IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF ARKANSAS

UNITED STATES OF AMERICA	)	CASE NO. 4:04CR00175 WRW
	)	
	)	18 U.S.C., § 371
	)	18 U.S.C., § 1030
	)	18 U.S.C., § 1029
V.	)	18 U.S.C., § 1957
	)	18 U.S.C., § 1512
	)	18 U.S.C., § 3013
	)	18 U.S.C., § 3571
	)	18 U.S.C., § 982(a)(1)
SCOTT LEVINE	)	18 U.S.C., § 982(a)(2)(B)

INDICTMENT

THE GRAND JURY CHARGES THAT:

COUNT 1

(Conspiracy)

A. INTRODUCTION

At various times relevant to this Indictment:

1. Snipermail.com, Inc., (hereinafter "Snipermail") was a Florida corporation, located in the Boca Raton, Florida area, engaged in the business of distributing advertisements via the Internet to email addresses on behalf of advertisers or their brokers. Snipermail purported to maintain a database containing several million e-mail addresses which it claimed were obtained via a "double verified opt-in process." That is, the e-mail users chose to receive material pertaining to their interests after which they received an e-mail verifying that they were, indeed, interested in receiving promotions via e-mail. Once the customer confirmed an interest in receiving such promotions, Snipermail

required them to complete an online form providing various demographic and geographic information about themselves. Snipermail then rented the e-mail addresses and other relevant information to other businesses for use in their advertising campaigns after purportedly determining which subscribers matched the target group for the advertiser. In many instances, however, ad campaigns were sent to a general population of e-mail addresses without regard to the targeted requirements of an agreement with the broker. Snipermail charged according to the number of e-mails distributed, generally on a cost per-thousand basis. Snipermail also generated income by selling the names and addresses of consumers to other businesses for use in traditional mail campaigns.

2. The defendant SCOTT LEVINE, was the controlling force behind Snipermail, managing employees, dictating the mode of operations, and reserving for himself and his family the overwhelming majority of the financial benefits derived from the operation of the company. At least since 2002, LEVINE has had an ownership interest in Snipermail.

3. Magdiel Castro, a/k/a Mike Castro, was the registered agent and president of Snipermail. He is the brother-in-law of SCOTT LEVINE. Castro was purported to have an ownership interest in Snipermail.

4. Jeffrey Richman was the sales manager of Snipermail and a long term business associate of SCOTT LEVINE.

5. RichMedia, Inc. was a Florida corporation operated by Jeffrey Richman.

6. Jeffrey Burstein was employed by Snipermail from March 2000 through March 2003 as the computer systems administrator of Snipermail.

7. William F. Clinton was employed by Snipermail from the Spring of 2001 through May 28, 2003 as a computer specialist.

8. Melvin Donald Atkinson was a computer analyst at Snipermail.

9. Marcos Cavalcante was a graphic designer and computer specialist at Snipermail.

10. Acxiom Corporation ("Acxiom")is a corporation with offices in Little Rock and Conway, Arkansas. Acxiom is one of the world's largest repositories for personal, financial, and company data. It provides the service of storing huge amounts of customer provided data as well as enhancing the quality and utility of that data through various proprietary computer processes.

11. Acxiom uses its File Transfer Protocol (FTP) server, ("ftp.acxiom.com"), located in Conway, Arkansas, to store data being transferred. FTP is a method of communication used to send and receive files such as spreadsheets, word-processing documents or databases via the Internet. Acxiom customers may place data on

the FTP server for Acxiom to retrieve and process. Acxiom may also place information on the FTP server that it has analyzed and processed for the customer to retrieve. Each Acxiom customer has a username and password for accessing "ftp.acxiom.com" which is shared by Acxiom and the customer. In the normal course of business, both Acxiom and its customers may distribute the username and password to suppliers and partners. However, each supplier or partner is only authorized to utilize the username and password of his or her respective client.

