

(Overall Document Classification Required)

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication**

Title: (U) 2/15/2011 MEETING WITH [REDACTED]

Date: 09/21/2020

Drafted By: Missing

Case ID #: 288A-HO-NEW

(U) [REDACTED]

[REDACTED] COMPUTER

INTRUSION MATTERS

Details: 2/28/2011 On February 15, 2011, [REDACTED]

[REDACTED] cell phone  
number [REDACTED] telephone  
number [REDACTED] met with Special Agent [REDACTED] (SA  
[REDACTED] and Special Agent [REDACTED] (SA [REDACTED] offices,

[REDACTED] on the Internet and discovered  
that he was a part of the hacking group "Team Poison." Team Poison is  
known to deface government websites and is affiliated with hacking  
into user accounts. Team Poison likes to communicate on IRC through

(Overall Document Classification Required)

b6  
b7C  
b7Db6  
b7C  
b7Db3  
b6  
b7C  
b7D  
b7E

(Overall Document Classification Required)

Title: (U) 2/15/2011 MEETING WITH [REDACTED]

b7D

Re: 288A-HO-NEW, 09/21/2020

the Freenode network. [REDACTED]



b3  
b6  
b7C  
b7D  
b7E

(Overall Document Classification Required)

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1475926-000

Total Deleted Page(s) = 1  
Page 6 ~ b6; b7C; b7D; b7E;

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

(Overall Document Classification Required)

# FEDERAL BUREAU OF INVESTIGATION

## Electronic Communication

Title: (U) INTERVIEW OF [REDACTED]

Date: 09/21/2020

b6  
b7C  
b7D

Drafted By: Missing

Case ID #: 288A-HO-NEW

(U) [REDACTED]

[REDACTED] COMPUTER  
INTRUSION MATTERS

Details: 03/08/2011 On March 3, 2011, [REDACTED]

[REDACTED] date of birth [REDACTED]

[REDACTED]  
[REDACTED]  
was interviewed by Special Agents [REDACTED]

b6  
b7C  
b7D

[REDACTED]  
[REDACTED] provided the following information during the

b6  
b7C  
b7D

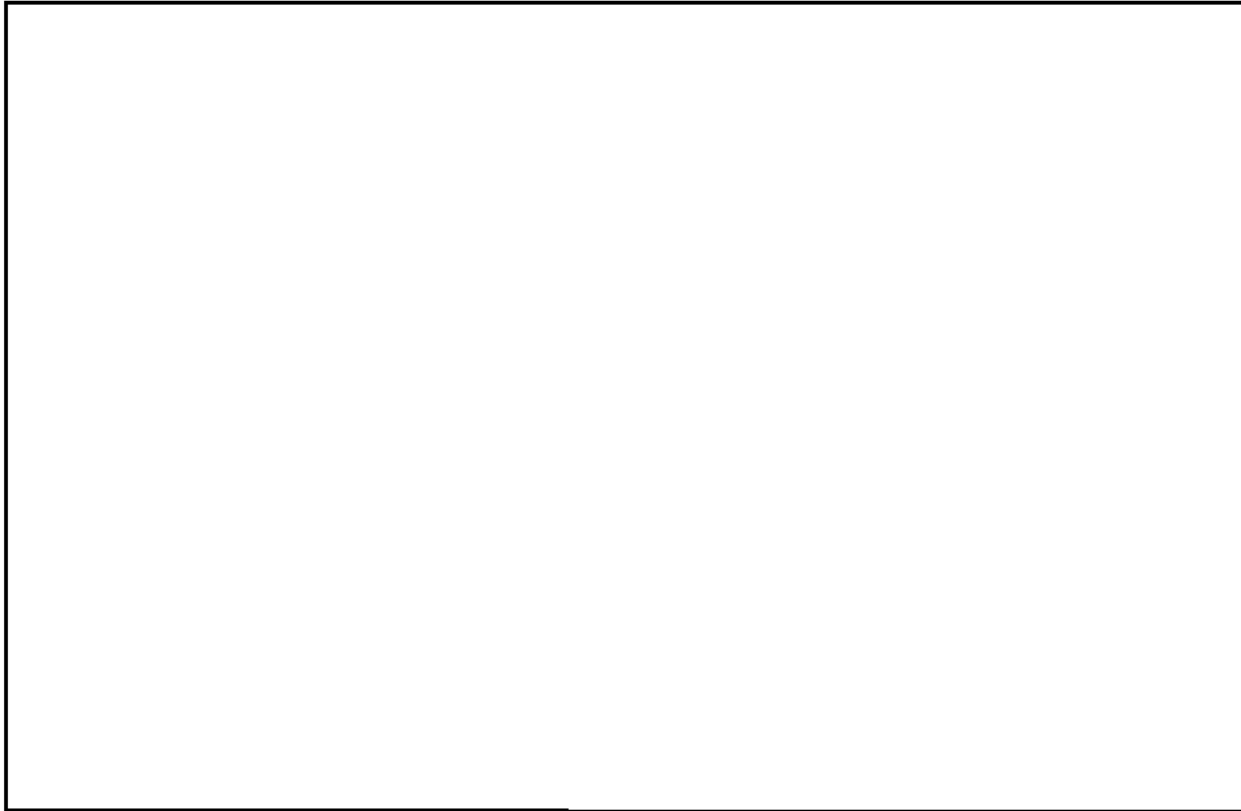
(Overall Document Classification Required)

