

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>



April 19, 2019

MR. JOHN GREENEWALD, JR.
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384

FOIPA Request No.: 1385116-000
Subject: Equifax, Inc.

Dear Mr. Greenewald:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemptions boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552		Section 552a
<input type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input type="checkbox"/> (j)(2)
<input checked="" type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)
<u>50 U.S.C., Section 3024(i)(1)</u>	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)
_____	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)

37 pages were reviewed and 37 pages are being released.

Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

- Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].
- This information has been referred to the OGA(s) for review and direct response to you.
- We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. The **“Standard Responses to Requests”** section of the Addendum applies to all requests. If the subject of your request is a person, the **“Standard Responses to Requests for Individuals”** section also applies. The **“General Information”** section includes useful information about FBI records.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIA online portal by creating an account on the following website: <https://www.foiaonline.gov/foiaonline/action/public/home>. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

See additional information which follows.

The enclosed documents represent the final release of information responsive to your FOIA request. These documents are being provided on the enclosed CD at no charge.

Records which may have been responsive to your request were destroyed. Since this material could not be reviewed, it is not known if it was responsive to your request. Record retention and disposal is carried out under supervision of the National Archives and Records Administration (NARA), Title 44, United States Code, Section 3301 as implemented by Title 36, Code of Federal Regulations, Part 1228; Title 44, United States Code, Section 3310 as implemented by Title 36, Code of Federal Regulations, Part 1229.10.

For your information, a search of the indices to our Central Records System reflected there were additional records potentially responsive to your FOIA request. We have attempted to obtain this material so it could be reviewed to determine whether it was responsive to your request. We were advised that the potentially responsive records were not in their expected location and could not be located after a reasonable search. Following a reasonable waiting period, another attempt was made to obtain this material. This search for the missing records also met with unsuccessful results.

For your additional information, a record that may be responsive to your FOIA request has been transferred to the National Archives and Records Administration (NARA). You may desire to direct a request to NARA, 8601 Adelphi Road, College Park, MD 20740-6001. Please reference the file number 94-HQ-69069.

Sincerely,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Information Management Division

Enclosure(s)

FBI FOIPA Addendum

As referenced in our letter, the FBI FOIPA Addendum includes information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. If you submitted a request regarding yourself or another person, Part 2 includes additional standard responses that apply to requests for individuals. If you have questions regarding the standard responses in Parts 1 or 2, visit the www.fbi.gov/foia website under “Contact Us.” Previously mentioned appeal and dispute resolution services are also available. Part 3 includes general information about FBI records that you may find useful.

Part 1: Standard Responses to All Requests: See Below for all Requests

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). FBI responses are limited to those records subject to the requirements of the FOIA. Additional information about the FBI and the FOIPA can be found on the fbi.gov website.
- (ii) **National Security/Intelligence Records.** The FBI can neither confirm nor deny the existence of national security and foreign intelligence records pursuant to FOIA exemptions (b)(1) and (b)(3) and PA exemption (j)(2) as applicable to requests for records about individuals [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2); 50 U.S.C. § 3024(i)(1)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3); 50 USC § 3024(i)(1). This is a standard response and should not be read to indicate that national security or foreign intelligence records do or do not exist.

Part 2: Standard Responses to Requests for Individuals: See Below for all Requests for Individuals

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual’s name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E) and (b)(7)(F) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

- (i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching those systems or locations where responsive records would reasonably be found. Most requests are satisfied by searching the Central Record System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled and maintained by the FBI in the course of fulfilling its dual law enforcement and intelligence mission as well as the performance of agency administrative and personnel functions. The CRS spans the entire FBI organization and encompasses the records of FBI Headquarters (“FBIHQ”), FBI Field Offices, and FBI Legal Attaché Offices (“Legats”) worldwide. A CRS search includes Electronic Surveillance (ELSUR) records.
- (ii) **FBI Records**
Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Requests for Criminal History Records or “Rap Sheets.”** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks –often referred to as a criminal history record or “rap sheets.” These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.
- (iv) **The National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private citizens cannot request a name check.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

6/18/92
CIA
4/7/92

WDSAB; Intrusions
Into Equipment
Computers
CIA
DU:WMPFO

264B-WF-181147-1

SEARCHED	INDEXED
SERIALIZED	FILED

1866

b6
b7C

EQUIFAX

*The
Information
Source*

Equifax Credit Information Services, Inc.
1525 Windward Concourse
Alpharetta, Georgia 30302
Telephone (404) 740-7649
FAX (404) 740-6171

b6
b7C

DATE:	6 / 17 / 92
TO:	<div style="border: 1px solid black; width: 100%; height: 1.2em;"></div>
FAX #	(202) 324-6363
# PAGES	2
	Including Cover

b6
b7C

• MESSAGE •

Here is the request that I made to Pac-Tel regarding his support to help us find who the person(s) are that are stealing Equifax file information. This regards a stolen access code that our Equifax affiliate in Houston, Texas had assigned to Foleys Department Store.

b6
b7C

b6
b7C

The characteristics of this case are the same as a similar event that happened during April and May to our Brooks Brothers customer in New York. In that case, there were about 4,000 unauthorized accesses of our database. The Foley case is now close to 2,000 unauthorized accesses.

