No. 2009R00728

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FILED

2011 JUL -6 P 4: 04

EJD

San Jose Division

SEALED BY ORDER OF THE COURT

CR11 00456

THE UNITED STATES OF AMERICA

vs.

SANFORD WALLACE,
a/k/a "The Spam King,"
a/k/a "Spamford" a/k/a "David Frederix"

INDICTMENT

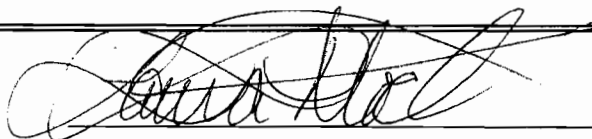|	
COUNTS 1, 3 and 7:	18 U.S.C. §§ 1037(a)(1) and (b)(2)(A); - Fraud and Related Activity in Connection with Electronic Mail;
COUNTS 2, 6 and 9:	18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(I) - Intentional Damage to a Protected Computer;
COUNTS 4 and 8:	18 U.S.C. §§ 1037(a)(2) and (b)(2)(C)-Fraud and Related Activity in Connection With Electronic Mail;
COUNT 5:	18 U.S.C. §§ 1037(a)(4) and (b)(2)(B) - Fraud and Related Activity in Connection With Electronic Mail;
COUNTS 10 and 11:	18 U.S.C. § 401(3) - Criminal Contempt.

A true bill.

_____
Foreperson

Filed in open court this ___6th___ *day of* ___July___

A.D. 2011

DOCUMENT NO.
CLA's INITIALS
1
c
DISTRICT COURT

_____
United States Magistrate Judge

Bail. $ No bail arrest warrant

MELINDA HAAG (CABN 132612)
United States Attorney

F I L E D

'1 JUL -b P 4: 04

SEALED BY ORDER OF THE COURT

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

EJD

UNITED STATES OF AMERICA,

    Plaintiff,

    v.

SANFORD WALLACE,
a/k/a "The Spam King,"
a/k/a "Spamford,"
a/k/a "David Frederix,"

    Defendant.

CR11 00456

)
)
)
)
)
)
)
)
)
)
)
)
)
)
)
)
)
)
)
)

VIOLATIONS: 18 U.S.C. §§ 1037(a)(1) and
(b)(2)(A) - Fraud and Related Activity in
Connection With Electronic Mail; 18 U.S.C.
§§ 1037(a)(2) and (b)(2)(C) - Fraud and
Related Activity in Connection With
Electronic Mail; 18 U.S.C. §§ 1037(a)(4)
and (b)(2)(B) - Fraud and Related Activity in
Connection With Electronic Mail; 18 U.S.C.
§§ 1030(a)(5)(A) and (c)(4)(B)(i) -
Intentional Damage to a Protected
Computer; 18 U.S.C. § 401(3) – Criminal
Contempt (Felony); 18 U.S.C. §§ 1030(i)
and (j) - Criminal Forfeiture; 18 U.S.C.
§ 1037(c) - Criminal Forfeiture

SAN JOSE VENUE

I N D I C T M E N T

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this indictment:

1.   Facebook, Inc. (Facebook) owned and operated the popular social networking site

located at www.facebook.com, which has more than 500 million users worldwide. The company

was headquartered and maintained its computer network in Palo Alto, California, and other

locations.

INDICTMENT

2.   In order to establish an account with Facebook, a user must register and create a unique username and password. Once registered, the user can customize his or her profile by, among other things, adding contact information, lists of personal interests, and photographs, that the user can share with other Facebook users. Only a registered user may access Facebook user profiles, invite other Facebook users to be a "friend," and use the Facebook network, service, or applications. Facebook "friends" have the ability to send and receive messages, and share information with each other, and have complete control over those with whom they chose to interact with on Facebook. A user also has the ability to control access to the user's profile through a privacy setting. A Facebook user may only be contacted by registered Facebook users, authorized Facebook Pages and Groups, or Facebook itself.