(Overall Document Classification Required)

Title: (U) INTERVIEW OF [REDACTED]

Re: 288A-HO-NEW, 09/21/2020

b6  
b7C  
b7D



b6  
b7C  
b7D  
b7E

[REDACTED] executed exploits with "Team Poison" a well-known hacking group. Team Poison was also known for defacing websites. [REDACTED]



b6  
b7C  
b7D  
b7E

(Overall Document Classification Required)

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1422660-000

Total Deleted Page(s) = 21

Page 14 ~ b6; b7C; b7E;  
Page 15 ~ b6; b7C; b7E;  
Page 84 ~ b6; b7C; b7D; b7E;  
Page 85 ~ b6; b7C; b7D; b7E;  
Page 86 ~ b6; b7C; b7D;  
Page 87 ~ b6; b7C; b7D;  
Page 88 ~ b6; b7C; b7D;  
Page 89 ~ b6; b7C; b7D;  
Page 90 ~ b6; b7C; b7D;  
Page 91 ~ b6; b7C; b7D;  
Page 92 ~ b6; b7C; b7D;  
Page 106 ~ b6; b7C; b7D; b7E;  
Page 107 ~ b4; b6; b7C; b7D; b7E;  
Page 108 ~ b4; b6; b7C; b7D; b7E;  
Page 110 ~ b6; b7C; b7D;  
Page 113 ~ b6; b7C; b7D; b7E;  
Page 114 ~ b6; b7C; b7D; b7E;  
Page 115 ~ b6; b7C; b7D; b7E;  
Page 116 ~ b6; b7C; b7D; b7E;  
Page 117 ~ b6; b7C; b7D; b7E;  
Page 118 ~ b6; b7C; b7D; b7E;

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

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 12/02/2011

To: Cyber

Attn: SSA [REDACTED]

b6  
b7C

New York

Attn: SSA [REDACTED]

CCU-1

ID-24

From: New York

CY-2

Contact: SA [REDACTED]

b6  
b7C  
b7E

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-NY-~~NEW~~ (Pending)

Title: TEAMPOISON

VICTIM - FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION  
OO:NY

**Synopsis:** Request case opening and notification to Cyber substantive desk at FBIHQ.

**Details:** On November 28, 2011, New York Office, Squad ID-24 notified Squad CY-2 of [REDACTED] that indicated a SQLi vulnerability at THE FIRST NATIONAL BANK OF LONG ISLAND (FNBLI).

b7E

According to open source information FNBLI has become a target of #OpRobinHood. #OpRobinHood is a joint venture between hacker groups "TeaMp0ison" and Anonymous to "take on the banks, steal money and donate it to charities and protests."

