

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

05-80167 CR-RYSKAMP

Case No:

HOPKINS

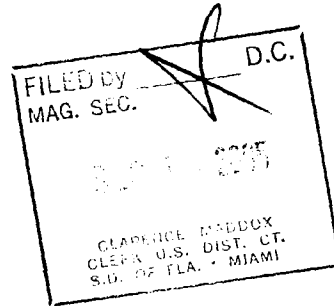
18 U.S.C. § 371
18 U.S.C. § 1030(a)(4)
18 U.S.C. § 1028A
18 U.S.C. § 2

UNITED STATES OF AMERICA

vs.

TIMOTHY C. McKEAGE,
JUSTIN A. PERRAS,
JASON DANIEL HAWKS,
ZACHARY WILEY MANN, and
JEFFREY ROBERT WEINBERG,

Defendants.



INDICTMENT

The Grand Jury charges that:

GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. The company LexisNexis provided authoritative legal, news, public records and business information in online, print or CD-ROM formats. The Lexis service, the first commercial, full-text legal information service, was begun in 1973 to help legal practitioners research the law more efficiently. The companion Nexis news and business information service was launched in 1979 to provide researchers with recent and archival news and financial information. LexisNexis

3
w/c

has since grown to become the largest news and business online information service, providing comprehensive company, country, financial, demographic, market research, and industry reports.

2. Seisint, Inc. was a Florida corporation in Boca Raton, Florida that was purchased in or around September 2004 by LexisNexis. Seisint, Inc. was the original owner of the Accurint database. The Accurint database allows organizations to quickly and easily extract information from tens of billions of data records on individuals and businesses, using proprietary data-linking methods. Customers who have an Accurint account may access the database by visiting a web site and entering a username and password. Once they have obtained access, Accurint customers can run computerized searches of the database for specific terms (including the names of debtors or criminal defendants). The Accurint database was located on servers at a facility in Boca Raton in the Southern District of Florida.

3. Access to the Accurint database was given to legitimate customers after an initial vetting process. This process was used to determine the legitimacy of the business itself and the customers' legal right to access the database. Once a business entity obtained an account, the entity would procure access to the Accurint database by contacting representatives from Seisint, Inc. who would supply the contact listed on the business' application with a username name and password. This username was considered the master account name for that particular customer. Once a business received this master account information, it was the master account holder's responsibility to maintain and change passwords, as well as to create and modify additional usernames. Only master account holders had the ability to create additional usernames for their respective accounts. It was also the master account holder's responsibility to determine which of their respective

employees should be allowed to access the Accurint database. Seisint, Inc. and LexisNexis did not maintain any passwords for their customers.

4. The Port Orange Police Department, in Port Orange, Florida was a legitimate Accurint account holder. The Port Orange Police Department would access the Accurint database using a protected computer, that was used in interstate commerce and communication, which was used in furtherance of the administration of justice.

5. Denton County, in the State of Texas, was a legitimate Accurint account holder. Denton County would access the Accurint database using a protected computer that was used in interstate commerce and communication.

6. Computers and other devices connected to the Internet are identified by an address known as the Internet Protocol Address (“IP address”). An IP address is a unique numeric address that looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer or other device (or group of computers or other devices using the same account to access the Internet) connected to the Internet must be assigned an IP address which acts much like a home or business street address, enabling Internet sites to properly route traffic sent to and from that computer. There are two types of IP addresses: dynamic and static. A static IP address is one that is permanently assigned to a given computer on a network. With dynamic addressing, however, each time a computer establishes an Internet connection, that computer is assigned a different IP address from a pool of available addresses.

7. One way a computer user can hide the user’s true IP address is to use a “proxy server,” a computer system that the user passes through before reaching the computer system or server ultimately accessed by the user. This makes it appear to the computer system/server that the

user's IP address is located within the proxy server and not from the user's own computer and true IP address.

8. As the term is used relating to computer programs, a "Trojan Horse" is a destructive computer program that masquerades as a benign computer application. A Trojan Horse is often used to introduce viruses and other malicious software to victim computers to allow the remote use of the infected computer, without the legitimate user's knowledge or authorization.

9. In the field of computer security, "social engineering" is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information.

10. Defendants **TIMOTHY C. McKEAGE, JUSTIN A. PERRAS, JASON DANIEL HAWKS, ZACHARY WILEY MANN, and JEFFREY ROBERT WEINBERG** were avid computer users who participated in online communications with each other and with other individuals.