3.   When an individual accesses Facebook's website, he or she must agree to Facebook's Terms of Use, which set forth the permissible and impermissible uses of Facebook's network. For example, a user is prohibited from accessing Facebook's website to engage in the following:

   a.   harvesting or collecting e-mail addresses or other contact information of other users from Facebook by electronic or other means for purposes of sending unsolicited e-mails or other unsolicited communications;

   b.   using the Facebook's website in a manner that could damage, disable, overburden, or impair the website;

   c.   uploading, posting, transmitting, sharing, or otherwise making available any unsolicited or unauthorized advertising, solicitation, promotional materials, junk mail, spam, chain letters, pyramid schemes, or any other form of solicitation;

   d.   using or attempting to use another's account, service, or system without authorization from Facebook, or create a false identity on Facebook.

WALLACE'S SCHEME TO SPAM FACEBOOK USERS

4.   SANFORD WALLACE was a resident of Las Vegas, Nevada.

5.   From approximately November 2008 through March 2009, WALLACE developed and executed a scheme to send spam messages to Facebook users that compromised

1 approximately 500,000 legitimate Facebook accounts, and resulted in over 27 million spam

2 messages being sent through Facebook's servers.

3   6.   To accomplish his scheme, WALLACE first tested his spamming capabilities

4 between two Facebook accounts. On November 4, 2008, WALLACE used a fake Facebook

5 account of "David Frederix" and his legitimate Facebook "Sanford MasterWeb Wallace" account

6 to test variations of spam messages in order to evade Facebook's filtering mechanisms. Once

7 WALLACE evaded Facebook's spam filters, he employed an automated scripting process to sign

8 into a compromised Facebook user's account, retrieve a list of all of the user's friends, and then

9 post a spam message to each of the user's friends' Facebook walls.

10   7.   It was part of the scheme that WALLACE purposely deceived legitimate

11 Facebook account holders into visiting the website mentioned on the spam message that was

12 purportedly from a Facebook friend.

13   8.   It was part of the scheme that WALLACE collected users' e-mail addresses and

14 passwords by deceiving users into providing the user's full name, valid e-mail address, and

15 password. Once the user entered his or her information, the user would be redirected to an

16 affiliate website where WALLACE earned substantial revenue for directing Internet traffic.

17   9.   WALLACE continued his spamming scheme by storing the information provided

18 by Facebook users, such as e-mail addresses and passwords. WALLACE then used the user's

19 e-mail address and password to log into Facebook in order to continue to send spam messages.

20   10.   It was further part of the scheme that WALLACE hid his identity as the sender of

21 spam messages. On May 21, 2008, he opened an account at the domain registrar Moniker Online

22 Services under the name of an individual identified as "A.A." in order to register over 1,000

23 domain names. WALLACE used at least one domain name, "GayestProfile.com," registered

24 through Moniker, to post spam messages in Facebook users' accounts in November 2008.

25 Neither "A.A." nor other individuals linked to the account gave WALLACE permission to use

26 their names to establish an account at Moniker.

27   11.   In addition, on December 14, 2008, WALLACE opened an account at the domain

28 registrar Dynadot, LLC under the fictitious name "Laura Frederix," and registered approximately

1,500 domain names. WALLACE used these domain names in spamming attacks on Facebook

users in December 2008 and February 2009.

DEFINITIONS

12. As used herein, "spam" refers to the fraudulent commercial electronic mail

messages sent to multiple individuals over the Internet, or to the act of sending such messages.

13. The term "commercial electronic mail message" means any electronic mail

message the primary purpose of which is the commercial advertisement or promotion of a

commercial product or service, including content on an Internet website operated for a

commercial purpose.

14. A domain name is an identification label that defines a realm of administrative

autonomy, authority, or control in the Internet. Domain names are host names that identify

Internet Protocol resources such as websites. Domain names are formed by the rules and

procedures of the Domain Name System. Domain names are often referred to simply as domains

and domain name registrants are frequently referred to as domain owners, although domain name

registration with a registrar does not confer any legal ownership of the domain name, only an

exclusive right of use.