We need to catch these perpetrators!

b6
b7C

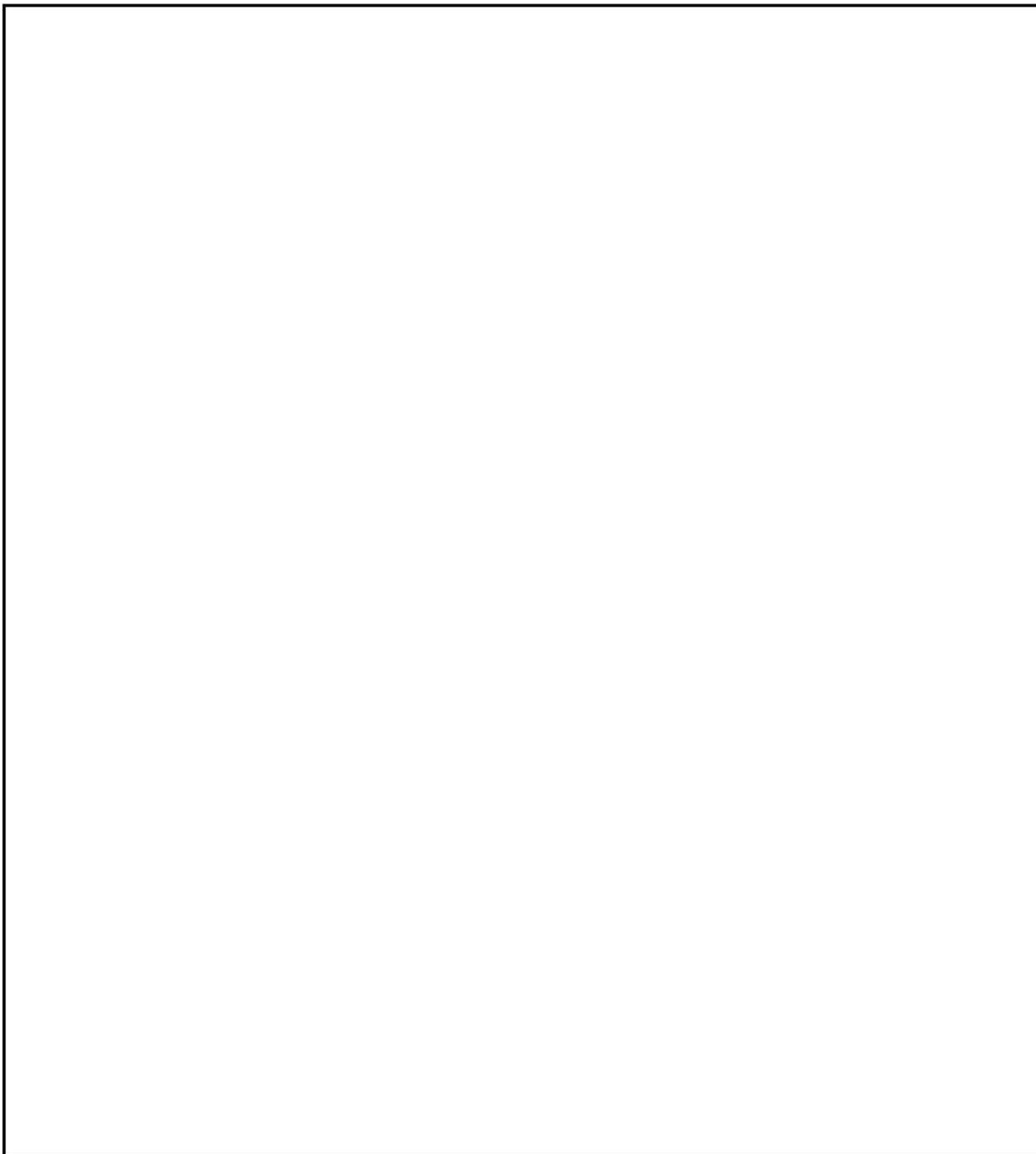
EQUIFAX MEMORANDUM

TO..... [] Pac-Tel

FROM..... [] Equifax Security

SUBJECT..... Unauthorized Access Through Equifax Ports

COPY TO..... [] FBI - Washington, D.C.



b6
b7C

b6
b7C
b7E

0-14

FBI

TRANSMIT VIA:

- Teletype
- Facsimile
- AIRTEL

PRECEDENCE:

- Immediate
- Priority
- Routine

CLASSIFICATION:

- ~~TOP SECRET~~
- ~~SECRET~~
- ~~CONFIDENTIAL~~
- UNCLAS E F T O
- UNCLAS

Date 6/18/92

FM FBI WMFO (264B-WF-NEW) C
 TO DIRECTOR FBI/PRIORITY/
 FBI ATLANTA/PRIORITY/
 FBI NEW YORK/PRIORITY/
 FBI SACRAMENTO/PRIORITY/
 FBI SAN FRANCISCO/PRIORITY/
 FBI SEATTLE/PRIORITY/

BT

UNCLAS

CITE: //3920//

SUBJECT: UNSUB; INTRUSIONS INTO COMPUTER SYSTEMS OF EQUIFAX,
 INC., AT SACRAMENTO, CALIFORNIA, SEATTLE, WASHINGTON, AND NEW
 YORK, NEW YORK; CFA; OO:WMFO.