COUNT 1
(Conspiracy to Commit Computer Fraud and Aggravated Identity Theft)
18 U.S.C. § 371

1. Paragraphs 1 through 10 of the General Allegations section are realleged and incorporated by reference as though fully set forth herein.

2. From on or about January 21, 2005, and continuing through on or about May 16, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendants,

TIMOTHY C. McKEAGE,
JUSTIN A. PERRAS,
JASON DANIEL HAWKS,
ZACHARY WILEY MANN, and
JEFFREY ROBERT WEINBERG,

did willfully, that is, with the specific intent to further the unlawful purpose, and knowingly combine, conspire, confederate, and agree with each other, and with persons known and unknown to the Grand Jury, to commit offenses against the United States, that is:

- A. to violate Title 18, United States Code, Section 1030(a)(4) by knowingly and with intent to defraud, access a protected computer that was used in interstate commerce and communication, without authorization, and by means of such conduct furthers an intended fraud and obtains anything of value; and
- B. to violate Title 18, United States Code, Section 1028A by knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony contained in Title 18, United States Code, Chapter 47, that is, a violation of Title 18, United States Code, Section 1030(a)(4).

PURPOSE OF THE CONSPIRACY

3. It was a purpose of the conspiracy for the defendants to access protected computers without authorization and to obtain identity information, which they transferred, possessed, and used without lawful authority.

MANNER AND MEANS OF THE CONSPIRACY

The manner and means by which the defendants and their co-conspirators sought to accomplish the purpose and objects of the conspiracy included, the following:

4. Conspirators utilized a Trojan Horse to infect the Port Orange Police Department's computer, which was used in interstate commerce and communication, in order to obtain unauthorized access to the Department's computer, and thereafter fraudulently accessed the Department's Accurint account.

Department's Accurint account.

5. Conspirators utilized social engineering to obtain unauthorized access to the Accurint account of Denton County, Texas.

6. Through these unauthorized accesses, conspirators fraudulently created usernames and passwords for the Accurint database, which were used and distributed by the conspirators to access the Accurint database.

7. Conspirators fraudulently accessed the Accurint database to obtain, transfer, possess, and use identification information of others, including names, addresses, dates of birth, and social security numbers.

OVERT ACTS

In furtherance of the conspiracy, and to accomplish its purpose and objects, at least one of the co-conspirators committed or caused to be committed, in the Southern District of Florida, and elsewhere, at least one of the following overt acts, among others:

1. Between on or about January 21, 2005, and on or about March 12, 2005, **TIMOTHY C. McKEAGE** used a Trojan Horse program to access the Port Orange Police Department's computer system. The Trojan Horse program infected a computer of the Port Orange Police Department, which was used in interstate commerce and communication, thereby allowing **TIMOTHY C. McKEAGE** unauthorized access to the computer.

2. Between on or about January 21, 2005, and on or about March 12, 2005, **TIMOTHY C. McKEAGE** utilized this unauthorized access to fraudulently obtain usernames, passwords, and other information, which he subsequently used to create additional usernames and passwords to access the Accurint database.

3. Between on or about January 21, 2005, and on or about March 12, 2005, **TIMOTHY C. McKEAGE** fraudulently utilized usernames and passwords to access the Accurint database and obtain identification information of other individuals.

4. Between on or about January 21, 2005, and on or about March 12, 2005, **TIMOTHY C. McKEAGE** provided **JEFFREY DAVID WEINBERG** and other co-conspirators fraudulently created usernames and passwords that allowed access to the Port Orange Police Department account on the Accurint database.

5. Between on or about January 21, 2005, and on or about March 12, 2005, **JUSTIN A. PERRAS** fraudulently obtained access to a Denton County, Texas Accurint account by impersonating LexisNexis personnel and contacting Seisint, Inc., in order to obtain unauthorized access to the Accurint database. Through this unauthorized access, **JUSTIN A. PERRAS** fraudulently created usernames and passwords for the Accurint database, which he then used and distributed to co-conspirators.

6. On or about January 21, 2005, **TIMOTHY C. McKEAGE** fraudulently obtained an Accurint report of an individual, J.P., containing J.P.'s name, address, date of birth, social security number, and other identification information.

7. On or about January 21, 2005, **TIMOTHY C. McKEAGE** fraudulently obtained an Accurint report of an individual, D.G., containing D.G.'s name, address, date of birth, social security number, and other identification information.