15. A server is a centralized computer that provides services for other computers

connected to it via a network. The other computers attached to a server are sometimes called

"clients." Server computers can be physically stored in any location; it is common for a

network's server to be located hundreds (and even thousands) of miles away from the client

computers.

16. The Internet Protocol address (or simply "IP" address) is a unique numeric address

used by computers on the Internet. An IP address consists of a series of four numbers, each in

the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the

Internet computer must be assigned an IP address so that Internet traffic sent from and directed to

that computer may be directed properly from its source to its destination. Most Internet service

providers control a range of IP addresses.

17. A proxy or proxy server is a computer system or an application that acts as an

INDICTMENT   4

intermediary for request from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server.

COUNT ONE: (18 U.S.C. §§ 1037(a)(1) and (b)(2)(A) - Fraud and Related Activity in Connection With Electronic Mail)

18.   The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

19.   From on or about November 5, 2008, and continuing to on or about approximately November 6, 2008, in the Northern of California and elsewhere, the defendant,

SANFORD WALLACE,

knowingly accessed a protected computer without authorization, and intentionally initiated the transmission of multiple commercial electronic mail messages from or through such computer, in and affecting interstate and foreign commerce, to wit: the defendant accessed Facebook's computer network in order to initiate the transmission of program that resulted in more than 125,000 spam messages being sent to Facebook users.

All in violation of Title 18, United States Code, Sections 1037(a)(1) and (b)(2)(A).

COUNT TWO: (18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i) - Intentional Damage to a Protected Computer)

20.   The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

21.   From on or about November 5, 2008, and continuing until approximately November 6, 2008, in the Northern District of California, the defendant,

SANFORD WALLACE,

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss to a person during a one-year period from the defendant's course of conducting affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), to wit:

Facebook's computer network sustained damage from the large amount of computer network resources used during the defendant's transmission of spam messages through its system, which resulted in Facebook spending a significant amount of time, money, and resources responding to and fixing the damage caused to its network as well as to protect and defend its network from future spam campaigns by the defendant.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

COUNT THREE: (18 U.S.C. §§ 1037(a)(1) and (b)(2)(A) - Fraud and Related Activity in Connection With Electronic Mail)

22.   The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

23.   On or about December 28, 2008, in the Northern of California and elsewhere, the defendant,

SANFORD WALLACE,

knowingly accessed a protected computer without authorization, and intentionally initiated the transmission of multiple commercial electronic mail messages from or through such computer, in and affecting interstate and foreign commerce, to wit: the defendant accessed Facebook's computer network in order to initiate the transmission of program that resulted in nearly 300,000 spam messages being sent to Facebook users.

All in violation of Title 18, United States Code, Sections 1037(a)(1) and (b)(2)(A).

COUNT FOUR: (18 U.S.C. §§ 1037(a)(2) and (b)(2)(C) - Fraud and Related Activity in Connection With Electronic Mail)

24.   The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

25.   On or about December 28, 2008, in the Northern of California and elsewhere, the defendant,

SANFORD WALLACE,

knowingly used a protected computer to relay and retransmit multiple commercial electronic mail messages, in and affecting interstate and foreign commerce, with the intent to deceive and mislead recipients and an Internet access service, as to the origin of such messages, and the

INDICTMENT   6

volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, and 250,000 during any one-year period; to wit: the defendant accessed Facebook's computer network from 143 IP addresses that were proxies in order to deceive Facebook and Facebook users as to the origin of the messages and to initiate the transmission of program that resulted in nearly 300,000 spam messages being sent to Facebook users.

All in violation of Title 18, United States Code, Sections 1037(a)(2) and (b)(2)(C).