12. At all material times herein:

a. A computer network is two or more computer systems and/or devices which are interconnected in such a way that they may communicate with each other. The most prevalent example of a large computer network is the internet or world wide web (WWW).

b. Each computer or device on the internet or any network must be uniquely identifiable. Much like the postal system, each address must be unique so that mail delivery will be effective and efficient. Networks and computers on the internet are generally identifiable by their Internet Protocol ("IP") address. This address must be unique in order for effective and efficient communications between computers and networks. For example, the Acxiom server in question is identifiable by its IP address of 65.64.17.91. Another way to identify that computer system is by its Uniform Resource Locator (URL) that is

http://ftp.acxiom.com. A special computer system called a Domain Name Server (DNS) maintains a large database of IP addresses and URLs so that someone could communicate with the Acxiom system from the internet using either the IP address or the URL. URLs are popular because they are much more "user friendly" than a collection of numbers.

c. Some IP addresses are permanently assigned to computer systems and networks and are called "static" IP addresses. Some, however, are assigned open or available IP addresses each time the user logs onto the internet. These are called "dynamic" IP addresses.

d. At any given moment in time, only one computer can have a given IP address. Blocks of IP addresses are assigned to various entities, organizations, and governments. They may only use IP addresses assigned to their group. They must decide how they will most effectively utilize their block of IP addresses. Internet Service Providers (ISPs) sell access to the internet by allowing users and entities to use their IP addresses to access the internet.

e. Given a specific IP address, date, and time, one can track the IP address back to an entity that manages or controls that IP address. Also, if that entity maintains logs of IP activity, one may be able to track the IP address back to an

individual computer using that particular IP address at a given date and time, through the logs.

f. A protected computer is a computer which is used in interstate or foreign commerce or communication. The access in question was initiated by a computer or computers at Snipermail, Boca Raton, Florida via the Internet and connected to an Acxiom computer, "ftp.acxiom.com", in Conway, Arkansas.

13. Company No. 1 was a customer of Acxiom. Company No. 1 contracted with other entities for services, and in turn these entities entered into sub-contracts with Snipermail. These agreements permitted Snipermail to place certain files on the "ftp.acxiom.com" server, using Company No.1's username and password.

14. Company No. 2 is a customer of Acxiom.

B. THE CONSPIRACY

Beginning at a time unknown to the grand jury, but no later than November 2001, and continuing thereafter up to and through the date of this Indictment, in the Eastern District of Arkansas and elsewhere, defendant SCOTT LEVINE, conspired with persons known and unknown to the Grand Jury, to violate the laws of the United States by committing certain offenses, that is:

(1) to intentionally access a protected computer without authority or in excess of authority and thereby obtain information in violation of Title 18, United States Code, Section 1030(a)(2)(C);

(2) to knowingly and with intent to defraud possess fifteen or more devices which are unauthorized access devices, such offense affecting interstate commerce, in violation of Title 18, United States Code, Section 1029(a)(3);

(3) to conduct a monetary transaction in criminally derived property of a value greater than $10,000 which was derived from specified unlawful activity, which in any way or degree affected interstate and foreign commerce, that involved the proceeds of unlawful activity, in violation of Title 18, United States Code, Section 1957; and

(4) to corruptly alter, destroy, mutilate, and conceal a record, document, or other object, and attempt to do so, with the intent to impair the object's integrity or availability for use in an official proceeding, in violation of Title 18, United States Code, Section 1512(c)(1).

C. MANNER AND MEANS OF THE CONSPIRACY

It was part of the conspiracy that one or more conspirators would access Acxiom's "ftp.acxiom.com" server from Snipermail, as a supplier of services to one or more of Acxiom's customers, exceed the authorization extended to such suppliers by entering areas which they had no authority to enter, and download files which they had no authority to download.

It was further part of the conspiracy that the conspirators would decrypt Acxiom encrypted password files in order to have access to greater amounts of Acxiom data, incorporate the stolen data into the Snipermail system, and sell the newly acquired information together with their existing data to Snipermail clients.

