National CSS in the San Francisco branch, but, after being told of the substance of what [redacted] had related during his interview, [redacted] had no recollection of the matter under investigation. No records are kept of such inquiries received by his department and he opined that, if any inquiries were made within his department, they would have been quickly answered by either himself or one of his subordinates. Since there is absolutely no way of tracing back through a system to see who was using a particular ID and password, any caller inquiring about such a matter would have been informed of this without any need for researching the matter. b6 b7C

[redacted] agreed to determine from National CSS records which of his subordinates were working during the afternoon of November 14, 1980, and to then query these employees to ascertain if any of them recalled receiving such a call from anyone. Should any positive information be disclosed, [redacted] agreed to immediately notify SA [redacted]. He related no additional pertinent information. b6 b7C

196-397-30

Interviewed on 2/9/81 at Sunnyvale, California File # SF 196A-795

by SA [redacted] /cea Date dictated 2/13/81 b6 b7C

FD-302 (Rev. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/10/81

[redacted] National CSS, Inc., 650 California Street, Suite 1840, San Francisco, telephone [redacted] was contacted at his place of employment for the purpose of making back-up copies of certain magnetic media and to then secure the original items as evidence in connection with the unauthorized possession of passwords and customer account numbers belonging to National CSS and found on a computer disc pack located in the computer room of Mediametrics (MM) of Moraga, California. SA [redacted] was present throughout this process, which was done on a National CSS 3200 Series mini-computer known as SFR-1. This computer system was shut down during this process and was not accessible to normal users.

SA [redacted] proceeded into the private office of [redacted] National CSS, and located a sealed box that [redacted] turned over to SA [redacted] This box contained a disc pack and a number of magnetic tapes that were original items of evidence concerning this investigation and they had been placed in the box by [redacted] on January 6, 1981, in SA [redacted] presence. SA [redacted] then sealed the container in such a manner that any entry into the box could be detected. The container was inspected by SA [redacted] and all seals were found intact. The box was then opened and its contents inventoried. The following items were found therein and each was appropriately marked by SA [redacted] with his initials, the date, and the item number indicated below:

1. BASF Brand magnetic tape number Q2 164 0 X304 A3 25 labeled "DIRECTORY/BACKUP 000117 ENTIRE PACK".

2. BASF Brand magnetic tape # 12 276 0 A483 A2 07 labeled "TP DUMP GUILD" and "0918".

3. IBM Brand magnetic tape # 37 2078622 labeled "DDR" and "R2189".

4. IBM Brand magnetic tape # 16 2152969 labeled "DDR T1".

196 390-31

Interviewed on 1/21/81 at San Francisco, Calif. File # SF 196A-795

by SA [redacted] / sdc Date dictated 1/27/81

5. Memorex Brand magnetic tape # 25E HJ 3512W A1 and # R37635 CD35 4534 and labeled "TP2".

6. IBM Brand magnetic tape # 05 1025353 labeled "TP3".

7. IBM Brand magnetic tape # 0 3017529 labeled "TP4".

8. Memorex Brand magnetic tape # 25JRA909 labeled "COPY OF AIMS DUMP FOR [redacted]. b6 b7C

9. Memorex Brand disc pack, serial number 7008291, labeled "TMSPK1".

These original items of evidence were removed to the National CSS computer room for processing. Using a standard utility package called "DASD Dump Restore Program", the contents of the disc pack were duplicated onto magnetic tapes. A copy was obtained of the nine page National CSS Technical Bulletin on this utility package and it was secured as Item #10. Each of the five magnetic tapes used with this utility program were Memorex Brand magnetic tapes # 25JRA909 which were all labeled "PACK TMSPK1 DDR DUMP", along with the appropriate reel number that each tape represented. These tapes were secured as items number 11 through 15. A copy of the utility package used in this process was put out onto an IBM Brand magnetic tape and was labeled "DDR 1.1 STAND ALONE 1-21-81" and was secured as Item #16.

Copies were then made of the two original backup tapes (Items 1 & 2 herein) using a standard tape-to-tape utility. Both copies were put out on the same type of Memorex Brand magnetic tape as the contents of the disc pack and these were labeled "COPY OF DIRECTORY BACKUP TAPE 000117" (Item #17) and "COPY OF TP DUMP GUILD" (Item #18).

All of the magnetic tapes that represented copies of the original evidence were appropriately marked on the outside containers and on the magnetic tape itself for identification purposes. These items, along with all of the original evidence, were then placed into sealed containers and kept in the possession and control of SA [redacted]. At the conclusion of the processing, SA [redacted] secured the original system console log made from computer SFR-1 for the period 9:52 AM, January 21, 1981, to 11:41 AM, January 21, 1981, which shows the exact sequence and further details of the copying process. This was secured as Item #19. b6 b7C

3
SF 196A-795
FTW/sdc

Item numbers 3 thru 8, and 11 thru 18 are being retained at the San Francisco Division of the FBI under appropriate chain of custody, while Items 1, 2, 9, 10 and 19 will be forwarded under suitable safeguards and chain of custody to the New Haven Division of the FBI.

FD-302 (Rev. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/23/81

[redacted] b6 b7C

[redacted] was interviewed at his home concerning his recollection of receiving a phone call on or about November 14, 1980, while employed by National CSS. [redacted] voluntarily related the following information:

[redacted] b6 b7C

[redacted] He had no recollection at all of receiving a phone call from an individual named Bruce Paul or from anyone representing a company called "The Guild" nor had he had any prior dealings with either Paul or The Guild. He was familiar with Mediametrics, in that he had heard prior to his resignation from National CSS that some passwords of National CSS customers were found on the Mediametrics computer. His branch did not provide technical support to Mediametrics as they were handled by a different branch of National CSS.

[redacted] had a vague recollection of receiving a phone call sometime within the last six months of his employment with National CSS, but he was unable to narrow it down when this ocurred. This call was a rather short call and one that he had no reason to pay particular attention to at the time. The call was from a male who gave his name and [redacted] does not believe that he had any prior contact with this individual. He could not recall this name at all and he could not associate the name of Bruce Paul or The Guild with this phone call. b6 b7C

At any rate, the caller said something about wanting to know if there was any way of determining if a person using a particular computer ID was calling from a National CSS office. The caller specifically mentioned Mediametrics as being the system that had been logged onto and that he wanted to find out information about the location of a person using an ID on that system. [redacted] believes that the caller said something about having tried to get in touch with someone else within National CSS, possibly the mini division, but that he could not reach that person so he had called [redacted] branch. b6 b7C

196-397-32

Interviewed on 1/19/81 at Oakland, California File # SF 196A-795

by SA [redacted] /cea Date dictated 1/20/81 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

told the caller that, in his opinion, there was no way of tracing out the information that he desired but that such a problem was really outside of his area of expertise. believes that he referred the caller to the Data Communications Department of National CSS in Sunnyvale since they would be the ones who would know the answer to the caller's question. The call lasted about five minutes and thought there was a good chance that the caller was satisfied by explanation that there was no way of tracing out a computer connection in the manner that he desired. made no notations about this call nor did he notify anyone about having received it. b6 b7C

reviewed his appointment calendar for the middle of November, 1980, but there was no notations pertaining to this call found thereon and nothing on it served to refresh memory as to when this call occurred. He provided no additional pertinent information and agreed to notify SA should he recall anymore details. b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/15/81

[redacted] b6 b7C National CSS, Inc., 650 California Street, Suite 1840, San Francisco, California, telephone [redacted] and who resides at [redacted] telephone [redacted] was interviewed at his office concerning his knowledge of the unauthorized possession of passwords and customer account numbers belonging to National CSS and found on a computer disc pack located in the computer room of MediaMetrics (MM) of Moraga, California. Present throughout the interview was [redacted] voluntarily related the following information:

He has been employed by National CSS for approximately [redacted] b6 b7C and, as part of his employment, he has had dealings with [redacted] as well as other officials and employees of MM since MM is a customer of National CSS. The first indication that proprietary information belonging to National CSS was being possessed without authorization came during the afternoon of Thursday, November 13, 1980.