COUNT FIVE: (18 U.S.C. §§ 1037(a)(4) and (b)(2)(B) - Fraud and Related Activity in Connection With Electronic Mail)

26. The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

27. On or about December 28, 2008, in the Northern of California and elsewhere, the defendant,

                    SANFORD WALLACE,

knowingly registered, using information that materially falsified the identity of the actual registrant, two or more domain names, and intentionally initiated the transmission of multiple commercial electronic mail messages from such domain names, in or affecting interstate and foreign commerce, and the offense involved 10 or more falsified domain name registrations, to wit: the defendant accessed Facebook's computer network originating from 143 IP addresses utilizing over 1,500 domain names in order to deceive Facebook and Facebook users as to the origin of the messages and to initiate the transmission of a program that resulted in nearly 300,000 spam messages being sent to Facebook users. The domain names were registered under the fictitious name Laura Frederix and later changed to Victoria David, falsifying the identity of the actual registrant.

All in violation of Title 18, United States Code, Sections 1037(a)(2) and (b)(2)(C).

COUNT SIX: (18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i) - Intentional Damage to a Protected Computer)

28. The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

29. On or about December 28, 2008, in the Northern District of California, the defendant,

SANFORD WALLACE,

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss to a person during a one-year period from the defendant's course of conducting affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), to wit: Facebook's computer network sustained damage from the large amount of computer network resources used during the defendant's transmission of spam messages through its system, which resulted in Facebook spending a significant amount of time, money, and resources responding to and fixing the damage caused to its network as well as to protect and defend its network from future spam campaigns by the defendant.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

COUNT SEVEN: (18 U.S.C. § 1037(a)(1) and (b)(2)(A) - Fraud and Related Activity in Connection With Electronic Mail)

30. The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

31. On or about February 17, 2009, in the Northern of California and elsewhere, the defendant,

SANFORD WALLACE,

knowingly accessed a protected computer without authorization, and intentionally initiated the transmission of multiple commercial electronic mail messages from or through such computer, in and affecting interstate and foreign commerce, to wit: the defendant accessed Facebook's computer network in order to initiate the transmission of program that resulted in more than 125,00 spam messages being sent to Facebook users.

All in violation of Title 18, United States Code, Sections 1037(a)(1) and (b)(2)(A).

//

COUNT EIGHT: (18 U.S.C. §§ 1037(a)(2) and (b)(2)(C) - Fraud and Related Activity in Connection With Electronic Mail)

32.   The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

33.   On or about February 17, 2009, in the Northern of California and elsewhere, the defendant,

SANFORD WALLACE,

knowingly used a protected computer to relay and retransmit multiple commercial electronic mail messages, in and affecting interstate and foreign commerce, with the intent to deceive and mislead recipients and an Internet access service, as to the origin of such messages, and the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, and 250,000 during any one-year period, to wit: the defendant accessed Facebook's computer network from 50 IP addresses that were proxies in order to deceive Facebook and Facebook users as to the origin of the messages and to initiate the transmission of program that resulted in more than 125,000 spam messages being sent to Facebook users.

All in violation of Title 18, United States Code, Sections 1037(a)(2) and (b)(2)(C).

COUNT NINE: (18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i) - Intentional Damage to a Protected Computer)

34.   The factual allegations contained in Paragraphs One through Eleven above are realleged and incorporated herein as if set forth in full.

35.   On or about February 17, 2009, in the Northern District of California, the defendant,

SANFORD WALLACE,

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss to a person during a 1-year period from the defendant's course of conducting affecting protected computers aggregating at least $5,000 in value, in

violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), to wit: Facebook's computer network sustained damage from the large amount of computer network resources used during the defendant's transmission of spam messages through its system, which resulted in Facebook spending a significant amount of time, money, and resources responding to and fixing the damage caused to its network as well as to protect and defend its network from future spam campaigns by the defendant.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

COUNT TEN: (18 U.S.C. § 401(3) – Criminal Contempt)