It was further part of the conspiracy that LEVINE and others would recruit new participants in the illicit activity and persuade existing participants to continue their illicit behavior by promising some a share in the business, higher wages, continued employment, and others assistance with visa and immigration matters.

It was further part of the conspiracy that, after commencement of an investigation by law enforcement, the conspirators would remove computers; remove hard drives from computers containing the stolen data; and would hide or destroy the computers and/or hard drives containing the stolen data in order to delay detection.

D. OVERT ACTS

In furtherance of this conspiracy, and to effect the objects thereof, at least one of the co-conspirators herein committed and caused to be committed, at least one of the following overt acts, among others, in the Eastern District of Arkansas and elsewhere:

1) Those acts set forth in paragraph 2 of Counts 2 through 10 of the Indictment.

2) Those acts set forth in paragraph 2 of Counts 11 through 39 of the Indictment, more specifically including the following acts:

a) On or about March 31, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 downloaded 13 files from the "ftp.acxiom.com" server in Conway, Arkansas.

b) On or about May 22, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 downloaded a file from the "/hosting/pw/" folder called "ftpsam.txt" containing usernames and encrypted passwords for many of the accounts on the "ftp.acxiom.com" server in Conway, Arkansas.

c) On or about May 23, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 began downloading files from the "ftp.acxiom.com" server in Conway, Arkansas, using 23 separate account names to download 302 different files.

3) Those acts set forth in paragraph 2 of Counts 40 through 140 of the Indictment.

4) Those acts set forth in paragraphs 3 through 8 of Count 141 of the Indictment.

5) Those acts set forth in paragraph 3 of Count 142 of the Indictment.

6) Those acts set forth in paragraph 2 of Count 143 of the Indictment.

7) Those acts set forth in paragraphs 2 through 5 of Count 144 of the Indictment.

8) In or about January 2003, upon being informed by Burstein of his ability to access certain files in the "ftp.acxiom.com" system that Snipermail was not authorized to access, defendant LEVINE encouraged Burstein to download numerous files from the Acxiom system containing names, addresses, e-mail addresses, and other data, as set forth in Counts 2 through 10.

9) In approximately April of 2003, at LEVINE and Castro's direction, Clinton began incorporating files that LEVINE had downloaded from the "ftp.acxiom.com" server into a server at Snipermail. (See Counts 11-39).

10) On or about May 22, 2003, LEVINE downloaded a file entitled "ftpsam.txt" which contained Acxiom usernames and encrypted passwords. At LEVINE's request and with his encouragement, Clinton ran a decryption program against the file and was able to decrypt approximately 40% of the usernames and passwords.

11) On or after June 1, 2003 Atkinson was directed by LEVINE to incorporate data that LEVINE had downloaded from Acxiom into the Snipermail system.

12) From on or about June 2, 2003 through on or about August 1, 2003, Cavalcante continued to incorporate the stolen data into the Snipermail system. (See Counts 40 through 140).

13) In or after July 2003, at LEVINE's request and with his encouragement, Cavalcante ran a decryption program against the July 24, 2003, "ftpsam.txt" file containing usernames and encrypted passwords and was able to decrypt a further substantial number of the passwords.

14) On or about May 22, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 began downloading files from directories other than those associated with the user identification of Company No. 1 from the "ftp.acxiom.com" server in Conway, Arkansas.

15) On or about May 23, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 downloaded files from the "ftp.acxiom.com" server in Conway, Arkansas, containing usable names and addresses as well as "seed data" owned by Company No. 2 (See Count 141).

16) On or about June 11, 2003, one or more co-conspirators caused to be e-mailed from Snipermail to Direct Partner Solutions, in Alpharetta, Georgia, an invoice in the amount of $19,479.44 for an advertising campaign.

17) On or about July 12, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 downloaded a file called "ftpsam.txt" containing usernames and encrypted passwords for many of the accounts on the "ftp.acxiom.com" server in Conway, Arkansas.