On that date, [redacted] was in Los Angeles on business and had occasion to talk with [redacted] who was [redacted]. During their telephone conversation, [redacted] mentioned to him that [redacted] had called her and asked her assistance in gaining access to new passwords to the MM computer system that were being used by "The Guild". It was [redacted] understanding that The Guild was a customer of MM and that, for reasons unknown to him, MM and Guild were having some type of disagreement. At any rate, [redacted] had discovered that The Guild had changed their authorized passwords without notifying MM and [redacted] desired to determine what these new passwords were. [redacted] indicated that she assisted [redacted] as requested and determined what the new passwords were but that, when she attempted to log onto MM's computer using these new passwords, she found out that The Guild or someone had apparently added additional security procedures without MM's knowledge that would block access to The Guild ID. [redacted] explained to [redacted] that she was able to gain access to The Guild ID using undocumented system commands and that [redacted] was satisfied with what she had done since he was now able to log onto The Guild ID.

[redacted] mentioned this to [redacted] after the fact but [redacted] advised that he would have authorized her to do the procedure that she did. There was no other indication of trouble that [redacted] was aware of prior to that time.

196-397-33

Investigation on 1/12/81 at San Francisco, California File # SF 196A-795

by SA [redacted] /cea Date dictated 1/14/81

b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted], and they returned to the office at about 2:30 p.m. At that time, [redacted] advised both of them that [redacted] had contacted her again and indicated that he [redacted] had discovered "CDIR" data on a disc pack on the MM computer in an area reserved for The Guild ID. [redacted] advised that [redacted] said that he had used this "CDIR" data, which consisted of passwords and customer account information, to log onto some of the IDs on the National CSS Commercial Network System. [redacted] gave him no further details but [redacted] explained, if what [redacted] said was true, it would have been a most serious breech of security into the National CSS system and would have had monumental consequences.

b6
b7C

[redacted] immediately called [redacted] National CSS in Wilton, Connecticut. They had a phone conversation that lasted some 30 minutes and [redacted] explained the limited amount of information that he knew about to [redacted] They discussed the ramifications of the unauthorized possession of the "CDIR" data and [redacted] was in the room when this conference call was held. [redacted] said that someone should verify what [redacted] had said by looking at this "CDIR" data themselves. [redacted] indicated that he would confer with top National CSS officials and would get back to [redacted] before the end of the day.

b6
b7C

It was at this time that [redacted] went to a terminal located within National CSS in San Francisco and, using information that she obtained from [redacted] during a telephone call, she logged onto The Guild ID and gained access into the reserved area of the disc pack being used by The Guild. While this was in progress, someone identifying themself as "Bipper" from The Guild came onto [redacted] terminal and asked who it was that was using The Guild ID. [redacted] did not answer the message but continued with the work that she was doing and whoever had come onto her terminal then logged her off The Guild ID right in the middle of the work that she was doing.

b6
b7C

Between this time and [redacted] return call later that afternoon, [redacted] called [redacted] back at MM and explained to him the seriousness of the problem at hand. He told [redacted] that, as far as they could determine, the CDIR data was live and that he was requesting that MM take their computer system off of the National CSS network until such time as [redacted] could meet with [redacted] the following morning to secure the disc pack containing the CDIR data. [redacted] agreed to do this, and they made arrangements to meet the following day at MM.

b6
b7C

Either during this phone call with [redacted] or during their meeting the following day, [redacted] indicated to [redacted] that he had received a phone call from Bruce I. Paul, an employee of The Guild. According to [redacted] Paul wanted to know who was logged onto The Guild ID but that [redacted] did not tell him anything. [redacted] could not recall any other details that [redacted] may have told him. It was [redacted] impression based on what [redacted] told him that The Guild was aware that National CSS had discovered the CDIR data. b6 b7C

At approximately 5:00 p.m. on November 14, 1980, [redacted] called [redacted] back in a conference call with the following officials from Connecticut being on the line: [redacted] National CSS. [redacted] were on the San Francisco end of the call and it lasted over 30 minutes long. The primary purpose of the conference call was to discuss the ramifications of the breech of security and what response National CSS would make to it. [redacted] was instructed to obtain the original disc pack from MM and he informed them that he would do so the following day. There were no new revelations made in that phone call. b6 b7C

On Saturday, November 15, 1980, at approximately 8:00 a.m., [redacted] met [redacted] at MM. [redacted] had brought six magnetic tapes with him and, using the National CSS Utility named "DDR.DASDI", he attempted to copy the entire contents of the disc pack which contained The Guild reserved space onto the magnetic tapes. As he was doing this, he obtained read errors on the second tape so he was unsuccessful in this effort. He then made a disc to disc copy of the pack using an extra disc pack that he brought with him. This copied disc pack was then given to [redacted] took possession of the original. The utility that [redacted] used is a "stand alone" package that has its own operating system to it. b6 b7C

In addition to taking possession of the original disc pack, [redacted] received two magnetic tapes from [redacted] The first tape was the latest normal backup tape made by the MM system that contained the contents of the original disc pack. The second tape was a special backup that had been made by [redacted] and only contained the data under The Guild ID that appeared on the original disc pack. [redacted] also received a number of terminal logs, console logs, inventory listings, and other printouts. [redacted] wanted [redacted] to sign a receipt for these items so [redacted] called [redacted] to get permission to sign it. [redacted] gave permission and the receipt along with the agreement as to the use of the material [redacted] received was then executed. b6 b7C

[redacted] recalled that there was a second call either from or to [redacted] while [redacted] was at MM but he could not recall what this call was about other than it had something to do about the matter at hand. b6 b7C

Throughout November 15, 1980, and on November 16, 1980, [redacted] either made or received a number of phone calls from his company headquarters, but these dealt with internal company matters or his bringing company officials up to date on what had happened. b6 b7C

At approximately 10:00 a.m. on Monday, November 17, 1980, [redacted] telephoned [redacted] in response to a message that [redacted] had left earlier that day. [redacted] informed him that the CDIR data on the disc pack had been encrypted prior to the time that [redacted] acquired the original disc pack. [redacted] opined that [redacted] discovered this while he was working with the copied disc pack that [redacted] had made. [redacted] also advised him that they had checked MM records regarding spooling traffic under The Guild ID and found the following traffic: b6 b7C

Date	Spooling Number
July 24, 1980	21150002
" " "	21145941
" " "	21145951
July 15, 1980	10125448
" " "	10125526
" " "	10125552
July 18, 1980	18100827
" " "	18123459

[redacted] passed this information onto National CSS technical personnel but they were unable to trace it back through the system to determine the file name, type, or length that was sent over the network on these days and spooling sessions. b6 b7C

At approximately 10:45 a.m., on November 17, 1980, [redacted] decided to check the special backup tape that [redacted] had made of The Guild ID data to see if it was also encrypted. He went to National CSS computer named "SFR-1" and mounted the backup tape himself. He loaded the CDIR file named "SUNY" onto his own ID and stored it on his assigned area of a disc pack. He then edited this file and found that it was not encrypted. He looked up his own password on the file and found that it was valid at that time, although it has since been changed by [redacted] then erased the CDIR file from his disc pack area and secured the magnetic backup tape again. b6 b7C

Sometime during the week of November 17, 1980, [redacted] requested that [redacted] send some data from the CDIR file contained on this same backup tape over the network to [redacted] National CSS Headquarters. [redacted] gave the original backup tape to [redacted] who then mounted the tape and sent the requested data over the network. [redacted] returned the backup tape to [redacted] possession within approximately one hours. b6 b7C

On November 24, 1980, [redacted] took possession of the terminal logs that he had received from [redacted] and made xerox copies of them at the request of [redacted]. The copies were forwarded to him and the originals returned to [redacted] b6 b7C

Except as contained herein, [redacted] has maintained custody and control over the original disc pack, original backup tapes, and original logs and printouts. The disc pack and magnetic tapes were placed by [redacted] into a container on January 6, 1981, and then sealed by SA [redacted] This sealed container has been in [redacted] possession since that time. On that same date, he released all original logs and printouts to [redacted] for use during her interview and for release to SA [redacted] thereafter. b6 b7C

[redacted] He described [redacted] as being a very competent person professionally, and he had no problems with her at all. [redacted]

[redacted] was asked if he knew of any incidents of possible unauthorized access to any computers or data that may have resulted from the compromising of the CDIR data, but he knew of no such incidents. He was asked specifically about any knowledge of the entry to [redacted] and [redacted] computer system but he had no knowledge about this prior to his interview. b6 b7C

[redacted] provided SA [redacted] with a copy of the receipt he signed for [redacted] on November 15, 1980, as well as a copy of six pages of notes that he made concerning this incident starting on November 16, 1980. He provided no additional pertinent information. b6 b7C

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/9/81

[redacted] b6 b7C

[redacted] was interviewed at the offices of National CSS, Inc., 650 California Street, Suite 1840, San Francisco, concerning her knowledge of the unauthorized possession of passwords and customer account numbers belonging to National CSS and found on a computer disc pack located in the Computer Room of Mediametrics (MM) of Moraga, California. Present throughout the interview was [redacted]

[redacted] b6 b7C voluntarily related the following information:

[redacted] b6 b7C

[redacted] She primarily dealt with [redacted] but did have contact with other MM personnel. About one year prior to November of 1980, she was told by [redacted] that he had entered into some type of agreement with a computer consultant company called "The Guild", located in the State of Connecticut. As she recalls, [redacted] said that the agreement was made with [redacted] of "The Guild" and was to modify the application software that was being used on the National CSS hardware that MM was using and that, in exchange, MM was going to give "The Guild" free computer time and disc storage space. [redacted] told her that he entered into the agreement with "The Guild" as he was dissatisfied with the performance of National CSS with regards to software modification. Except for her conversations with [redacted] she had no other knowledge or involvement in the relationship between "The Guild" and MM.