36.   On or about April 17, 2009, in the Northern District of California and elsewhere, the defendant,

SANFORD WALLACE,

did willfully and knowingly disobey and resist a lawful order of a Court of the United States, that is, the orders issued by the Honorable Jeremy Fogel, United States District Court Judge, on March 2, 2009, and March 24, 2009, in the Northern District of California in the case of *Facebook, Inc. v. Sanford Wallace, et al*, No. 09-00798 JF, to wit: Judge Fogel ordered the defendant not to access Facebook's computer network, and the defendant logged into his Facebook account while aboard a Virgin Airlines flight from Las Vegas, Nevada, to New York, New York.

All in violation of Title 18, United States Code, Section 401(3).

COUNT ELEVEN: (18 U.S.C. § 401(3) – Criminal Contempt)

37.   On or about January 26, 2011, and continuing to at least to February 16, 2011, in the Northern District of California and elsewhere, the defendant,

SANFORD WALLACE,

did willfully and knowingly disobey and resist a lawful order of a Court of the United States, that is, the orders issued by the Honorable Jeremy Fogel, United States District Court Judge, on March 2, 2009, March 24, 2009, and September 18, 2009, in the Northern District of California in the case of *Facebook, Inc. v. Sanford Wallace, et al*, No. 09-00798 JF, to wit: Judge Fogel ordered the defendant not to access Facebook's computer network, and he refused to comply

INDICTMENT   10

with the order of the Court by maintaining a Facebook profile entitled "David Sinful-Saturdays Fredericks."

All in violation of Title 18, United States Code, Section 401(3).

FORFEITURE ALLEGATION ONE: (18 U.S.C. §§ 1030(i) and (j) and 21 U.S.C. § 853)

38.   The factual allegations contained in Paragraphs One through Eleven, and Counts Two, Six, and Nine are hereby realleged for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 1030(i) and (j).

39.   Upon conviction of the offense in violation of Title 18, United States Code, Section 1030(a)(5)(A) set forth in Counts Two, Six, and Nine of this Indictment, the defendant,

SANFORD WALLACE,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 1030(i) and (j), any personal property used or intended to be used to commit or to facilitate the commission of said violation or a conspiracy to violate said provision, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including but not limited to:

> a sum of money equal to the total amount of proceeds defendant obtained or derived from, directly or indirectly, from the violations.

40.   If any of the property described above, 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,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2).

INDICTMENT   11

All pursuant to Title 18, United States Code, Section 1030(i) and (j), and Title 21, United States Code, Section 853.

FORFEITURE ALLEGATION TWO: (18 U.S.C. § 1037(c) and 21 U.S.C. § 853)

41.   The factual allegations contained in Paragraphs One through Eleven and Counts One, Three through Five, Seven, and Eight are hereby realleged for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 1037(c).

42.   Upon conviction of the offense in violation of Title 18, United States Code, Section 1037(a)(1) and (a)(3) set forth in Counts One, Three, Four, Five, Seven, and Nine of this Indictment, the defendant,

SANFORD WALLACE,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 1030(c), any personal property used or intended to be used to commit or to facilitate the commission of said violation or a conspiracy to violate said provision, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including but not limited to:

        a sum of money equal to the total amount of proceeds defendant obtained or derived from, directly or indirectly, from the violation.

43.   If any of the property described above, 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,

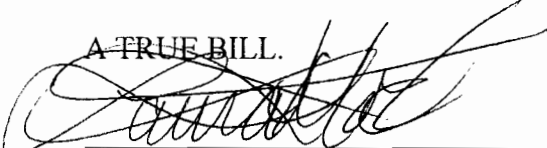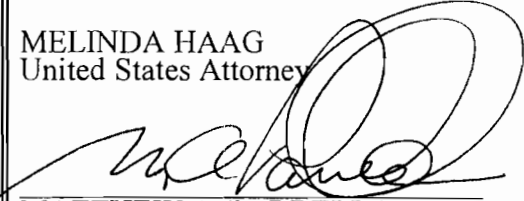the United States of America shall be entitled to forfeiture of substitute property pursuant to Title

//

//

21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(c).