18) On or about July 24, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 downloaded a file called "ftpsam.txt" containing usernames and encrypted passwords for many of the accounts on the "ftp.acxiom.com" server in Conway, Arkansas.

19) On or about July 31, 2003, one or more co-conspirators using Snipermail IP address 67.97.126.58 downloaded a file called "ftpsam.txt" containing usernames and encrypted passwords for many of the accounts on the "ftp.acxiom.com" server in Conway, Arkansas.

20) On or about August 7, 2003, one or more co-conspirators using Snipermail IP addresses 67.97.126.58 and 63.148.233.7 attempted to access the "ftp.acxiom.com" server in Conway, Arkansas.

All in violation of Title 18, United States Code, Section 371.

COUNTS 2- 10

(Unauthorized Access of a Protected Computer)

1. The Grand Jury realleges each allegation contained in paragraphs A 1 through 13 of Count 1 and incorporates them as if fully set forth herein.

2. On or about the following dates and times in the Eastern District of Arkansas, and elsewhere, the defendant

SCOTT LEVINE,

together with other persons known and unknown to the Grand Jury, aiding and abetting one another, intentionally accessed a computer

without authorization and in a manner that exceeded authorized access, which conduct involved interstate and foreign communication, and thereby obtained information from a protected computer, for purposes of commercial advantage and private financial gain, and additionally, obtained information valued in excess of $5,000, each access constituting a separate charge:

COUNT	DATE	TIME	BYTES
2	04/18/02	16:26:11	28160
3	04/18/02	16:30:26	17404928
4	04/18/02	16:30:27	28160
5	04/18/02	16:44:10	133321595
6	01/07/03	14:31:42	0
7	01/07/03	14:31:46	0
8	02/04/03	15:45:03	0
9	02/06/03	9:35:22	0
10	02/06/03	9:41:20	0

All in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i) and (iii), and 2.

COUNTS 11 - 39

(Unauthorized Access of a Protected Computer)

1. The Grand Jury realleges each allegation contained in paragraphs A 1 through 13 of Count 1, and incorporates them as if fully set forth herein.

2. On or about the following dates and times in the Eastern District of Arkansas, and elsewhere, the defendant

SCOTT LEVINE

together with other persons known and unknown to the Grand Jury, aiding and abetting one another, intentionally accessed a computer without authorization and in a manner that exceeded authorized access, which conduct involved interstate and foreign communication, and thereby obtained information from a protected computer, for purposes of commercial advantage and private financial gain, and additionally, obtained information valued in excess of $5,000, each access constituting a separate charge:

COUNT	DATE	TIME	BYTES
11	03/31/03	14:08:31	324618600
12	03/31/03	15:47:38	51411
13	03/31/03	16:42:03	15190036
14	03/31/03	16:55:50	103313168
15	03/31/03	17:56:25	61277881
16	04/11/03	11:46:11	27570595
17	04/14/03	7:53:06	622594
18	04/15/03	11:57:03	18383281
19	05/14/03	16:31:58	20887636
20	05/20/03	14:35:12	90587136
21	05/20/03	14:25:30	242746048
22	05/22/03	10:41:22	89960
23	05/22/03	12:18:09	1277
24	05/22/03	13:11:08	443154

COUNT	DATE	TIME	BYTES
25	05/22/03	15:27:24	443154
26	05/23/03	9:17:10	90728175
27	05/23/03	9:32:25	90716832
28	05/23/03	9:42:32	90706585
29	05/23/03	9:51:37	90719485
30	05/23/03	10:02:55	90728474
31	05/23/03	10:13:41	90698499
32	05/23/03	10:26:32	90719703
33	05/23/03	10:34:53	90727302
34	05/23/03	10:45:59	90713389
35	05/23/03	10:53:42	90708335
36	05/23/03	14:55:09	36323328
37	05/27/03	8:48:58	100496796
38	05/27/03	9:28:23	11408340
39	05/27/03	13:59:54	86919095

All in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i) and (iii), and 2.