In the afternoon of November 13, 1980, [redacted] called her at her office and explained that he and "The Guild" were having a disagreement in regards to The Guild doing the software modification and that he did not feel that The Guild was living up to their part of the bargain. b6 b7C

19½-391-34

Investigation on 1/6/81 at San Francisco, Calif. File # SF 196A-795

by SA [redacted] / sdc Date dictated 1/9/81 b6 b7C

[redacted] wanted to get The Guild off of MM's computer system all together, but wanted them to finish the particular part of the software modification that they were presently doing. [redacted] indicated that he had tried to get into the reserved area of the disc pack that was assigned to The Guild but that he was unable to do so because The Guild had changed the password without notifying MM. [redacted] said he had determined this when he had tried to log onto The Guild's identification and the known passwork was rejected. b6 b7C

[redacted] wanted [redacted] to tell him how he could find out what the new Guild password was and she explained this procedure to him over the telephone. She then went to a computer terminal located at National CSS and logged onto the MM computer through the National CSS Network System. She then did the required technical procedure to enable her to find out what the passwords for MM's system were and, once they were displayed on her terminal, she gave the information over the telephone to [redacted] b6 b7C

[redacted] then tried to log onto MM's computer using the new password for The Guild, but she was unable to do so because The Guild had put on additional security procedures that were not part of the normal system operating software. She then told [redacted] what the necessary system procedure was to enable him to override this added security procedure and [redacted] did this while talking to [redacted] on the telephone. [redacted] was able to log onto The Guild's identification and then read some security programs to [redacted] over the telephone. She then gave [redacted] the necessary information about what certain codes in the security programs meant so that he could have access to the area of the disc pack that MM had allocated for The Guild's use. b6 b7C

[redacted] indicated to her that he was going to try to see what type of information was in the reserved Guild space on the disc pack but [redacted] was not involved further in this procedure. The telephone call was concluded and she had no further involvement in this matter until the following day. b6 b7C

At about noon on November 14, 1980, [redacted] called [redacted] at National CSS and, in a joking manner, asked her what she would give for all of the passwords to the National CSS Network System and all of the National CSS customer identification numbers. [redacted] advised her that he had found files from several of the National CSS mainframe computers in that area of the disc pack assigned for use by The Guild. [redacted] said that he was calling to advise National CSS of this apparent unauthorized possession of the passwords and identification numbers and asked [redacted] what the company wanted to do. b6 b7C

[redacted] reported this information to [redacted] National CSS Computer Division, upon his return to the office and several other high-ranking officials of National CSS. At about 3:00 p.m. on that same day, she was instructed by [redacted] to attempt to log onto MM's computer system using The Guild's identification/password and get the passwords contained thereon to determine if they were live data. She then communicated telephonically with [redacted] and obtained from him the necessary keys to override the extra security measures that surrounded The Guild passwords. b6 b7C

[redacted] then went to a computer terminal located at National CSS. This terminal was equipped with a printer rather than a video monitor and it produced a written log of everything she did and the responses by MM's computer. After reviewing this terminal log, [redacted] recalled that she logged onto MM's computer using The Guild identification at approximately 2:58 p.m. on November 14, 1980, and that she used the general identification assigned to The Guild. She then listed the contents of the files located in that part of the disc pack allocated to The Guild's use and found, among other things, four files that appeared of significance to her. Three of these files (named "East", "Suny", "HSYS") had the same names as the "CDIR Data" files for each of the three mainframe National CSS computers. The fourth file found was named "BIPUSER" and she later found that this was a copy of the "HSYS" file that also appeared on the disc. b6 b7C

She then determined that the "HSYS" file had been last written to on August 4, 1980, and had last been accessed on November 13, 1980. As she was giving the commands to list out the first 40 records within the "HSYS" file she was interrupted by a message reading, "From BIPPER / Guild : Who the hell is this!!!!" She explained that this originated from someone using the password "BIPPER" at The Guild and that they had apparently tried to log onto the same general Guild identification that she was using. [redacted] continued that, more than likely, the person who unsuccessfully tried to log on the general Guild identification then used a "shadow" identification to get onto the system and then type out the indicated message. b6 b7C

After receiving the above message, which to her meant that somebody at The Guild was attempting to find out who was accessing The Guild's data, she ignored it and continued with her listing of the contents of the "HSYS" file. As she was in

the process of doing this, she was again interrupted and was logged off of the MM computer at 3:03 p.m. [redacted] explained that any user of the MM computer system with a privileged class of identification in codes A or B could cancel out any other user and log them off the system. b6 b7C

[redacted] then tried to log back onto the computer using the MM System Manager ID but she could not get on as she did not know the correct password. She either then called [redacted] to find out the password, or through trial and error was able to guess what it was so that she could successfully log on as the System Manager. She then attempted to locate a file named "SHOGUN" that [redacted] had said he had found in The Guild's area of the disc pack. She could not find this file so she then went into the file named "EAST" and the file named "SUNY". She found her own valid password to the National CSS Network, as well as the suspected valid passwords of other CSS employees. She noted that the "CDIR" records in these unauthorized password files were not of the same configuration as they appear on the National CSS computers. She explained that the "CDIR" records on the National System consist of 132 characters of information, whereas the unauthorized copies of these files had only about 30 characters to them. These abbreviated records consisted of the customer ID number, the password, and some other alpha-numeric data having to do with accounting functions and disc storage space. It was her opinion that these abbreviated "CDIR" records could have been edited by a special program that was then kept somewhere in The Guild's disc space or that the general system data base manager could have been used to edit the records. She noted that the genuine "CDIR" records do not have the customer ID numbers and passwords, as the first two fields so the abbreviated records were not merely a listing of the first thirty characters of each record. b6 b7C

After obtaining a partial listing of each of the unauthorized "CDIR" files, she signed off the MM computer at approximately 3:23 p.m. She was informed by [redacted] at a later time that he had made a complete listing of the entire portion of the disc pack containing The Guild data, including all of the passwords. Further, he told her that he had made a back-up tape of the contents of The Guild's disc space. Based on her examining the contents of the unauthorized "CDIR" files, she was of the opinion that it was indeed live data that definitely should not be in the possession of anyone outside of National CSS. Either herself or [redacted] told [redacted] that afternoon that he should take the MM computer system off of the National CSS Network so as to prevent any access to the unauthorized b6 b7C

"CDIR" files. [redacted] agreed to do this and they set an appointment to meet the following morning at MM for the purpose of retrieving the unauthorized files. b6 b7C

At approximately 8:00 a.m. on Saturday, November 15, 1980, [redacted] met with [redacted] at MM. At this time, [redacted] gave [redacted] the following items: b6 b7C

1. The terminal logs showing activities on The Guild terminal that had been initiated by [redacted] b6 b7C

2. One set of regular back-up magnetic tapes for the MM computer system.

3. One set of special magnetic tapes containing a dump of all data in The Guild disc space.

4. The original disc pack in which The Guild had reserved space and in which the unauthorized "CDIR" files resided.

5. Various printouts of Guild files that [redacted] had made. b6 b7C

Prior to their leaving the MM computer site, a complete copy of the disc pack was made and given back to [redacted] for his use. The aforementioned items were retained by [redacted] in a secure condition for possible future use. b6 b7C