RE WMFO TELETYPE TO BUREAU DATED 6/17/92, WMFO FAXS TO AT
 AND SC ON 6/17/92, AND TELEPHONE CALLS FROM SSA

b6
b7C

264B-WF-181147-20
 SEARCHED INDEXED
 SERIALIZED FILED

b6
b7C

Approved: _____ Original filename: SUBCOIN.WF **JUL 07 1992**

Time Received: 11:25 Telprep filename: _____

MRI/JULIAN DATE: 856/170 ISN: 028

FOX DATE & TIME OF ACCEPTANCE: 18 June 92 1628 11:28

me

^PAGE 2 264B-WF-NEW UNCLAS

[REDACTED] WMFO, AND SSA [REDACTED] SC, AND SSA [REDACTED] AT, ON
6/17/92.

b6
b7C

ALL OFFICES DISCONTINUE INVESTIGATION.

BASED ON THE MEMORANDUM BETWEEN THE FBI AND THE U.S.
SECRET SERVICE (USSS), USSS HAS PRIMARY JURISDICTION IN
COMPUTER CRIMES INVOLVING CREDIT REPORTING AGENCIES.

ON 6/17/92 [REDACTED] USSS,
WAS ADVISED OF THIS INVESTIGATION. [REDACTED] SUBSEQUENTLY ADVISED
USSS WOULD EXERCISE THE PROVISIONS OF THE MOU, TAKE OVER THE
INVESTIGATION, AND DID NOT DESIRE TO CONDUCT A JOINT
INVESTIGATION.

b6
b7C

BT

✓/READ 8567170
0000 MRI 00856

PF RUCNFB FBIAT FBINY FBISC FBISF FBISE

DE FBIWMFO #0028 1701529

ZNR UUUUU

P 181527Z JUN 92

FM FBI WMFO (264B-WF-NEW) C

TO DIRECTOR FBI/PRIORITY/

FBI ATLANTA/PRIORITY/

FBI NEW YORK/PRIORITY/

FBI SACRAMENTO/PRIORITY/

FBI SAN FRANCISCO/PRIORITY/

FBI SEATTLE/PRIORITY/

BT

UNCLAS

CITE: //3920//

SUBJECT: UNSUB; INTRUSIONS INTO COMPUTER SYSTEMS OF EQUIFAX,
INC., AT SACRAMENTO, CALIFORNIA, SEATTLE, WASHINGTON, AND NEW
YORK, NEW YORK; CFA; OO:WMFO.

RE WMFO TELETYPE TO BUREAU DATED 6/17/92, WMFO FAXS TO AT
AND SC ON 6/17/92, AND TELEPHONE CALLS FROM SSA
/BYE

b6
b7c

SEARCHED INDEXED
SERIALIZED *ms*

SEARCHED INDEXED
SERIALIZED FILED
[Handwritten signatures]

264B-WF-181147-2

Bob

⊗
bet

b6
b7c

[REDACTED] WMFO, AND SSA [REDACTED] SC, AND SSA [REDACTED] AT, ON

6/17/92.

ALL OFFICES DISCONTINUE INVESTIGATION.

BASED ON THE MEMORANDUM BETWEEN THE FBI AND THE U.S. SECRET SERVICE (USSS), USSS HAS PRIMARY JURISDICTION IN COMPUTER CRIMES INVOLVING CREDIT REPORTING AGENCIES.

ON 6/17/92, [REDACTED] USSS, WAS ADVISED OF THIS INVESTIGATION. [REDACTED] SUBSEQUENTLY ADVISED USSS WOULD EXERCISE THE PROVISIONS OF THE MOU, TAKE OVER THE INVESTIGATION, AND DID NOT DESIRE TO CONDUCT A JOINT INVESTIGATION.

BT

#0028

NNNN

b6
b7C

b6
b7C

C-14

FBI

TRANSMIT VIA:

- Teletype
- Facsimile
- AIRTEL

PRECEDENCE:

- Immediate
- Priority
- Routine

CLASSIFICATION:

- TOP SECRET
- SECRET
- ~~CONFIDENTIAL~~
- UNCLAS E F T O
- UNCLAS

Date 6/17/92

FM FBI WMFO (264B-WF-NEW)
 TO DIRECTOR FBI/PRIORITY/
 FBI ATLANTA/PRIORITY/
 FBI SACRAMENTO/PRIORITY/
 FBI SAN FRANCISCO/PRIORITY/
 FBI SEATTLE/PRIORITY/
 FBI NEW YORK/PRIORITY/

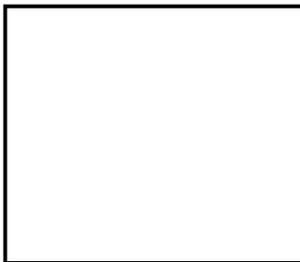
BT

UNCLAS

CITE: //3920//

PASS: FBIHQ ECU.