COUNTS 40 - 140

(Unauthorized Access of a Protected Computer)

1. The Grand Jury realleges each allegation contained in paragraphs A 1 through 13 of Count 1, and incorporates them as if fully set forth herein.

2. On or about the following dates and times in the Eastern District of Arkansas, and elsewhere, the defendant

SCOTT LEVINE,

together with other persons known and unknown to the Grand Jury, aiding and abetting one another, intentionally accessed a computer without authorization and in a manner that exceeded authorized access, which conduct involved interstate and foreign communication, and thereby obtained information from a protected computer, for purposes of commercial advantage and private financial gain, and additionally, obtained information valued in excess of $5,000, each access constituting a separate charge:

COUNT	DATE	TIME	BYTES
40	06/02/03	7:50:56	2464532
41	06/02/03	7:51:22	145633
42	06/02/03	7:51:33	127265
43	06/02/03	7:51:41	126136
44	06/02/03	7:51:51	117496
45	06/02/03	18:01:40	4839227
46	06/02/03	18:01:43	489075
47	06/04/03	8:12:27	6330744
48	06/04/03	8:28:22	249127162
49	06/06/03	15:21:27	372736
50	06/12/03	14:32:31	437830
51	06/19/03	11:00:28	440500
52	06/19/03	11:00:37	440500
53	06/20/03	8:04:48	440502

COUNT	DATE	TIME	BYTES
54	06/24/03	16:51:04	245582912
55	06/25/03	12:03:37	0
56	06/25/03	15:11:26	442905
57	06/28/03	10:37:26	96
58	06/28/03	11:47:39	151587761
59	06/30/03	11:48:59	128049834
60	07/12/03	13:21:33	448096
61	07/14/03	7:41:34	118310
62	07/14/03	11:06:12	29349742
63	07/14/03	11:32:06	665122
64	07/14/03	11:32:06	296696
65	07/14/03	11:32:49	4065716
66	07/14/03	16:31:10	9888583
67	07/14/03	16:31:21	165878
68	07/14/03	17:09:47	114794268
69	07/14/03	18:03:14	22745838
70	07/14/03	18:09:33	3420425
71	07/14/03	19:08:47	296425584
72	07/15/03	8:09:01	1241191
73	07/15/03	10:38:34	5789
74	07/15/03	10:38:36	20585
75	07/15/03	10:41:59	3821087
76	07/15/03	10:45:32	16573326
77	07/15/03	11:00:44	29039072
78	07/15/03	16:53:11	156947
79	07/15/03	17:04:51	1999576
80	07/15/03	17:09:25	28385729

COUNT	DATE	TIME	BYTES
81	07/15/03	17:25:08	5900238
82	07/15/03	17:28:30	60688442
83	07/15/03	17:44:22	42706122
84	07/15/03	17:53:28	2274140
85	07/15/03	18:33:24	86470164
86	07/16/03	10:15:07	10062834
87	07/16/03	11:39:22	697699
88	07/16/03	11:49:24	163125
89	07/16/03	11:49:51	489375
90	07/16/03	16:29:43	7082064
91	07/16/03	17:30:57	123592176
92	07/16/03	18:03:04	20325817
93	07/16/03	18:11:09	7067249
94	07/16/03	18:13:25	2355306
95	07/16/03	18:19:03	14227442
96	07/17/03	13:52:45	3483254
97	07/17/03	15:13:03	3611887
98	07/17/03	15:16:11	20763606
99	07/17/03	15:16:40	7624344
100	07/18/03	15:31:15	9259650
101	07/23/03	11:35:18	44043
102	07/23/03	11:36:22	3796713
103	07/23/03	11:37:26	1277717
104	07/23/03	12:57:39	136230857
105	07/23/03	13:07:36	246393380
106	07/23/03	14:08:09	2707396
107	07/23/03	14:45:20	10535