On either November 14 or 15, 1980, [redacted] told [redacted] that he had received a telephone call from Bruce I. Paul while [redacted] was examining the contents of the unauthorized "CDIR" files during the afternoon of November 14, 1980. Paul is a former Systems Programmer with National CSS and who was then an employee of "The Guild". According to [redacted] Paul wanted to know who was logged onto The Guild's ID on the MM computer. [redacted] said that he told Paul that he didn't know and that it was probably some National CSS Systems Programmers doing some routine work. b6 b7C

Sometime around this period, [redacted] also told her that Paul had called [redacted] of National CSS to find out who was on The Guild's ID but that [redacted] had told Paul that he did not know and could not find out for him. [redacted] did not recall if [redacted] said that Paul had told him this or if he had talked to [redacted] and [redacted] mentioned the conversation with Paul. [redacted] has never talked with Paul herself and knew nothing about him prior to this incident. b6 b7C

During the afternoon of November 15, 1980, she received a telephone call from [redacted] who advised her that the four unauthorized "CDIR" files on The Guild disc space had been encrypted and that the encryption took place during the afternoon of November 14, 1980, shortly after she had been looking at these files. The details of the encryption were contained on the terminal log initiated by [redacted] and the effect of this procedure is to scramble the contents of the four unauthorized "CDIR" files so that the contents do not make any sense unless they are decrypted by a person having the encryption key or deciphered. b6 b7C

[redacted] she received numerous telephone calls from [redacted] regarding this case. She could not recall the details of these numerous calls except that he was telling her what he had found on the copy of The Guild disc space that he was checking. She recalled that [redacted] said that he had found a module of a Pascal Compiler on the disc space assigned to The Guild. b6 b7C

[redacted] made one other trip to MM in Moraga and believed that it was during the last half of the week of November 17, 1980, or during the first part of the week of November 24, 1980. The purpose of her visit to MM was at the request of [redacted] of National CSS Headquarters, who wanted her to review the MM system logs in order to determine if there were older copies of back-up tapes that would contain the unauthorized "CDIR" files in unencrypted form and also to see the history of The Guild's use of MM's computer. Further, she was to look for anything suspicious on the logs that may relate to the unauthorized possession of the "CDIR" files. As she recalled, she started with the logs dating November 1, 1980, that had been printed out by the console printer in the MM computer room and these logs continued until the date that she was reviewing them. She brought back all of these logs with her, as well as printouts containing the directory of MM's disc pack layout. She turned all of these over to [redacted] who kept them in his possession for future use. b6 b7C

On November 26, 1980, the day before Thanksgiving, she received a telephone call from [redacted] (National CSS Headquarters), who advised her that they had evidence of a possible unauthorized access to two computers in San Francisco. [redacted] explained to her that they were reviewing all computer accesses through the network node used when The Guild accesses the National CSS Network during the time periods that The Guild was on the system. [redacted] advised that there was a suspected b6 b7C

unauthorized access to the computer of Marsh and McLennan, Inc. of San Francisco, a large insurance company. The other was to the National CSS Series 3200 computer known as "SFR-1" located at the National CSS Computer Division, 650 California Street, Suite 1840, San Francisco. She reviewed the system logs for "SFR-1" and found that there had been an attempted unauthorized access to the National CSS computer as suspected by [redacted] but that no penetration had occurred. For this reason she did not retain the system log nor forward a copy of it to [redacted] b6 b7C

With regards to the Marsh and McLennan computer, she contacted [redacted] at their computer center and asked to review their system logs for the period in question. She did not advise anyone at that company of the possible unauthorized access to their computer but told them it had to do with a technical problem that National CSS Headquarters had asked her to check out. She looked through the logs and determined that there was a hook-up with the Marsh and McLennan computer for approximately twenty minutes and that, as far as she recalls, this occurred at 3:00 a.m. She made a copy of the system log sheet showing this probable unauthorized entry and sent it to [redacted]. She did not make any further inquiries within Marsh and McLennan nor did she know if anyone else had made inquiries or notification there. b6 b7C

[redacted] then provided SA [redacted] with the original documents indicated hereafter that she had received from [redacted] and she offered her explanations about these documents as indicated. Further, she placed her initials and date on each of the items as did SA [redacted] who also placed the consecutive number on the document as indicated below: b6 b7C

1. The terminal log created on the terminal that [redacted] used between 2:58 p.m. - 3:23 p.m. on November 14, 1980, when she logged onto the MM computer using the general Guild ID. b6 b7C

2. Terminal log for period from 3:27 p.m. to 3:47 p.m. on November 14, 1980, of activity between the MM computer and a terminal using The Guild ID. [redacted] explained that this log (as well as items 3, 4 and 5 listed below), were made as a result of modifications to the security procedure done by [redacted] so that whenever any terminal logged onto the MM computer, a disc file was created of all transactions originating from or going to that particular terminal. This disc file was subsequently printed out in hard copy form. Whoever signed on The Guild ID checked to see what the configuration of the portion of the MM computer being used by The Guild and then checked to see a list of all work being directed to a printer but which had not yet been executed. The terminal then made an unsuccessful attempt to b6 b7C

get a hard copy list of which terminals had been using The Guild general ID. The terminal then listed out all files on that portion of the disc pack assigned to The Guild that had been accessed on November 14, 1980. This list included the three unauthorized "CDIR" files but not the file named "BIPUSER". The terminal then requested, and received, the same list of files but had the last write date and time, as well as the last access date and time printed out beside the particular file. The terminal then logged off of the MM computer.

3. Terminal log for the period from 4:15 p.m. to 4:51 p.m. on November 14, 1980, of activity from or to any terminal using The Guild ID. After signing on, the terminal immediately encrypted the three unauthorized "CDIR" files, as well as the file named "BIPUSER". The terminal then checked to see who was logged onto the MM computer at the time and, upon seeing that user [redacted] (which [redacted] believes to be [redacted] Ltd., a part of The Guild), the terminal then attempted to see what [redacted] was doing on the system. The terminal then checked to see all work directed to a printer but which had not yet been executed and then checked to see if there was a street address for a customer named [redacted]. There was no reply for the [redacted] inquiry, indicating that there was no such customer in the file. A security file named "11144734" was then loaded and it's contents printed out on the terminal. The terminal then changed all four Guild passwords (READ, WRITE, BATCH, and LOG) and then printed out a portion of MM computer's system security procedure. This procedure was then changed by adding some features which [redacted] believed had something to do about adding a second password in order to log on a Guild ID. The terminal then executed these changes in security procedures to see if they worked. The terminal then logged off at 4:37 p.m. on November 14, 1980, and the remainder of this printout was under the customer ID "NEWS" and, according to [redacted] does not appear to be related to The Guild.

b6
b7C

4. Terminal log for the period 4:44 p.m. to 4:52 p.m. on November 14, 1980, of activity from or to a terminal using The Guild ID. After logging on, the terminal checked to see what work was awaiting output to a printer. The terminal then checked to see if there were any files directed to The Guild disc area but not yet placed there. A query was then made to see who was logged onto the MM system at that time and the terminal then checked to see if a program named "SER* EXEC" was on the disc (which it was not). The terminal then attempted to

run a program named "SERVER" but was not successful for reasons not apparent to [redacted]. Just prior to logging off, the terminal checked to see if the user "NEWS" was on the system and received a negative reply. b6 b7C

5. Terminal log for the period 4:57 p.m. to 5:00 p.m. on November 14, 1980, of all activities from or to a terminal using The Guild ID. After logging on, the terminal edits the MM system security procedure and then checks to see what users are on the MM system. After finding that "HSL" is logged on, the terminal checks to see what "HSL" is doing.

6. A printout entitled "Inventory Guild" created at 4:46 p.m. on November 13, 1980, which lists all of the file names, file types, items within each file, date and time each file was last written, and date and time each file was last accessed, created under The Guild ID and stored in The Guild area of a disc pack.

7. The same printout indicated for Item #6 but having been created at 4:07 p.m. on November 30, 1980.

8. A printout labeled "DIRDATA" created at 5:26 p.m. on November 20, 1980, and containing a list of all users that are on a disc pack that The Guild has assigned space.

9. Printout entitled "DIRDATA" created at 4:35 p.m. on November 20, 1980, and containing a list as described for Item #8 above.