SUBJECT: UNSUB; INTRUSIONS INTO COMPUTER SYSTEMS OF EQUIFAX,
 INC., AT SACRAMENTO, CA., SEATTLE, WASHINGTON, AND NEW YORK,
 NEW YORK; CFA; OO:WMFO.



264B-WF-181147 -b6
 -b7c
 3
 SEARCHED _____ INDEXED _____
 SERIALIZED _____ FILED _____

264B-WF-181147

Approved: [Signature] Original filename: 324B-WF-167

Time Received: 1:55 pm Telprep filename: SMB00150.167

MRI/JULIAN DATE: 1068/169 ISN: 023

FOX DATE & TIME OF ACCEPTANCE: 17 JUNE 92 9:00 2:00 pm LAA

^PAGE 2 264B-WF-NEW UNCLAS

RE TELEPHONE CALLS TO SSA [REDACTED] AND SA [REDACTED]

b6
b7C

[REDACTED] SACRAMENTO, AND RELIEF SUPERVISOR [REDACTED] SF, ON
6/16/92.

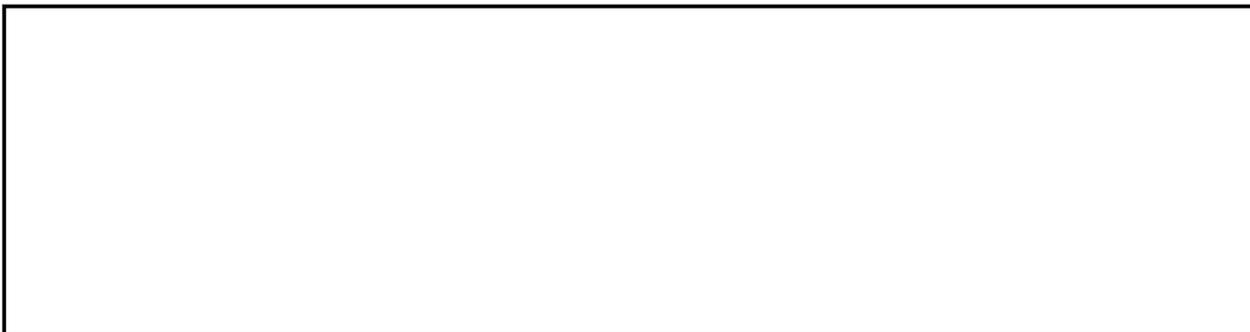
[REDACTED] EQUIFAX, INC., ATLANTA, GA., [REDACTED]

b6
b7C

[REDACTED] TELEPHONICALLY ADVISED WMFO ON 6/16/92, THAT EQUIFAX
IS BEING PENETRATED BY COMPUTER HACKERS USING A FOLEY
DEPARTMENT STORE ACCOUNT. FOLEY IS LOCATED IN HOUSTON, TEXAS.
PENETRATIONS ARE OCCURRING PRIMARILY IN SACRAMENTO, CA., AND
ALSO IN SEATTLE AND NEW YORK CITY.

EQUIFAX CONTACTED PACBELL AND REQUESTED TRAP AND TRACE.
PACBELL ADVISED EQUIFAX ON 6/16/92, THAT TRAP AND TRACE
INFORMATION COULD NOT BE FURNISHED TO EQUIFAX WITHOUT A COURT
ORDER.

b7E



^PAGE 3 264B-WF-NEW UNCLAS

SA [REDACTED] SC, ADVISED [REDACTED] PACBELL SECURITY, [REDACTED] IS WORKING ON THE EQUIFAX TRAP AND TRACE.

b6
b7C

THE EQUIFAX SACRAMENTO COMPUTER CENTER HAS NUMEROUS PORTS AND THE SUBJECTS ARE USING VARYING PORTS. [REDACTED] WILL FAX WMFO A COPY OF THE INCOMING TELEPHONE LINES BEING USED.

b6
b7C

THE COMPUTER CRIME SQUAD (C-17) AT WMFO HAS AGENTS WHO HAVE BEEN COMMERCIALY TRAINED IN [REDACTED] [REDACTED] THESE AGENTS ALSO HAVE PRACTICAL EXPERIENCE IN TELECOMMUNICATIONS.

b7E

WMFO MAY REQUEST OF AT, SC, AND SF APPROVAL FOR SA [REDACTED] [REDACTED] TO TRAVEL TO THESE DIVISIONS TO CONDUCT THE INVESTIGATION WITH A REPRESENTATIVE OF THE RESPECTIVE DIVISION. A SUBPOENA AND TRIP AND TRACE ORDER WILL BE REQUIRED.