All pursuant to Title 18, United States Code, Section 1037(c) and Title 21, United States Code, Section 853.

DATED: 07/06/2011

A TRUE BILL.

FOREPERSON

MELINDA HAAG
United States Attorney

MATTHEW A. PARRELLA
Chief, CHIP Unit

(Approved as to form:

AUSA SUSAN KNIGHT

INDICTMENT   13

AO 257 (Rev 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT

☐ SUPERSEDING

─── OFFENSE CHARGED ───

SEE ATTACHMENT

☐ Petty

☐ Minor

☐ Misde-
meanor

☒ Felony

SEALED BY ORDER
OF THE COURT

PENALTY SEE ATTACHMENT

─── PROCEEDING ───

Name of Complaintant Agency, or Person (& Title, if any)

FBI

☐ person is awaiting trial in another Federal or State Court,
give name of court

☐ this person/proceeding is transferred from another district
per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of
charges previously dismissed
which were dismissed on motion
of:

☐ U.S. ATTORNEY ☐ DEFENSE

} SHOW
DOCKET NO.

☐ this prosecution relates to a
pending case involving this same
defendant

☐ prior proceedings or appearance(s)
before U.S. Magistrate regarding this
defendant were recorded under

} MAGISTRATE
CASE NO.

Name and Office of Person
Furnishing Information on this form _____ MELINDA HAGG

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S.
Attorney (if assigned) SUSAN F. KNIGHT

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

2011 JUL -6 P 4: 04

─── DEFENDANT - U.S ───

▶ SANFORD WALLACE ⊞

DISTRICT COURT NUMBER

CR11 00456 EJI

DEFENDANT

HRL

IS NOT IN CUSTODY
Has not been arrested, pending outcome this proceeding.
1) ☒ If not detained give date any prior
summons was served on above charges ▶ _____

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction

6) ☐ Awaiting trial on other charges
If answer to (6) is "Yes", show name of institution

} ☒ Federal ☐ State

Has detainer ☐ Yes
been filed? ☐ No

} If "Yes"
give date
filed _____

DATE OF
ARREST ▶

Month/Day/Year
_____

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED
TO U.S. CUSTODY ▶

Month/Day/Year
_____

☐ This report amends AO 257 previously submitted

─── ADDITIONAL INFORMATION OR COMMENTS ───

PROCESS:

☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT Bail Amount: None

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

*Where defendant previously apprehended on complaint, no new summons or
warrant needed, since Magistrate has scheduled arraignment

Date/Time: _____ Before Judge: _____

Comments:

ATTACHMENT TO PENALTY SHEET
U.S. v. SANFORD WALLACE

COUNTS 1, 3 and 7:   18 U.S.C. §§ 1037(a)(1) and (b)(2)(A); - Fraud and Related
Activity in Connection with Electronic Mail

3 years imprisonment, $250,000 fine, 1 year supervised release,
$100 special assessment.

COUNTS 2, 6 and 9:   18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(I) - Intentional Damage
to a Protected Computer

10 years imprisonment, $250,000 fine, 3 years supervised release,
$100 special assessment.

COUNTS 4 and 8:   18 U.S.C. §§ 1037(a)(2) and (b)(2)(C)-Fraud and Related Activity
in Connection With Electronic Mail

3 years imprisonment, $250,000 fine, 1 year supervised release,
$100 special assessment.

COUNT 5:   18 U.S.C. §§ 1037(a)(4) and (b)(2)(B) - Fraud and Related Activity
in Connection With Electronic Mail

3 years imprisonment, $250,000 fine, 1 year supervised release,
$100 special assessment.

COUNTS 10 and 11:   18 U.S.C. § 401(3) - Criminal Contempt

Penalties determined by the court