10. Printout entitled "DIRDATA" created at 5:35 p.m. on November 20, 1980, and described under Item #8 above.

11. One terminal log starting at 6:16 p.m. on November 20, 1980, from a terminal connected to National CSS Computer "SFR-1" and listing scannings made of the disc pack on which The Guild had assigned space.

12. A two page portion of a disc pack layout similar to Items #8-10 and created at 8:03 a.m. on November 15, 1980.

13. One continuous printout containing three separate items as follows:

A. A 95 page printout of National CSS user IDs, passwords, and other data created at 5:35 p.m. on November 13, 1980.

B. Terminal log for the period from 4:54 p.m. to 5:39 p.m. on November 13, 1980, of activities from or to a terminal logged on The Guild ID. It is believed that this represents activities done by [redacted] rather than someone from The Guild. b6 b7C

C. Terminal log for the period starting 5:40 p.m. (no ending time) on November 13, 1980, of activities from or to a terminal using The Guild ID. This also is believed to reflect activities by [redacted] at MM rather than someone from The Guild. b6 b7C

14. System logs generated by the console printer of MM's computer activities from 11:58 a.m., November 10, 1980, to 3:32 p.m., November 19, 1980. These logs are continuous, connected sheets of paper except for three breaks. These four sections are identified as Parts A - D, as follows:

A. Logs from 11:58 a.m. on November 10, 1980, to 9:42 a.m. on November 15, 1980.

B. Logs from 9:43 a.m. on November 15, 1980, to 1:21 a.m. on November 19, 1980.

C. Logs from 1:21 a.m. on November 19, 1980, to 8:28 a.m. on November 19, 1980.

D. Logs from 8:28 a.m. on November 19, 1980, to 3:32 p.m. on November 19, 1980.

[redacted] provided no additional information pertinent to this investigation and agreed to notify SA [redacted] in the event she recalled anything at a later date of significance. A receipt was provided by SA [redacted] to National CSS [redacted] covering all of the original documentation that had been obtained from [redacted] b6 b7C

The original documentation obtained from [redacted] and detailed herein is being retained as evidence under appropriate chain of custody by the FBI. b6 b7C

FD-36 (Rev. 5-22-78)

FBI

TRANSMIT VIA:	PRECEDENCE:	CLASSIFICATION:
☐ Teletype	☐ Immediate	☐ TOP SECRET
☐ Facsimile	☐ Priority	☐ SECRET
X AIRTEL	☐ Routine	☐ CONFIDENTIAL
		☐ UNCLAS E F T O
		☐ UNCLAS

Date 6-24-81

TO: SAC, NEW HAVEN (196A-397)(P)

FROM: SAC, SAN FRANCISCO (196A-795)(RUC)(EBMRA)

SUBJ: BRUCE IVAN PAUL;
NATIONAL CSS, INC. - VICTIM;
FBW (A) - COMPUTER FRAUD
OO: NH

Re NH teletype to SF dated 12-3-80, NH airtel to SF dated 2-24-81, and NH airtel to SF dated 4-27-81.

Enclosed for NH are the following 49 items:

1. FD-302 (Orig + 1) on [redacted] dated 1-6-81.
2. FD-302 (Orig + 1) on [redacted] dated 1-12-81.
3. FD-302 (Orig + 1) on [redacted] dated 1-19-81.
4. FD-302 (Orig + 1) on [redacted] dated 1-21-81.
5. FD-302 (Orig + 1) on [redacted] dated 2-9-81.
6. FD-302 (Orig + 1) on [redacted] dated 5-11-81.
7. FD-302 (Orig + 1) on [redacted] dated 5-26-81.
8. FD-302 (Orig + 1) on [redacted] dated 5-27-81.
9. FD-302 (Orig + 1) on [redacted] of 12-11-80/5-26-81.
10. FD-302 (Orig + 1) on [redacted] dated 6-2-81.
11. FD-302 (Orig + 1) on [redacted] dated 6-15-81.
12. FD-302 (Orig + 1) on [redacted] dated 6-15-81.
13. FD-340 on interview notes of [redacted] and Evidence List of items obtained from her dated 1-6-81.
14. FD-340 on interview notes of [redacted] and Evidence List of items obtained from him dated 1-12-81.
15. FD-340 on copy of receipt signed by [redacted] and copy of six pages of notes made by [redacted] dated 1-12-81.
16. FD-340 on copy of four pages of computerized notes and copy of three pages of handwritten notes by [redacted] dated 1-13-81.
17. FD-340 on Evidence List of items from [redacted] dated 1-13-81.
18. FD-340 on interview notes of [redacted] dated 1-19-81.

dlf

(2) - New Haven (196A-397) (Encls. 49 in 2 boxes)
1 - San Francisco (196A-795)
FTW/dbm
(3)

196-397-35

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
JUL 6 1981
FBI—NEW HAVEN

[redacted] dlf

b6
b7C

Approved: _____ Transmitted _____ (Number) _____ (Time) Per _____

19. FD-340 on interview notes of [redacted] and Evidence List of items obtained from him dated 1-21-81. b6 b7C

20. FD-340 on copy of 9-page National CSS Technical Bulletin on "DASD DUMP RESTORE" program obtained from [redacted] dated 1-21-81.

21. FD-340 on original console log from National CSS computer "SFR-1" for period 9:52 AM, 1-21-81 to 11:41 AM, 1-21-81 and obtained from [redacted] dated 1-21-81.

22. FD-340 on interview notes of [redacted] dated 2-9-81.

23. FD-340 on interview notes of [redacted] dated 5-11-81.

24. FD-340 on original console log from Marsh-McLennan NCSS 3200 series minicomputer for period 7:42 PM, 11-10-80 to 4:54 AM, 11-11-80, obtained from [redacted] dated 5-11-81.

25. FD-340 on interview notes of [redacted] for period 12-11-80/5-26-81.

26. FD-340 on interview notes of [redacted] dated 6-2-81.

27. FD-340 on interview notes of [redacted] dated 6-15-81.

28. FD-340 on miscellaneous investigative notes of SA [redacted] for period 12-11-80/6-18-81.

29. FD-192 dated 1-6-81 on the following 14 items:

a. Terminal Log created by [redacted] for period 2:58 PM - 3:23 PM, 11-14-80.

b. Terminal Log for period 3:27 PM - 3:47 PM, 11-14-80, of activity between terminal using Guild ID and Mediametrics computer.

c. Terminal Log for period 4:15 PM - 4:51 PM, 11-14-80, of activity between terminal using Guild ID and Mediametrics computer.

d. Terminal Log for period 4:44 PM - 4:52 PM, 11-14-80, of activity between terminal using Guild ID and Mediametrics computer.

e. Terminal Log for period 4:57 PM - 5:00 PM, 11-14-80, of activity between terminal using Guild ID and Mediametrics computer.

f. Printout entitled "Inventory Guild" created 4:46 PM, 11-13-80.

g. Printout entitled "Inventory Guild" created 4:07 PM, 11-13-80.

h. Printout entitled "DIRDATA" created 5:26 PM, 11-20-80.

i. Printout entitled "DIRDATA" created 4:35 PM, 11-20-80.

j. Printout entitled "DIRDATA" created 5:35 PM, 11-20-80.

k. Terminal Log created starting at 6:16 PM, 11-20-80, between terminal and National CSS computer "SFR-1".

l. Two page portion of printout entitled "DIRDATA" created 8:03 AM, 11-15-80.

m. One continuous printout containing (i) 95 page listing of National CSS IDs, passwords, and other data created 5:35 PM, 11-13-80, (ii) terminal log for period 4:54 PM - 5:39 PM, 11-13-80, of activity between terminal using Guild ID and Mediametrics computer, and (iii) terminal log for period 5:40 PM (no ending time shown), 11-13-80, for the same activity.

n. Mediametrics system console logs for period 11:58 AM, 11-10-80, to 3:32 PM, 11-19-80.

30. FD-192 dated 1-13-81 on the following two items:

a. Continuous printout from Mediametrics printer of 55 items starting at 17:33:26, 11-15-80, to approximately 18:10:06, 11-15-80.

b. Continuous printout measuring approximately 4½" high from Mediametrics printer of 242 items starting at 18:05:45, 11-15-80, to 18:17:55, 11-15-80.