b6
b7C

IT IS EXPECTED THE COMPUTER HACKERS ARE NOT LOCATED IN CALIFORNIA, BUT FROM OTHER AREAS OF THE COUNTRY OR INTERNATIONAL. THEREFORE, [REDACTED] COMPUTER CRIMES UNIT, DOJ, HAS BEEN BRIEFED ON THE INVESTIGATION AND WILL BE COORDINATING THE VARIOUS USA OFFICES.

b6
b7C

^PAGE 4 264B-WF-NEW UNCLAS

ANY QUESTIONS MAY BE DIRECTED TO SSA



WMFO, EXTENSION 9164, 6364.

BT

b6
b7c

REFAD 1068/169
0000 MRI 01068

PP RUCNFB FBIAT FBISC FBISF FBISE FBINY

DE FBIWMFO #0023 1691802

ZNR UUUUU

P 171800Z JUN 92

FM FBI WMFO (264B-WF-NEW)

TO DIRECTOR FBI/PRIORITY/

FBI ATLANTA/PRIORITY/

FBI SACRAMENTO/PRIORITY/

FBI SAN FRANCISCO/PRIORITY/

FBI SEATTLE/PRIORITY/

FBI NEW YORK/PRIORITY/

BT

UNCLAS

CITE: //3920//

PASS: FBIHQ ECU.

SUBJECT: UNSUB; INTRUSIONS INTO COMPUTER SYSTEMS OF EQUIFAX,
INC., AT SACRAMENTO, CA., SEATTLE, WASHINGTON, AND NEW YORK,
NEW YORK; CFA; OO:WMFO.

RE TELEPHONE CALLS TO SSA AND SA

b6
b7c

264 B-WF-181147-
SEARCHED _____ INDEXED _____
SERIALIZED ms FILED ms 3

PAGE TWO DE FBIWMFO 0023 UNCLAS

[REDACTED] SACRAMENTO, AND RELIEF SUPERVISOR [REDACTED] SF, ON
6/16/92.

b6
b7C

[REDACTED] EQUIFAX, INC., ATLANTA, GA., [REDACTED]
[REDACTED] TELEPHONICALLY ADVISED WMFO ON 6/16/92, THAT EQUIFAX
IS BEING PENETRATED BY COMPUTER HACKERS USING A FOLEY
DEPARTMENT STORE ACCOUNT. FOLEY IS LOCATED IN HOUSTON, TEXAS.
PENETRATIONS ARE OCCURRING PRIMARILY IN SACRAMENTO, CA., AND
ALSO IN SEATTLE AND NEW YORK CITY.

b6
b7C

EQUIFAX CONTACTED PACBELL AND REQUESTED TRAP AND TRACE.
PACBELL ADVISED EQUIFAX ON 6/16/92, THAT TRAP AND TRACE
INFORMATION COULD NOT BE FURNISHED TO EQUIFAX WITHOUT A COURT
ORDER.

b7E



SA [REDACTED] SC, ADVISED [REDACTED] PACBELL
SECURITY, [REDACTED] IS WORKING ON THE EQUIFAX TRAP AND
TRACE.

b6
b7C

THE EQUIFAX SACRAMENTO COMPUTER CENTER HAS NUMEROUS PORTS

PAGE THREE DE FBTWME-~~XXXXXXXXXX~~

AND THE SUBJECTS ARE USING VARYING PORTS. [REDACTED] WILL FAX WMFO
A COPY OF THE INCOMING TELEPHONE LINES BEING USED.

b6
b7C

THE COMPUTER CRIME SQUAD (C-17) AT WMFO HAS AGENTS WHO
HAVE BEEN COMMERCIALY TRAINED IN [REDACTED]
[REDACTED] THESE AGENTS ALSO HAVE PRACTICAL
EXPERIENCE IN TELECOMMUNICATIONS.

b7E

WMFO MAY REQUEST OF AT, SC, AND SF APPROVAL FOR SA [REDACTED]
[REDACTED] TO TRAVEL TO THESE DIVISIONS TO CONDUCT THE
INVESTIGATION WITH A REPRESENTATIVE OF THE RESPECTIVE
DIVISION. A SUBPOENA AND TRIP AND TRACE ORDER WILL BE
REQUIRED.

b6
b7C

IT IS EXPECTED THE COMPUTER HACKERS ARE NOT LOCATED IN
CALIFORNIA, BUT FROM OTHER AREAS OF THE COUNTRY OR
INTERNATIONAL. THEREFORE, [REDACTED] COMPUTER
CRIMES UNIT, DOJ, HAS BEEN BRIEFED ON THE INVESTIGATION AND
WILL BE COORDINATING THE VARIOUS USA OFFICES.

b6
b7C

ANY QUESTIONS MAY BE DIRECTED TO SSA [REDACTED]
WMFO, EXTENSION 9164, 6364.

b6
b7C

BT

#0023

NNNN

AIRTEL

To : Director, FBI
(Attn: Economic Crimes Unit
White-Collar Crimes Section
Criminal Investigative Division)

From : SAC, WMFO (264B-WF-181147) (C)

TITLE : UNSUB(s);
INTRUSION INTO COMPUTER SYSTEMS OF EQUIFAX.,
at SACRAMENTO, CA, SEATTLE, WA and NEW YORK,
YORK - Victim;
COMPUTER FRAUD AND ABUSE
OO:WMFO

REFERENCE: WMFO teletypes to the Director, dated 6/17/92 and 6/18/92

Check Box

Enclosed are the original and five copies of a LHM for dissemination.