COUNT	DATE	TIME	BYTES
108	07/23/03	18:35:11	662200000
109	07/24/03	14:22:27	451513
110	07/24/03	15:21:07	26286321
111	07/29/03	18:06:26	9200430
112	07/30/03	16:19:32	9950033
113	07/31/03	15:06:01	11427894
114	07/31/03	17:38:47	455112
115	08/01/03	9:47:22	328983694
116	08/01/03	10:30:22	68304896
117	08/01/03	10:39:48	30804731
118	08/01/03	10:40:51	34466327
119	08/01/03	10:49:15	79613890
120	08/01/03	10:52:13	98501043
121	08/01/03	13:02:09	641135
122	08/01/03	13:27:46	36118096
123	08/01/03	14:48:09	72758628
124	08/01/03	14:59:47	82634793
125	08/01/03	15:28:19	152043589
126	08/01/03	16:42:44	1605459
127	08/01/03	16:45:40	13130
128	08/01/03	16:52:57	17668082
129	08/01/03	17:08:27	27005161
130	08/01/03	17:05:42	32189255
131	08/01/03	17:50:34	92450801
132	08/01/03	18:01:09	89317174
133	08/01/03	18:16:24	91559626
134	08/01/03	18:35:04	92650015

COUNT	DATE	TIME	BYTES
135	08/01/03	20:08:13	482445643
136	08/01/03	20:12:48	320433516
137	08/01/03	20:12:55	8990421
138	08/01/03	20:13:53	2901840
139	08/01/03	20:14:05	349296
140	08/01/03	21:04:26	902476458

All in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i) and (iii), and 2.

COUNT 141

(Company No. 2 Money Laundering)

1. The Grand Jury realleges each allegation contained in paragraphs A 1 through 14 of Count 1, and incorporates them as if fully set forth herein.

2. Company No. 3 is an entity that is engaged in the manufacture, sale and promotion of a brand-name pharmaceutical. Company No. 3 contracted with a business called ID Media to provide a postal advertising campaign targeted at users of a competing product. ID Media contracted with a list broker named Direct Partner Solutions to obtain the target names and addresses. Direct Partner Solutions in turn contracted with Snipermail for the list. The Snipermail representative who sold the data to Direct Partner Solutions was SCOTT LEVINE.

3. "Seeds and decoys" refers to name and address listings inserted by a list owner into a mailing list in order to become aware of unauthorized use of the list. The owner may use fictitious names with addresses that correspond to an address controlled by the list owner. Company No. 2 had inserted "seeds and decoys" in its customer list provided to Acxiom.

4. On or about May 23, 2003, one day after downloading and decrypting the "ftpsam.txt" passwords file, an individual or individuals at Snipermail, using IP address 67.97.126.58, accessed "ftp.acxiom.com" using Company No. 2's user ID and password and downloaded 10 files. The accessing of the 10 files are charged in Counts 26 through 35 as computer intrusions in violation of Title 18, United States Code Section 1030(a)(2)(C). As a result of that access, an individual or individuals at Snipermail obtained Company No. 2's names and addresses, which were downloaded and incorporated into Snipermail's system.

5. In or about August 2003, Company No. 2 received numerous advertisements for Company No. 3's product addressed to its "seeds and decoys" addresses.

6. At all times pertinent, Snipermail maintained a bank account at Washington Mutual Bank, Boca Raton, Florida, a financial institution within the meaning of Title 18, United States Code, Sections 1957(f)(1) and 1956(c)(6).

7. Payment for the addresses supplied by Snipermail to Direct Partner Solutions was by check. The check was deposited, in the ordinary course of business, into the Snipermail account at Washington Mutual Bank. The deposit constituted a "monetary transaction" as defined in Title 18, United States Code, Section 1957(f)(1).