8. On or about January 25, 2005, **JUSTIN A. PERRAS** fraudulently obtained an Accurint report of an individual, J.B., containing J.B.'s name, address, date of birth, social security number, and other identification information.

9. On or about January 25, 2005, **JUSTIN A. PERRAS** fraudulently obtained an Accurint report of an individual, A.S., containing A.S.'s name, address, date of birth, social security number, and other identification information.

10. On or about January 29, 2005, **JASON DANIEL HAWKS** fraudulently obtained an Accurint report of an individual, D.O., containing D.O.'s name, address, date of birth, social security number, and other identification information.

11. On or about January 30, 2005, **JASON DANIEL HAWKS** fraudulently obtained an Accurint report of an individual, S.G., containing S.G.'s name, address, date of birth, social security number, and other identification information.

12. On or about January 30, 2005, **JASON DANIEL HAWKS** fraudulently obtained an Accurint report of an individual, L.G., containing L.G.'s name, address, date of birth, social security number, and other identification information.

13. On or about January 30, 2005, **JASON DANIEL HAWKS** fraudulently obtained an Accurint report of an individual, N.G., containing N.G.'s name, address, date of birth, social security number, and other identification information.

14. On or about January 30, 2005, **ZACHARY WILEY MANN** fraudulently obtained an Accurint report of an individual, L.F., containing L.F.'s name, address, date of birth, social security number, and other identification information.

15. On or about January 30, 2005, **ZACHARY WILEY MANN** fraudulently obtained an Accurint report of an individual, D.B., containing D.B.'s name, address, date of birth, social security number, and other identification information.

16. On or about April 14, 2005, **ZACHARY WILEY MANN** transferred portions of the

fraudulently obtained Accurint report concerning D.B., by posting excerpts of the report, including D.B.'s name, address, date of birth, social security number, and criminal history, on the Internet.

17. On or about January 23, 2005, **JEFFREY ROBERT WEINBERG** fraudulently obtained an Accurint report of an individual, P.H., containing P.H.'s name, address, date of birth, social security number, and other identification information.

18. On or about January 23, 2005, **JEFFREY ROBERT WEINBERG** fraudulently obtained an Accurint report of an individual, D.M., containing D.M.'s name, address, date of birth, social security number, and other identification information.

19. On or about January 23, 2005, **JEFFREY ROBERT WEINBERG** fraudulently obtained an Accurint report of an individual, P.M., containing P.M.'s name, address, date of birth, social security number, and other identification information.

20. On or about January 23, 2005, **JEFFREY ROBERT WEINBERG** fraudulently obtained an Accurint report of an individual, B.D., containing B.D.'s name, address, date of birth, social security number, and other identification information.

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

COUNT 2
(Computer Fraud)
18 U.S.C. §§ 1030(a)(4) and 2

Between on or about January 21, 2005, and on or about March 12, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

TIMOTHY C. McKEAGE,

knowingly and with intent to defraud, accessed a protected computer used in interstate commerce

and communication, without authorization, and by means of such conduct, furthered an intended fraud and obtained anything of value, that is, Accurint database reports.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 2, and 1030(c)(3)(A).

COUNT 3
(Computer Fraud)
18 U.S.C. §§ 1030(a)(4) and 2

Between on or about January 21, 2005, and on or about March 12, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

JUSTIN A. PERRAS,

knowingly and with intent to defraud, accessed a protected computer used in interstate commerce and communication, without authorization, and by means of such conduct, furthered an intended fraud and obtained anything of value, that is, Accurint database reports.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 2, and 1030(c)(3)(A).

COUNT 4
(Computer Fraud)
18 U.S.C. §§ 1030(a)(4) and 2

Between on or about January 21, 2005, and on or about March 12, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

JASON DANIEL HAWKS,

knowingly and with intent to defraud, accessed a protected computer used in interstate commerce and communication, without authorization, and by means of such conduct, furthered an intended fraud and obtained anything of value, that is, Accurint database reports.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 2, and 1030(c)(3)(A).

COUNT 5
(Computer Fraud)
18 U.S.C. §§ 1030(a)(4) and 2

Between on or about January 21, 2005, and on or about March 12, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

ZACHARY WILEY MANN,

knowingly and with intent to defraud, accessed a protected computer used in interstate commerce and communication, without authorization, and by means of such conduct, furthered an intended fraud and obtained anything of value, that is, Accurint database reports.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 2, and 1030(c)(3)(A).