Check one

Submission: Initial Supplemental

6/18/92 Date case opened (if applicable)

6/17/92 Date of complaint

6/9/92 Date of first known offense/intrusion

Unknown - Estimated number of computer users affected.

\$ Unknown - Estimated loss to date.

Unknown Brand and series model of computer.
(ie: IBM, DEC, Apple, etc.)

Unknown Operating system and version.

3 - Bureau
(1 - ECU, WCCS, CID)
(1 - CI-4D, INTD)

② - Field Office
BEB:beb
(5)

264B-WF-181147-4
~~SEARCHED~~ ~~SERIALIZED~~ ~~INDEXED~~

FBI/DOJ

Fill in below with Yes (Y), No (N), or Unknown (U):

- N Is a federal government computer affected?
Department/Agency: _____
- Y Is a federal interest computer affected?
Victim institution: FOLEY DEPARTMENT STORES, Houston, TX
- Y Does the offense involve a telecommunications network?
- U Is (former) employee suspected?
- U Is the method of intrusion known?
- Y Is the system still vulnerable?
- Y Is the intrusion continuing?

National Security Issues:

- N Does agency/institution computers contain classified information?
- N Was classified information compromised in this matter?
- N Is a foreign or hostile intelligence service involved?

Check Type Of Crime(s):

IMPAIRMENT (264-A)

- Virus Planted
- Malicious Software Planted
- Interruption of Service/Prevent use
- Destruction of Information or Software
- Modification of Information or Software

THEFT OF INFORMATION (264-B)

- Data
- Passwords
- Computer Processing Time
- Telephone Services
- Application Software
- Operating System Software

INTRUSION (264-C)

- Unauthorized Access
- Exceeding Authorized Access

Check Action Taken:

- Case Opened/Reopened/Incorporated into Pending Matter
- No Action Due to State/Local Prosecution
- USA Declination
- Facts Known do not meet Prosecutive Guidelines
- Matter Referred to Another Federal Agency (U.S. Secret Service)
- Investigation Delayed Due to Lack of Resources
- Other: _____

Administrative: Investigation was opened and subsequently it was discovered that investigation falls within the jurisdiction of the USSS. The FBI discontinued and referred to USSS. Prior to discontinuance, FBI at Sacramento

b7E

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to
File No. 264B-WF-181147

Washington D. C. 20535

June 26, 1992

UNSUB
INTRUSION INTO COMPUTER
SYSTEMS OF EQUIFAX, INC.,
AT SACRAMENTO, CALIFORNIA,
SEATTLE, WASHINGTON AND
NEW YORK, NEW YORK
COMPUTER FRAUD AND ABUSE

On June 16, 1992, captioned investigation was predicated upon receipt of information from [redacted] Equifax, Inc., Atlanta, Georgia, indicating that computer systems operated by Equifax had been and were currently being penetrated by unknown system intruders utilizing a Foley Department Store access code. The headquarters for Foley Department Stores is located in Houston, Texas but the system intrusions occurred primarily in Sacramento, California, Seattle, Washington and New York, New York.

b6
b7C

On June 16, 1992, the known facts of this investigation were presented to [redacted] Computer Crimes Unit, Department of Justice, who advised that he would coordinate the prosecution of this investigation through the various offices of the United States Attorney.

b6
b7C

On June 17, 1992, captioned investigation was discontinued following a review of the Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS) which revealed that the USSS maintains primary jurisdiction in computer crimes involving credit reporting agencies. Because Equifax is considered a credit reporting agency, [redacted] Electronic Crimes Branch, USSS, was apprised of the facts of the investigation. [redacted] subsequently advised that the USSS would exercise the provisions of the MOU by taking over the investigation. Additionally, [redacted] stated the USSS did not desire to conduct a joint investigation with the FBI.

b6
b7C

5-Bureau
②-WMFO (264B-WF-181147)
BEB:beb
(7)

Memorandum



To : SAC, WMFO [redacted] (P)

Date 10/2/92

b7E

From

Best [redacted]

b6
b7C

Subject:

[redacted]

CFA
OO:PD

Since the middle of July, 1992, the writer has been involved with captioned matter on a virtual full-time basis. The writer's involvement has primarily consisted of [redacted]

b7E

[redacted]