8. On or about July 3, 2003, in the Eastern District of Arkansas and elsewhere, defendant

SCOTT LEVINE,

together with other individuals known and unknown to the Grand Jury, aiding and abetting one another, knowingly engaged in and caused a monetary transaction of a value greater that $10,000 with criminally derived property, that is, SCOTT LEVINE caused to be deposited into the Snipermail account at Washington Mutual Bank a check in the amount of $19,479.44 which Snipermail derived from the sale of data obtained from the unlawful intrusion of a protected computer as set forth in Counts 26 through 35 of this Indictment.

All in violation of Title 18, United States Code, Section 1957 and 2.

COUNT 142

(Access Device Fraud)

1. The Grand Jury realleges each allegation contained in paragraphs A 1 through 12 of Count 1, and incorporates them as if fully set forth herein.

2. An "access device" means any code, account number, electronic serial number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.

3. On or about May 22, 2003, in the Eastern District of Arkansas and elsewhere, defendant

SCOTT LEVINE,

together with other individuals known and unknown to the Grand Jury, aiding and abetting one another, knowingly and with intent to defraud possessed fifteen or more user identifications and passwords, which are unauthorized access devices, said activity affecting interstate and foreign commerce, in that the user identifications and passwords were obtained via the Internet.

All in violation of Title 18, United States Code, Section 1029(a)(3) and 2.

COUNT 143

(Access Device Fraud)

1. The Grand Jury realleges each allegation contained in paragraphs A 1 through 12 of Count 1, and paragraph 2 of Count 142 and incorporates them as if fully set forth herein.

2. On or about July 24, 2003, in the Eastern District of Arkansas and elsewhere, the defendant

SCOTT LEVINE,

together with other individuals known and unknown to the Grand Jury, aiding and abetting one another, knowingly and with intent to defraud possessed fifteen or more user identifications and passwords, which are unauthorized access devices, said activity affecting interstate and foreign commerce, in that the user identifications and passwords were obtained via the Internet.

All in violation of Title 18, United States Code, Section 1029(a)(3) and 2.

COUNT 144

(Obstruction of Justice)

1. The Grand Jury realleges each allegation contained in paragraphs A 1 through 14 of Count 1, and incorporates them as if fully set forth herein.

2. On or after August 7, 2003 in the Eastern District of Arkansas and elsewhere,

SCOTT LEVINE

together with other individuals known and unknown to the Grand Jury, aiding and abetting one another, attempted to corruptly alter, destroy, mutilate and conceal an object, that is computers and computer hard drives, with intent to impair their integrity and availability for use in an official proceeding.

3. It was part of LEVINE's attempt to obstruct justice that, upon inquiry by law enforcement and the victim of specific downloads of Acxiom data onto the Snipermail system, SCOTT LEVINE and others, removed and caused to be removed certain computers and hard drives containing the Acxiom data from their regular space in the office and placed them in a stairwell where boxes and other objects were stored.

4. It was further part of LEVINE'S attempt to obstruct justice that LEVINE solicited Castro and Richman to assist him in carrying out the conduct described in Paragraph 3, above.

5. It was further part of LEVINE's attempt to obstruct justice that upon inquiry by law enforcement and the victim of specific downloads of Acxiom data onto the Snipermail system that SCOTT LEVINE gave cash to Cavalcante and instructed him to purchase computer hard drives to replace ones that had been removed.

All in violation of Title 18, United States Code, Section 1512(c)(1) and 2.

SENTENCING ALLEGATIONS

1. With respect to each count of this Indictment, except Count 144, with which he is charged:

(a) SCOTT LEVINE was an organizer and leader of a criminal activity that involved five or more participants and was otherwise extensive; and

(b) SCOTT LEVINE willfully obstructed and impeded, and attempted to obstruct and impede, the administration of justice during the course of the investigation and prosecution of the charged offense, and this obstructive conduct related to the charged offense and its relevant conduct, as well as other closely-related offenses.