COUNT 6
(Computer Fraud)
18 U.S.C. §§ 1030(a)(4) and 2

Between on or about January 21, 2005, and on or about March 12, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

JEFFREY ROBERT WEINBERG,

knowingly and with intent to defraud, accessed a protected computer used in interstate commerce and communication, without authorization, and by means of such conduct, furthered an intended fraud and obtained anything of value, that is, Accurint database reports.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 2, and 1030(c)(3)(A).

COUNT 7
(Aggravated Identity Theft)
18 U.S.C. §§ 1028A and 2

From on or about January 21, 2005, through on or about May 16, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

TIMOTHY C. McKEAGE,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, J.P., during and in relation to a felony contained in Title 18, United States Code, Chapter 47, that is, a violation of Title 18, United States Code, Section 1030(a)(4).

In violation of Title 18, United States Code, Sections 1028A and 2.

COUNT 8
(Aggravated Identity Theft)
18 U.S.C. §§ 1028A and 2

From on or about January 25, 2005, through on or about May 16, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

JUSTIN A. PERRAS,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, A.S., during and in relation to a felony contained in Title 18, United States Code, Chapter 47, that is, a violation of Title 18, United States Code, Section 1030(a)(4).

In violation of Title 18, United States Code, Sections 1028A and 2.

COUNT 9
(Aggravated Identity Theft)
18 U.S.C. §§ 1028A and 2

From on or about January 30, 2005, through on or about May 16, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

JASON DANIEL HAWKS,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, L.G., during and in relation to a felony contained in Title 18, United States Code, Chapter 47, that is, a violation of Title 18, United States Code, Section 1030(a)(4).

COUNT 10
(Aggravated Identity Theft)
18 U.S.C. §§ 1028A and 2

From on or about January 30, 2005, through on or about May 16, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

ZACHARY WILEY MANN,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, L.F., during and in relation to a felony contained in Title 18, United States Code, Chapter 47, that is, a violation of Title 18, United States Code, Section 1030(a)(4).

In violation of Title 18, United States Code, Sections 1028A and 2.

COUNT 11
(Aggravated Identity Theft)
18 U.S.C. §§ 1028A and 2


From on or about January 23, 2005, through on or about May 16, 2005, in Palm Beach County, in the Southern District of Florida, and elsewhere, the defendant,

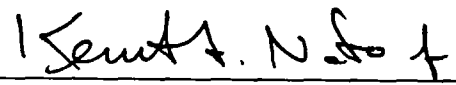
JEFFREY ROBERT WEINBERG,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, P.H., during and in relation to a felony contained in Title 18, United States Code, Chapter 47, that is, a violation of Title 18, United States Code, Section 1030(a)(4).

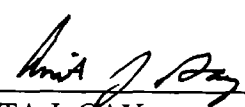
In violation of Title 18, United States Code, Sections 1028A and 2.

A TRUE BILL


FOREPERSON



R. ALEXANDER ACOSTA
UNITED STATES ATTORNEY



ANITA J. GAY
ASSISTANT UNITED STATES ATTORNEY

VICTIM LIST REPORTING FORM

AUSA: Anita J. Gay

1. **CASE: United States v. Timothy McKeage, et al.**
2. **USAO NUMBER: 2005R00622**
3. **SHORT DESCRIPTION**
OF CHARGES: Computer Fraud; Aggravated Identity Theft
[Example: Drugs; bank robbery; boilerroom; carjacking; counterfeiting, etc.]
4. **Number of Victims: Persons: 0 Banks/Corps: 1**
[May be approximate].

A Victim List must accompany the indictment in any case in which a person or entity has suffered a financial loss or personal injury, as well as in the following “mandatory restitution” cases [Title 18, U.S.C. 3664(d)]:

Crimes of Violence
Sexual Abuse
Sexual Exploitation and Other Abuse of Children
Domestic Violence
Telemarketing Fraud
Property Crimes under Title 18, including fraud & deceit
Consumer Product Tampering

Provide the following information as to each victim:

Name
Street Address
City, State, Zip Code
Social Security Number

Seisint
6601 Park of Commerce Blvd. N.W.
Boca Raton, Florida 33487
(561) 999-4400

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

UNITED STATES OF AMERICA

05-80167 CR-RYSKAMP

7/HOPKINS

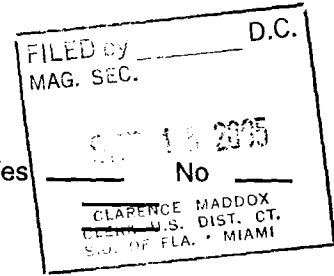
vs.