As

such the writer has been unavailable to address the following cases:

[redacted]

b7E

264C-WF-181147

[redacted]

1 - [redacted]

① - 264B-WF-181147

BEB: bh

(9)

264B-WF-181147-5

b7E

SEARCHED *hw* INDEXED *hw*
SERIALIZED *hw* FILED *hw*

OCT 1992

FBI - WASH. FIELD OFFICE

[Signature]

Memorandum



To : SAC, WMFO (264B-WF-181147) (P)

Date 10/2/92

From : SA [Redacted]

b6
b7C

Subject: UNSUB(S);
INTRUSION INTO COMPUTER SYSTEMS OF EQUIFAX,
at Sacramento, CA, Seattle, WA and New York, NY;
CFA
OO:WMFO

A review of captioned matter for file review revealed that captioned matter is a closed investigation as indicated on serial #4. However, the current status is pending. It is recommended that captioned matter be closed insofar as the investigation has been referred to the United States Secret Service (USSS) which maintains jurisdiction over such matters.

Close
MA
10/6/92
10/2/92

① - 264B-WF-181147
BEB:bh
(1)

264B-WF-181147-6

SEARCHED	INDEXED
SERIALIZED	FILED
OCT 1992	
FBI - WASH. FIELD OFFICE	

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 11/28/2007

To: Atlanta
Cyber

Attn: Computer Intrusion Section (CI)

From: Atlanta
Squad C-9
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

rsm

Case ID #: 102883-1
288A-AT-NEW

[redacted]

(P.1)
b3
b7E

Title: UNSUB(S);
EQUIFAX - VICTIM;
PHISHING E-MAIL

Synopsis: To recommend opening a new phishing e-mail case based on the information provided below.

Details: On 10/29/2007, [redacted]

b6
b7C
b7E

[redacted] Equifax, Inc. 1525 Windward Concourse, Alpharetta, Georgia, reported that they were currently a victim of a phishing attack possibly part of the Rock Phish Group. Equifax noticed that started receiving 100,000 bounce backs per hour to their e-mail servers. These bounce backs were from phishing e-mails that were attempted to be sent to Equifax costumers [redacted]

b7E

b6
b7C

OVA
SA [redacted]
JBT
11/29/07

To: Atlanta From: Atlanta
Re: 288A-AT-NEW, 11/28/2007

[Redacted]

b7E

Equifax is in the process of identifying if any [Redacted] consumer accounts have been accessed due to the phishing e-mails.

b7E

Special Agent (SA) [Redacted] recommends that a case be opened based on the information provided by Equifax. Even though Equifax and its customers have not yet suffer any loss to date.

b6
b7C
b7E

[Redacted]

◆◆

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/11/2007

To: Atlanta

From: Atlanta

I-2

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

sh

Case ID #: [redacted] (Pending)

288A-AT-102883 - (Pending)

Title: [redacted]

UNSUB(S);
EQUIFAX - VICTIM
COMPUTER INTRUSION - PHISHING

Synopsis: To claim statistical accomplishment [redacted] assistance.

Details: On October 29, 2007, [redacted]

[redacted] Equifax, reported that Equifax was currently a victim of a phishing attack which was possibly part of the Rock Phish Group. Equifax noticed that they started receiving 100,000 bounce backs per hour to their email servers. These bounce backs were from phishing emails that were attempted to be sent to Equifax customers [redacted]

[redacted]

[redacted]

Equifax is in the process of identifying if any [redacted] customer accounts have been accessed due to the phishing emails.

b6
b7C
b6
b7C
b7E
b7E

b7E
b6
b7C
b7E

b7E

b7E

0BT
12/14/07

To: Atlanta From: Atlanta
Re: [redacted] 12/11/2007

b7E

Accomplishment Information:

Number: [redacted]
Type: [redacted]
ITU: [redacted]
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: 12

b6
b7C
b7E

◆◆

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/29/2007

[redacted]
[redacted] Equifax, Inc., 1525 Windward Concourse,
Alpharetta, Georgia, cellular telephone number [redacted] work
telephone number [redacted] provided the following information:

b6
b7C

b6
b7C
b7E

~~(S)~~
~~(P)~~

[Large redacted area]

Investigation on 10/30/2007 at Atlanta, Georgia

File # 288A-AT-102883, [redacted] Date dictated N/A

by SA [redacted]

b3
b7E
b6
b7C

102883-



103007.302

b6
b7c

~~102883~~

BT
1/23/08

4
5

288A-AT-102883,

[Redacted]

b3
b7E

Continuation of FD-302 of

[Redacted]

, On 10/30/2007, Page 2

b6
b7C



b6
b7C
b7E

A copy of the spreadsheet provided by [Redacted] is included in the 1A section of the case file.