31. FD-192 dated 1-21-81 on the following three items:

SF 196A-795

a. Memorex brand disk pack, serial #7008291, labeled as "TMSPK1" (sealed and in its own shipping box).

b. BASF brand magnetic tape #Q2 164 0 X304 A3 25, labeled as "DIRECTORY/BACKUP ØØØ 117 ENTIRE PACK" (sealed).

c. BASF brand magnetic tape #12 276 0 A483 A2 07, labeled as "TP DUMP GUILD" and "0918" (sealed).

32. FD-192 dated 5-26-81 on one continuous printout representing Mediametrics system console log for period from 5:28 PM, 9-20-80, to 11:49 AM, 9-27-80.

33. Chronology of Significant Events on 11-14-80 (Orig + 1).

It is noted that the magnetic media listed on the FD-192 dated 1-21-81 (Item #31) have been individually sealed as evidence in such a way that entry into the tapes/disk pack can be detected. These seals should be inspected upon receipt by NH and the FD-192 marked to indicate if they were all intact. Appropriate notations should be made if the seals need to be broken in the future and the items should be re-sealed when access to the contents is no longer needed.

done SEALS INTACT dgl 7/6/81

Even though NH is Office of Origin, SF is retaining the following items as bulky exhibits since they represent magnetic copies of the computerized data being sent herewith to NH:

1. IBM brand magnetic tape labeled "DDR" and "R2189".
2. IBM brand magnetic tape labeled "DDR T1".
3. Memorex brand magnetic tape labeled "TP2".
4. IBM brand magnetic tape labeled "TP3".
5. IBM brand magnetic tape labeled "TP4".
6. Memorex brand magnetic tape labeled as "COPY OF AIMS DUMP FOR [redacted]". b6 b7C
7. Memorex brand magnetic tape labeled as "PACK TMSPK1 DDR DUMP 1 OF 5".
8. Memorex brand magnetic tape labeled as "PACK TMSPK1 DDR DUMP 2 OF 5".
9. Memorex brand magnetic tape labeled as "PACK TMSPK1 DDR DUMP 3 OF 5".
10. Memorex brand magnetic tape labeled as "PACK TMSPK1 DDR DUMP 4 OF 5".
11. Memorex brand magnetic tape labeled as "PACK TMSPK1 DDR DUMP 5 OF 5".
12. IBM brand magnetic tape labeled "DDR 1.1 STAND ALONE 1-21-81".
13. Memorex brand magnetic tape labeled as "COPY OF DIRECTORY BACKUP TAPE ØØØ117".
14. Memorex brand magnetic tape labeled "COPY OF TP DUMP GUILD".

Based on the investigation conducted by SF, the following points are being brought to NH's attention for any action deemed appropriate:

1. A listing of the files under the Guild ID shows that all four CDIR files have a "last Write" date of 8-4-80 prior to their encryption. Three of these were between 6:31 AM - 6:33 AM, while the HSYS file was done at 12:45 PM. Spooling traffic on either HSYS or EAST host computers may show movement of files of these record sizes over the NCSS network to the Mediametric (MM) system. This may be of assistance in determining where the unauthorized CDIR came from and who moved them.

2. Witness [redacted] advised that he inadvertently directed that a printout of the contents of one of the CDIR files (later determined to be named "BIPUSER") be done on a HSYS printer and that he unsuccessfully tried to kill the job. It occurred between 5:00 PM and 7:00 PM, PST, 11-13-80, and was the only spooling traffic from AIMS via the NCSS network to HSYS. The printout would have been 95 pages long with the header page showing the Guild's name and address. It was formatted into five columns named (from left to right) "USERID", "RPW", "VIRTUAL ADDRESS", "VDEV", "ACCOUNT CLASS". It is not known if this printout was picked up by the Guild or forwarded to them, or what happened to it but, since it contains CDIR data, efforts should be made to recover it. b6 b7C

3. Items 30(a) and 30(b) above list the contents of many of the files that were stored under the Guild ID. It is suggested that some technical person at National CSS Headquarters review these printouts to determine if any of the data other than the four CDIR files are proprietary information. Some of the names on the files suggests such a possibility.

4. Witness [redacted] opined that perhaps an edit program was designed and used to take the original CDIR data (which has a record length of about 132 characters long) and abbreviate it to the 30 character version found on the unauthorized CDIR files. It is possible that such an edit program is stored under the Guild ID. b6 b7C

5. Witness [redacted] advised that Marsh-McLennan was not aware that all levels of passwords (including the VPSYSMGR ID) provided on new NCSS 3200 series systems were the same as all other 3200 series systems until after the unauthorized entry into their system had been brought to their attention. National CSS may want to consider specifically notifying other users of the 3200 series systems to insure that these standard passwords have been changed to prevent further unauthorized access, and to attend to this matter during acceptance testing with future customers. b6 b7C

6. Witness [redacted] advised that there were several attempts by the Guild to log onto MM's system between 3:00 AM - 7:00 AM, 11-19-80. This was done after MM had changed all of their passwords and system IDs following the problems that occurred on 11-14-80 and after being assured by the San Francisco Branch of National CSS that such changes would completely lock out the Guild from MM's system. National CSS at San Francisco has not conducted any kind of technical investigation of this 11-19-80 unauthorized access and they do not know what, if anything, National CSS Headquarters has done about the incident. MM's system logs for this period are enclosed as item 29(n) herewith. b6 b7C

7. Attempts to secure the original console log for National CSS San Francisco Branch computer "SFR-1" that contains the attempted unauthorized access in November 1980 have been unproductive as all logs for that period have apparently been destroyed. Witness [redacted] advised that she did not send the original or a copy of it to [redacted] however, it may be wise to double check with [redacted] since [redacted] may be in error. b6 b7C

8. MM, after repeated requests, has been unable to locate a computerized file they created of all available accounting-type data from their system on the Guild IDs, such as date/time of all log-ons and log-offs, ARUs used, I/O devices, CPU connect time, et cetra. MM advised that, if such data is needed for investigative purposes and if National CSS is willing to compile the data, MM would go back and make available appropriate backup tapes so that this information can be reconstructed. Since SF does not know how beneficial this would be to the investigation and if National CSS would do the work, it is being left to the discretion of NH to pursue.

9. As discussed in telephone calls between SF and NH, witness [redacted] has a very poor memory. Further, he has a tendency to make unequivocal statements that are later found to be incorrect. It is strongly suggested that he be given thorough preparation before he testifies, including reviewing his FD-302 and other relevant documents, in order to refresh his memory of the events and to avoid unnecessary confusion to his testimony. b6 b7C

10. Witness [redacted] how lives at [redacted] rather than what is listed in her FD-302. She is still employed as indicated. b6 b7C

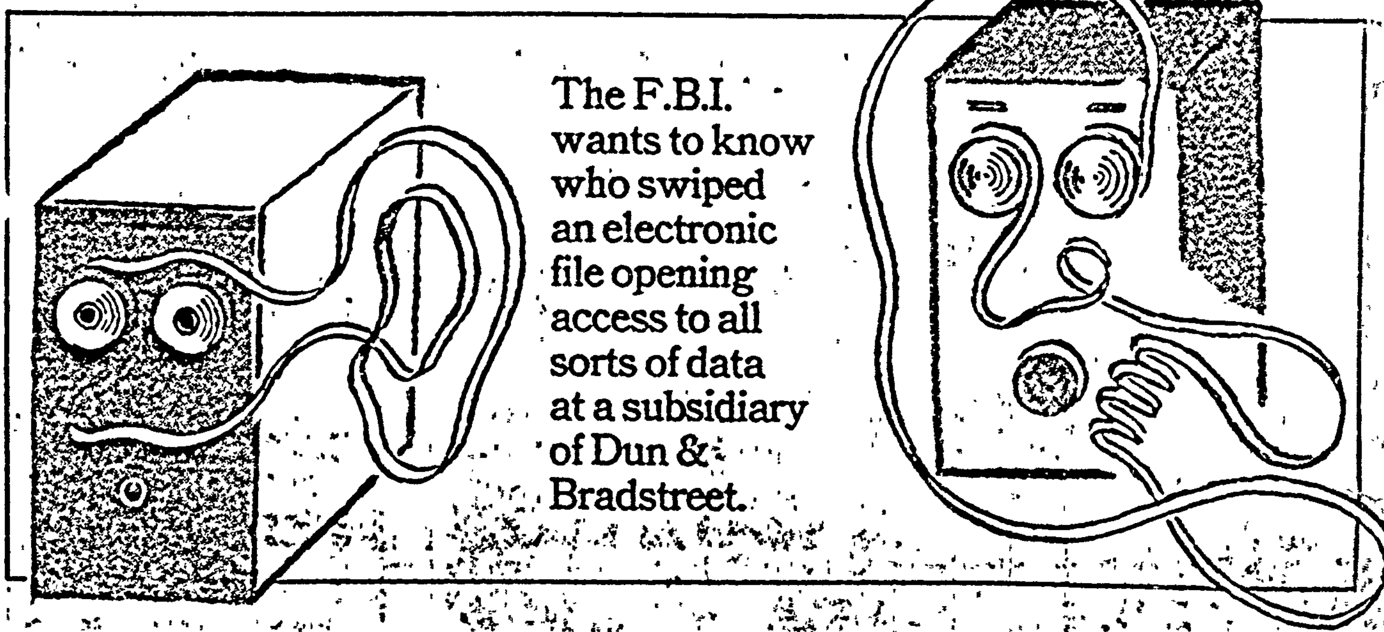
Since all investigation has been completed, SF is considering this matter RUC'd.