2. With respect to each count of this indictment, except Count 141, with which he is charged:

(a) the loss exceeded $7,000,000.

3. With respect to count 144 of the Indictment, with which he is charged:

(a) SCOTT LEVINE was an organizer, leader, manager, and supervisor in the charged criminal activity.

FORFEITURE ALLEGATION 1

(Conspiracy to Commit Computer Intrusion)

1. Upon being convicted of one or more of the offenses in Counts 1 - 140 of this Indictment, defendant SCOTT LEVINE shall forfeit to the United States of America pursuant to Title 18, United States Code, Section 982(a)(2)(B), all property, real or personal, constituting, or derived from proceeds obtained, directly or indirectly, as the result of such violations.

2. If any of the above-described forfeitable property, as a result of any act or omission of the defendant

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States to seek forfeiture of properties of said defendant up to the amount set forth above, including, but not limited to, the following:

All that lot or parcel of land, together with its buildings, appurtenances, improvements, fixtures, attachments and easements, located at 18619 Long Lake Dr., Boca Raton, FL 33496-1938, more particularly described as:

Long Lake Estates Plat 1 Lot 30, Palm Beach County, Florida

All pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b).

FORFEITURE ALLEGATION 2

(Money Laundering)

1. Pursuant to Title 18, United States Code, Section 982(a)(1), upon being convicted of the offense set forth in Count 141 of this Indictment, defendant SCOTT LEVINE shall forfeit to the United States the following property:

a. All right, title, and interest in any and all property involved in each offense in violation of Title 18, United States Code, Section 1957, and all property traceable to such property, including, but not limited to, the following: 1) all money or other property that was the subject of each transaction, transportation, transmission or transfer in violation of Section 1957; 2) all commissions, fees and other property constituting proceeds obtained as a result of those violations; and 3) all property used in any manner or part to commit or to facilitate the commission of those violations.

b. A sum of money equal to the total amount of money involved in the offense.

2. If any of the above-described forfeitable property, as a result of any act or omission of the defendant - -

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States to seek forfeiture of properties of said defendant up to the amount set forth above, including, but not limited to, the following:

All that lot or parcel of land, together with its buildings, appurtenances, improvements, fixtures, attachments and easements, located at 18619 Long Lake Dr., Boca Raton, FL 33496-1938, more particularly described as:

Long Lake Estates Plat 1 Lot 30, Palm Beach County, Florida

All pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b).

FORFEITURE ALLEGATION 3

(Access Device Fraud)

1. Upon being convicted of one or more of the offenses in Counts 142 - 143 of this Indictment, defendant SCOTT LEVINE shall forfeit to the United States of America pursuant to Title 18, United States Code, Section 982(a)(2)(B), all property, real or personal, constituting, or derived from proceeds obtained, directly or indirectly, as the result of such violations.

2. If any of the above-described forfeitable property, as a result of any act or omission of the defendant

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States to seek forfeiture of properties of said defendant up to the amount set forth above, including, but not limited to, the following:

All that lot or parcel of land, together with its buildings, appurtenances, improvements, fixtures, attachments and easements, located at 18619 Long Lake Dr., Boca Raton, FL 33496-1938, more particularly described as:

Long Lake Estates Plat 1 Lot 30, Palm Beach County, Florida

All pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b).

A TRUE BILL

FOREPERSON

H. E. (BUD) CUMMINS
UNITED STATES ATTORNEY

UNITED STATES ATTORNEY/ASSISTANT
GEORGE C. VENA
TODD L. NEWTON
Assistant United States Attorneys
P.O. BOX 1229
LITTLE ROCK, AR 72203
(501) 340-2600

MARTHA STANSELL-GAMM
CHIEF, COMPUTER CRIME AND
INTELLECTUAL PROPERTY SECTION

AMANDA M. HUBBARD
Trial Attorney
John C. Keeney Building,
Suite 600
10th St. & Constitution Ave, NW
Washington, DC 20530
(202) 514-1026