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/29/2007

[redacted]
[redacted] Equifax, Inc., 1525 Windward Concourse,
Alpharetta, Georgia, cellular telephone number [redacted] work
telephone number [redacted] provided the following information:

b6
b7C

[redacted]

b6
b7C
b7E

⊗
Ⓚ

Investigation on 11/08/2007 at Atlanta, Georgia

File # 288A-AT-102883, [redacted]

Date dictated N/A

by SA [redacted]

b3
b7E

b6
b7C

102883--110807.302

b6
b7c

JBT
1/23/00

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/04/2007

[redacted]
[redacted] Equifax, Inc., 1525 Windward Concourse,
Alpharetta, Georgia, cellular telephone number [redacted] work
telephone number [redacted] was interviewed at her place of
employment. After being advised of the identity of the
interviewing Agent and the nature of the interview, [redacted] provided
the following information:

b6
b7C

[redacted] advised that Equifax was seeing two weeks of the
phishing activity and then it stopped. There have been a total of
four days in a row of no activity. Equifax has not had any
undeliverable e-mails bouncing back to their e-mail servers.
Equifax has identified a total of three hundred thirty nine
phishing websites.

(X) b6
(R) b7C

[redacted] explained that Equifax has [redacted]
[redacted]

b6
b7C
b7E

[redacted]

b7E

Equifax has been able to narrow the records down from
three million to one hundred and forty eight. There have been
several hundred unsuccessful login attempts. Approximately forty
banks and/or credit unions have admitted to falling for the
phishing scam. Equifax has had no response from there small
consumers, such as car dealerships. Equifax will continue to look
over the historical IP data before and after the attack.

Investigation on 11/15/2007 at Alpharetta, Georgia

File # 288A-AT-102883,⁵ [redacted]

Date dictated N/A

by SA [redacted]
SA [redacted]

b3
b7E
b6
b7C

102883



111507.302

b6
b7c

YBT
1/23/08

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/29/2007

[redacted]
[redacted] Equifax, Inc., 1525 Windward Concourse,
Alpharetta, Georgia, cellular telephone number [redacted] work
telephone number [redacted] provided the following information:

b6
b7C

Approximately thirty to forty banks and credit unions
that are customers of Equifax have admitted to providing credential
information to the phishing e-mails. Equifax has not seen any
unauthorized access to these accounts to date. [redacted]

⊗
ⓑ b7E

[Large redacted area]

Investigation on 11/08/2007 at Atlanta, Georgia

File # 288A-AT-1028837 [redacted] Date dictated N/A

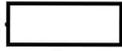
by SA [redacted]

b3
b7E

b6
b7C

102883

102883



110807-1.302 b6
b7c

JBT 1/23/08

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/04/2008

[redacted]
[redacted] Equifax, Inc., 1525 Windward Concourse,
Alpharetta, Georgia, cellular telephone number [redacted] work
telephone number [redacted] provided the following information:

b6
b7C

Several Equifax customers had exposed their credentials during the most recent Rock Phish Attack. Equifax found that all of the exposed credentials were used on 01/31/2008 from the unique IP addresses listed below:

[redacted]

⊗
R b6
b7C
b7E

Fortunately, Equifax currently [redacted]

b7E

[redacted] Customers would have also gotten an error code with an 800 telephone number to call. Equifax is attempting to retrieve any call logs around the same time that the attempts occurred. There were also some IP addresses in [redacted] that were used to access accounts.

Rjc

Investigation on 02/01/2008 at Atlanta, Georgia

File # 288A-AT-102883, [redacted] Date dictated N/A

by SA [redacted]

b3
b7E

b6
b7C

102883 020108.302

b6
b7c

4
2



UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/27/2009

To: Atlanta

From: Atlanta

Squad C-9

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

rsm *RS*

Case ID #: 288A-AT-102883 (Closed) - *8*

Title: UNSUB(S);
EQUIFAX - VICTIM;
PHISHING E-MAIL

Synopsis: To recommend closing case based on now new criminal activity.

Details: On 10/29/2007, [redacted]

[redacted] Equifax, Inc. 1525 Windward Concourse, Alpharetta, Georgia, reported that they were currently a victim of a phishing attack possibly part of the Rock Phish Group. Equifax noticed that started receiving 100,000 bounce backs per hour to their e-mail servers. These bounce backs were from phishing e-mails that were attempted to be sent to Equifax costumers [redacted]

b6
b7C
b6
b7C

X
RS

b6
b7C
b7E

b7E

UNCLASSIFIED

102883 - CLOSE. EC

C-4

JB
5/27/09

UNCLASSIFIED

To: Atlanta From: Atlanta
Re: 288A-AT-102883, 05/27/2009

[Redacted]

b7E

Several Equifax customers had exposed their credentials during the most recent Rock Phish Attack. Equifax found that all of the exposed credentials were used on 01/31/2008 unique IP addresses. Fortunately, Equifax currently [Redacted]

b7E

[Redacted]

There has been no activity attempted against Equifax by Rock Phish in the past couple of months and therefore, no intelligence has been gathered.

There is no pending evidence and no pending leads on this case.

In view of above, SA [Redacted] request that the case be closed.

b6
b7C

◆◆

UNCLASSIFIED