196A-397-36

NH 196A-397

THE NEW YORK TIMES, SUNDAY, JULY 26, 1981

Case of the Purloined Password



The F.B.I. wants to know who swiped an electronic file opening access to all sorts of data at a subsidiary of Dun & Bradstreet.

By VIN McLELLAN

BOSTON

SINCE last fall, the Federal Bureau of Investigation has been conducting a criminal investigation into a curious computer-age crime — the theft of an information file called a password directory from the electronic memory of National CSS Inc., one of the nation's largest timesharing companies.

A password directory is essentially a list of the secret words used by customers to identify themselves and signal the timesharing company's computer to unlock and release information they have stored within the system. With the passwords, a thief would have access to the private files of the more than 3,000 companies that are NCSS customers and, in effect, use it as their computer center. So armed, he or she would also be able to manipulate and change that data without leaving any telltale evidence.

While the potential for this kind of crime has worried experts for years, the opportunity to unravel an actual case history is so rare that the cadre of F.B.I. agents trained for computer fraud discuss the NCSS case as a "learning experience."

In the timesharing industry, the issue of system vulnerability has become much more sensitive in recent years. With cheaper electronic storage, remote computing centers are now often used as information vaults. Timesharing clients, which once stored only processing instructions, "programs," within such systems, now often store whole data banks.

No significant cash or data loss has yet been associated with the theft, but with its ominous possibilities, the NCSS security scandal has badly jarred the huge $3 billion-a-year remote processing industry.

The tale has its odd angles. Bemused F.B.I. agents have found themselves confronted with a tradition of almost ritual thievery among computer pro-

NCSS service; perhaps, according to former NCSS officials, its "most vulnerable" client. Since it acquired the timesharing company in 1979, the traditional D.& B. credit services have become increasingly dependent on NCSS technology and the network.

For example, in the large "multi-access" data base used in D.& B.'s new "DunsVue" system, anyone who had obtained the NCSS password directory would have been able to change or erase or create data, according to NCSS technicians familiar with the D.& B. software. In other words, temporarily, at least, a thief could create or diminish credit.

Unfortunately, when you attach communication links to a computer, even with passwords, "you really don't know who is at the other end of the line," said Harold Feinleib, until recently NCSS vice president for advanced systems. "The only secure computer centers are those without telecommunications."

With the password-based security systems used in most timesharing systems, security is a relative thing, measured by the willingness of all participants to accept security discipline. "It's like the seatbelt problem," Mr. Bartholomew said. That is, how does one get people to take precautions?

National CSS, based in Wilton, Conn., with revenues of $100 million last year, is regarded as one of the most technically sophisticated companies in the business. "I don't have a feeling that other systems are any better than NCSS on security," mused Mr. Feinleib. "Most are worse. You wonder. Do these things happen all over?"

The theft, apparently, was an all-electronic one. Someone, somehow, penetrated several levels of the system's internal security and plucked the directories from three NCSS computers in Connecticut and another in California — the four big machines in the network — then ordered the system to shuttle the passwords around the country over telephone circuits.

"uncooperative," hiding behind a phalanx of corporate lawyers.

"Getting information was like pulling teeth," said an official close to the investigation. After the F.B.I. threatened NCSS executives with grand jury subpoenas, cooperation improved, he added, but the inquiry has largely gone around, rather than through, corporate channels.

The theft seemed at first to indicate only that the NCSS system was vulnerable to its 100-odd "system programmers" — the elite technical staff.

"With current procedures, if the system programmer wants to breach security, there is no way to stop him," said Robert Jesserum, former director of development at NCSS, now president of Electronic Information Systems in Stamford. "It's a matter of trusting a lot of people," he said.

But reports soon developed that some sophisticated, lower-level field technicians — even without NCSS system programming experience — had been able to penetrate NCSS security.

According to former NCSS executives, there have also been incidents in which programmers working for NCSS clients have also managed to breach directory security in recent years. Three years ago at the Bank of America in San Francisco, which leases a copy of the NCSS "operating system" to manage its own internal computer network, a six-month security review was initiated after one of its programmers proved he could steal the NCSS directory from the bank's system, according to a bank technician interviewed early this year.

"Every timesharing firm in the world has these skeletons in the closet," laughed Mr. Smith, the former NCSS manager. "Get the heads of technicial development from these companies together," he said, and when they start swapping stories "they'll probably be in hysterics."

Obviously, however, not all raids on the system are criminal in intent.

"Whenever security is breached, there is a threat," said Mr. [illegible] of

curity, noted Mr. Jescerum, evolved as designers patched loopholes discovered by hackers.

But the potential for [illegible] is definitely there. Which may be why D.& B.'s reaction to the discovery of the directory theft was far more forceful than many at NCSS felt necessary.

"I think it was a total over-reaction," said John Pryor, who recently resigned as NCSS vice president for sales, reflecting the general NCSS view that hackers were at work.

Corporate D.& B., however, moved in quickly to directly manage the crisis. Senior NCSS officials claim that even the very guarded NCSS alert, signed by NCSS president David Fehr, was actually written by D.& B. chairman Hamilton Drake. (Again, D.& B. refused comment.)

"It has come to our attention that a former employee may have obtained information which could potentially compromise system access security," read the terse Nov. 20 memo. "Although a breach of any customer's data security is highly unlikely, in line with our total commitment to maintain absolute security, we strongly urge that you immediately change all passwords by which you access the National CSS' systems." The message ended with regrets, but no further details.

For at least one customer, the auditing firm Coopers & Lybrand, an NCSS customer as well as D.& B.'s corporate auditor, it wasn't enough by half.

A week before the alert, Frank Logrippo, Coopers' manager of internal financial reporting, had received a call from Gretchen Mitchell, a senior NCSS customer liaison. She told him that the directories had just been found in California. He immediately began changing the hundreds of passwords his company used on NCSS. When Mr. Fehr's bulletin reached him, he said, he saw NCSS dissembling.

"If the passwords were found at someone else's site," Mr. Lo[illegible]

age, remote computing centers are now often used as information vaults. "Timesharing clients, which once stored only processing instructions, "programs," within such systems, now often store whole data banks.

No significant cash or data loss has yet been associated with the theft, but with its ominous possibilities, the NCSS security scandal has badly jarred the huge $8 billion-a-year remote processing industry.

The tale has its odd angles. Bemused F.B.I. agents have found themselves confronted with a tradition of almost ritual thievery among computer programers. Dun & Bradstreet, the credit rating service that has expanded into a business information conglomerate and is now NCSS's parent, drew the wrath of many industry professionals for not covering up the incident — even as it infuriated some NCSS clients by warning them they had a security problem, but refusing to give them any details of the "problem."

The industry tradition has been to handle security problems quietly and privately. "Everybody in this business has dealt with penetration," said Chester Bartholomew, protection and control director for Boeing Computer Services, a Seattle timesharing concern. "Usually, we have enough information to take a rifle shot at it rather than let loose with a shotgun blast."

But D.& B. required NCSS to notify all its remote processing clients that there was some sort of security problem and that all passwords should be changed, according to NCSS sources. It was the first "broadcast" security alert to the entire customer base of a major timesharing company in the 25-year history of the industry — but it made no mention of stolen passwords.