TIMOTHY C. McKEAGE,
JUSTIN A. PERRAS,
JASON DANIEL HAWKS,
ZACHARY WILEY MANN, and
JEFFREY ROBERT WEINBERG,

CERTIFICATE OF TRIAL ATTORNEY*

Defendants.

Superseding Case Information:



Court Division: (Select One)

___ Miami ___ Key West
___ FTL X WPB ___ FTP

New Defendant(s) _____
Number of New Defendants _____
Total number of counts _____

Yes _____ No _____

I do hereby certify that:

1. I have carefully considered the allegations of the indictment, the number of defendants, the number of probable witnesses and the legal complexities of the Indictment/Information attached hereto.

2. I am aware that the information supplied on this statement will be relied upon by the Judges of this Court in setting their calendars and scheduling criminal trials under the mandate of the Speedy Trial Act, Title 28 U.S.C. Section 3161.

3. Interpreter: (Yes or No) No
List language and/or dialect _____

4. This case will take 10 days for the parties to try.

5. Please check appropriate category and type of offense listed below:
(Check only one) (Check only one)

I	0 to 5 days	_____	Petty	_____
II	6 to 10 days	<u>X</u>	Minor	_____
III	11 to 20 days	_____	Misdem.	_____
IV	21 to 60 days	_____	Felony	<u>X</u>
V	61 days and over	_____		

6. Has this case been previously filed in this District Court? (Yes or No) No

If yes:
Judge: _____ Case No. _____

(Attach copy of dispositive order)
Has a complaint been filed in this matter? (Yes or No) No

If yes:
Magistrate Case No. _____

Related Miscellaneous numbers: _____

Defendant(s) in federal custody as of _____

Defendant(s) in state custody as of _____

Rule 20 from the _____ District of _____

Is this a potential death penalty case? (Yes or No) No

7. Does this case originate from a matter pending in the U.S. Attorney's Office prior to April 1, 2003? ___ Yes X No

8. Does this case originate from a matter pending in the U. S. Attorney's Office prior to April 1, 1999? ___ Yes X No
If yes, was it pending in the Central Region? ___ Yes ___ No

9. Does this case originate from a matter pending in the Northern Region of the U.S. Attorney's Office prior to October 14, 2003? ___ Yes X No

10. Does this case originate from a matter pending in the Narcotics Section (Miami) prior to May 18, 2003? ___ Yes X No

ANITA J. GAY
ASSISTANT UNITED STATES ATTORNEY
Florida Bar No. 0745227

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PENALTY SHEET

Defendant's Name: Timothy C. McKeage

Case No. **05-80167 CR-RYSKAMP** / HOPKINS

Count #: 1

Conspiracy to Commit Computer Fraud and Aggravated Identity Theft

18 U.S.C. § 371

*** Max. Penalty: 5 years' imprisonment**

Count #: 2

Computer Fraud

18 U.S.C. § 1030(a)(4)

***Max. Penalty: 5 years' imprisonment**

Count #: 7

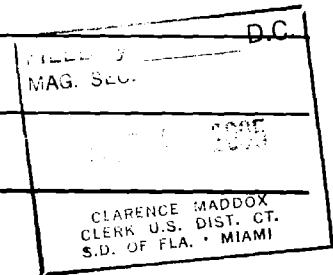
Aggravated Identity Theft

18 U.S.C. § 1028A

***Max. Penalty: 2 years' imprisonment**

Count #:

***Max. Penalty:**



***Refers only to possible term of incarceration, does not include possible fines, restitution, special assessments, parole terms, or forfeitures that may be applicable.**

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PENALTY SHEET

Defendant's Name: Justin A. Perras

Case No: **05-80167 CR-RYSKAMP** ⁷HOPKINS

Count #: 1

Conspiracy to Commit Computer Fraud and Aggravated Identity Theft

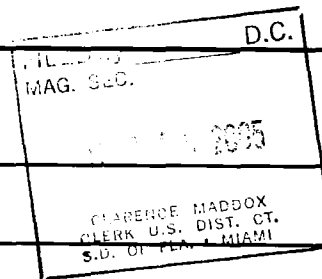
18 U.S.C. § 371

*** Max. Penalty: 5 years' imprisonment**

Count #: 3

Computer Fraud

18 U.S.C. § 1030(a)(4)



***Max. Penalty: 5 years' imprisonment**

Count #: 8

Aggravated Identity Theft

18 U.S.C. § 1028A

***Max. Penalty: 2 years' imprisonment**

Count #:

***Max. Penalty:**

***Refers only to possible term of incarceration, does not include possible fines, restitution, special assessments, parole terms, or forfeitures that may be applicable.**

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PENALTY SHEET

Defendant's Name: Jason Daniel Hawks

Case No. **05-80167CR-RYSKAMP** 7HOPKINS

Count #: 1

Conspiracy to Commit Computer Fraud and Aggravated Identity Theft

18 U.S.C. § 371

*** Max. Penalty: 5 years' imprisonment**

Count #: 4

Computer Fraud

18 U.S.C. § 1030(a)(4)

***Max. Penalty: 5 years' imprisonment**

Count #: 9

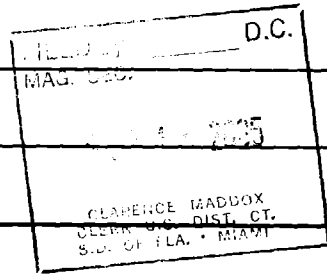
Aggravated Identity Theft

18 U.S.C. § 1028A

***Max. Penalty: 2 years' imprisonment**

Count #:

***Max. Penalty:**



***Refers only to possible term of incarceration, does not include possible fines, restitution, special assessments, parole terms, or forfeitures that may be applicable.**

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PENALTY SHEET

Defendant's Name: Zachary Wiley Mann

Case No: 05-80167 CR-RYSKAMP HOPKINS

Count #: 1

Conspiracy to Commit Computer Fraud and Aggravated Identity Theft

18 U.S.C. § 371

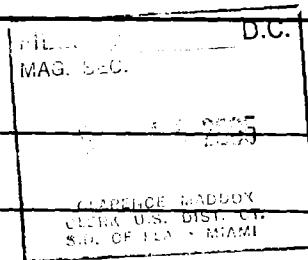
*** Max. Penalty: 5 years' imprisonment**

Count #: 5

Computer Fraud

18 U.S.C. § 1030(a)(4)

***Max. Penalty: 5 years' imprisonment**



Count #: 10

Aggravated Identity Theft

18 U.S.C. § 1028A

***Max. Penalty: 2 years' imprisonment**

Count #:

***Max. Penalty:**

***Refers only to possible term of incarceration, does not include possible fines, restitution, special assessments, parole terms, or forfeitures that may be applicable.**

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PENALTY SHEET

Defendant's Name: Jeffrey Robert Weinberg

Case No: **05-80167** CR-RYSKAMP /HOPKINS

Count #: 1

Conspiracy to Commit Computer Fraud and Aggravated Identity Theft

18 U.S.C. § 371

*** Max. Penalty: 5 years' imprisonment**

Count #: 6

Computer Fraud

18 U.S.C. § 1030(a)(4)

FILED BY	D.C.
MAG. SEC.	
AUG 1 2005	
CLERK OF DISTRICT COURT SOUTHERN DISTRICT OF FLORIDA MIAMI	

***Max. Penalty: 5 years' imprisonment**

Count #: 11

Aggravated Identity Theft

18 U.S.C. § 1028A

***Max. Penalty: 2 years' imprisonment**

Count #:

***Max. Penalty:**

***Refers only to possible term of incarceration, does not include possible fines, restitution, special assessments, parole terms, or forfeitures that may be applicable.**

05-80167CR-1748-1
HOPKINS

UNITED STATES DISTRICT COURT

SOUTHERN District of FLORIDA

THE UNITED STATES OF AMERICA

vs.

Timothy C. McKeage,
et al.,

Defendants.

INDICTMENT

18 U.S.C. § 371
18 U.S.C. § 1030(a)(4)
18 U.S.C. § 1028A
18 U.S.C. § 2

A true bill.

Franklin P. Frazier
FGJ 04-805 (MIA) Foreman

Filed in open court this 15th day of September A.D. 2005.

W. J. Flood Deputy Clerk

Bail \$ _____

Grand Jury
Indictment No. 04-805-EGS-0037