D.& B. also vetoed a news story on the NCSS incident prepared for Datamation, a major computer industry trade magazine. Datamation staff members said that this was the first incidence of editorial intervention since D.& B. acquired the magazine in 1977. (John L. Kirkley, Datamation's editor, said policy was for D.& B.'s technical publication subsidiary to review any story concerning D.& B. affiliates and that the NCSS instance was Datamation's first such piece. After review, he said, a more general treatment of the security issue was requested, and "that's what we're doing.")

Last week, NCSS spokesman Daniel Bencan said that it was "company policy" not to discuss the case while the F.B.I. inquiry continues. D.& B. officials did not respond to repeated requests for comment.

But extensive interviews with Justice Department officials and present former NCSS people, outline a history of widespread unauthorized access to NCSS directories. An F.B.I. [illegible] use to the United States [illegible] in Connecticut, [illegible]ed, is expected be[illegible]ing to Justice De[illegible]

[illegible]or user of the [illegible]

[illegible]oston-based [illegible]logy and [illegible]ter for [illegible]y.

nies in the business. "I don't have a feeling that other systems are any better than NCSS on security," mused Mr. Feinleib. "Most are worse. You wonder. Do these things happen all over?"

The theft, apparently, was an all-electronic one. Someone, somehow, penetrated several levels of the system's internal security and plucked the directories from three NCSS computers in Connecticut and another in California — the four big machines in the network — then ordered the system to shuttle the passwords around the country over telephone circuits.

Law enforcement officials say it is unclear how many times the system was raided. As is common with computer data-theft, NCSS apparently had no idea the company had been robbed until told of the directories being found in someone else's computer.

NCSS got the first hint of the problem on Oct. 31, 1979, Halloween, when Larry Smith, an independent business consultant and former NCSS manager for advanced product design, placed an angry phone call to the company.

Someone, he charged, had used his NCSS password and I.D. and billed him $30 for the use of a "program product" called RAMIS, a product for which Mr. Smith had developed a successor while at NCSS. Mr. Smith said that where the computer usually recorded RAMIS accounting information, a four-letter obscenity appeared.

"It's like somebody wrote, 'Kilroy was here,'" Mr. Smith said.

Mr. Smith, like many other NCSS executives and senior technicians, had made a tidy profit when D.& B. bought the company. He then teamed up with James Morley, a business consultant, plus several NCSS programmers to form a software consulting firm, called the Guild, in Richfield, Conn.

Within months, the Guild had attracted from NCSS a client called Media Metrics, a small advertising research concern in Moraga, Calif. Soon thereafter, Mr. Smith and an associate resigned from the Guild to start a competing company, Hanson-Smith Ltd., in Shelton, Conn. ("My attorney insists it was a friendly split because nobody sued anybody else," Mr. Smith said. "But that is the extent to which it was friendly.")

A week and a half after Mr. Smith's angry phone call, a technician at Media Metrics went rummaging through the memory of the Media Metrics computer in search of extra storage space. There, according to Mr. Smith and F.B.I. sources, he happened upon the NCSS directory — which, of course, had no business being there. Media Metrics president John Putnam was notified, and he called the Guild and then NCSS, according to NCSS sources. (Mr. Putnam declines to discuss the incident.)

On a Saturday night in November, an NCSS attorney placed a frantic call to the F.B.I., according to Justice Department and NCSS sources.

But when the F.B.I. proved unwilling to guarantee to "handle the situation quietly" and unable to move directly against the suspected thieves to reclaim the password data, said a Justice Department source, NCSS officials suddenly became defensive and its programmers proved he could steal the NCSS directory from the bank's system, according to a bank technician interviewed early this year.

"I very timesharing firm in the world has these skeletons in the closet," laughed Mr. Smith, the former NCSS manager. "Get the heads of technicial development from these companies together," he said, and when they start swapping stories "they'll probably be in hysterics."

Obviously, however, not all raids on the system are criminal in intent.

"Whenever security is breached, there is a threat," said Mr. Morley of the Guild. But, he added, "in this specific case, whoever did it, probably did it as programmers do things, to play — rather than with any serious intentions of offering them for sale or doing anything with them themselves."

Indeed, because of its very importance, the password directory is the traditional target for what the computer industry calls "hackers."

Hackers are technical experts: skilled, often young, computer programmers, who almost whimsically probe the defenses of a computer system, searching out the limits and the possibilities of the machine. Despite their seemingly subversive role, hackers are a recognized asset in the computer industry, often highly prized.

Security was never a "major factor" in the original design of today's timesharing systems, explained Mr. Feinleib — and original design has been constantly extended to cover new applications, carry new responsibilities. So much of what passes for se[illegible] auditor, it wasn't enough by half.

A week before the alert, Frank Logrippo, Coopers' manager of internal financial reporting, had received a call from Gretchen Mitchell, a senior NCSS customer liaison. She told him that the directories had just been found in California. He immediately began changing the hundreds of passwords his company used on NCSS. When Mr. Fehr's bulletin reached him, he said, he saw NCSS dissembling.

"If the passwords were found at someone else's site," Mr. Logrippo said, "it's not 'may be compromised' — it's compromised!"

Whatever the outcome of the NCSS case, the F.B.I. investigation may, in passing, have uncovered a clear case of industrial espionage. Several years ago, according to two former NCSS executives, NCSS was offered the password directory of its largest direct competitor — the Service Bureau Corporation, now a $900 million subsidiary of the Control Data Corporation — by a programmer at a New Jersey pharmaceutical company that was then a client on the S.B.C. network.

The S.B.C. directory, covering some 18,000 clients, was on the block for $5,000 cash, according to Michael Pomerantz, former NCSS district sales manager for New England, who said he received the initial offer. Mr. Pomerantz said NCSS had rejected the offer and notified S.B.C. In the typically murky style of the industry, senior officials at S.B.C. say they can find no record of the incident.

A PROGRAM CALLED PILFER

Three years ago, very much in the industry tradition, a group of National CSS field representatives were found to have developed several elaborate systems to penetrate NCSS security. It was a classic instance of the mischievous but perversely positive "hacker" tradition among computer programmers.

As the handful of those directly involved described it, the group discovered two loopholes. One was a technical weakness in the system. Another simply exploited a high-priority password a Detroit businessman had seen taped to a wall when he was given a tour of the NCSS data center.

For over a year, NCSS's Detroit-based technical "reps" had regularly consulted and used the directory. They were even able to set up an electronic "trap" in the computer to catch new passwords — and changes in key passwords.

Arthur Bolder, a former NCSS account representative who is now a consultant in Ann Arbor, Mich., became something of a folk hero at NCSS when he voluntarily came forward, after another tech rep was caught, to reveal the full scope of the group's capabilities.

Mr. Bolder had written a little program called Pilfer. As he explained it, he simply had to type in the name of an NCSS client or an NCSS executive, and the program would automatically break system security, get the user's password, and deliver to Mr. Bolder an open line to whatever was stored in the computer under that account.

Mr. Bolder said he was threatened with immediate discharge if he ever told anyone how Pilfer worked. Yet even his 1979 letter of reprimand — from Robert Weisman, now NCSS chairman and president of the Association of Data Processing Service Organizations, the industry trade association — acknowledged the hacker tradition.

"The Company realizes the benefit to NCSS and in fact encourages the efforts of employees to identify security weaknesses to the VP, the directory, and other sensitive software in files," Mr. Weisman wrote. Mr. Bolder had erred not in beating the system but in failing to report his success.

196A-397

150 Court Street
Post Office Box 2058
New Haven, Connecticut 06521
August 11, 1981

[redacted] b6 b7C

National CSS, Inc.
187 Danbury Road
Wilton, Connecticut 06897

Dear Sir:

At the request of [redacted] b6 b7C this office began an investigation on November 15, 1980, involving possible criminal violations of several sections of the United States Federal Criminal Code.

During the course of our investigation it became necessary to rely upon certain members of your staff located in both Wilton, Connecticut and San Francisco, California to provide us with varying degrees of technical assistance. The cooperation of [redacted] b6 b7C was very much appreciated.

The continuing cooperation of your staff has made it unnecessary to resort to the time consuming and costly process of utilizing Federal Grand Jury subpoenas to obtain requested information.

Once again, I wish to thank you for the cooperation extended to Special Agents [redacted] b6 b7C during the course of the investigation.

Very truly yours,

LGB/wrd

L. Grey Brockman
Special Agent in Charge

1 - Addressee
1 - 196A-397
DEF/sab
(2)

sab

[redacted] b6 b7C

196-397-37