On November 28, 2011, writer contacted [REDACTED]

b6  
b7C

[REDACTED] FNBLI, and advised him of the SQLi vulnerability and the possible intrusion into their computer network. Subsequent to the initial contact, [REDACTED] contacted writer and confirmed there was a SQLi attempt on one of FNBLI.COM's web servers. FNBLI and their service provider FISERV confirmed attacker IP address [REDACTED] made numerous attempts to gain access to FNBLI's server beginning on November 28, 2011, at 11:01 AM EDT. A WHOIS

UNCLASSIFIED

307369

b6  
b7C  
b7E

OPEN (OR REOPEN) CASE  
SEARCHED [REDACTED] INDEXED [REDACTED]  
SERIALIZED [REDACTED] FILED [REDACTED]  
DEC 11 2011  
FBI NEW YORK  
FI EFFECTIVE [REDACTED]

UNCLASSIFIED

To: Cyber From: New York  
Re: 288A-NY-NEW, 12/02/2011

lookup revealed that IP [redacted] resolves to KABEL  
DEUTSCHLAND.

b6  
b7C  
b7E

FNBLI corporate headquarters is located at 10 Glen Head  
Road, Glen Head, New York, 11545.

Writer contacted United States Attorney [redacted]  
Southern District of New York (SDNY), who was advised of the  
above and was assigned this matter. Captioned case subjects  
could be prosecuted for Title 18 U.S.C. 1030, Unauthorized  
Access, if the above information could be further corroborated.  
It is requested this matter be opened and assigned to SA [redacted]  
[redacted] and assign SA [redacted] as co-case.

b6  
b7C

UNCLASSIFIED



UNCLASSIFIED

To: Cyber From: New York  
Re: 288A-NY-NEW, 12/02/2011

LEAD(s):

Set Lead 1: (Info)

CYBER

AT WASHINGTON, D.C.

Read and clear.

Set Lead 2: (Info)

NEW YORK

AT NEW YORK, NY

Read and clear.

♦♦

UNCLASSIFIED



File Number 289A-NY-307369 - 1A1Field Office Acquiring Evidence NYSerial # of Originating Document 11Date Received 11/29/11 - 12/13/2011From FNBLI  
(Name of Contributor/Interviewee)

(Address)

(City and State)

By SA To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoReference: EC  
(Communication Enclosing Material)Description: ☒ Original notes re interview of1) CD-ROM containing images from   
 images, & web logs from FNBLI.b6  
b7Cb6  
b7C  
b7E

LH120211-WPD

12/5/2011

--

b6  
b7C

2



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No. 288A-NY-307369

New York, NY  
December 2, 2011

UNSUB(S); VICTIM - THE FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION

The New York Office of the Federal Bureau of Investigation (FBI) is investigating a possible computer intrusion into the computer network of a financial institution. The subject of the investigation is using a SQL injection to attempt to gain unauthorized access to the financial institution server.

Investigation was initiated by [REDACTED]

b7E

[REDACTED] which indicated a SQL vulnerability at THE FIRST NATIONAL BANK OF LONG ISLAND (FNBLI). According to open source information FNBLI has become a target of #OpRobinHood. #OpRobinHood is a joint venture between hacker groups "TeaMp0ison" and Anonymous to "take on the banks, steal money and donate it to charities and protests." TeaMp0ison, in a announcement on Pastebin.com, claimed responsibility for targeting FNBLI and for revealing the FNBLI's server vulnerability.

On November 28, 2011, the FBI contacted FNBLI who confirmed there was a SQLi attempt on one of FNBLI.COM's servers. FNBLI and their service provider confirmed, by viewing the web traffic logs, attacker IP address [REDACTED] made numerous attempts to gain access to FNBLI's server beginning on November 28, 2011, at 11:01 AM EDT. A WHOIS lookup revealed that IP [REDACTED] resolves to Internet Service Provider KABEL DEUTSCHLAND.

b6  
b7C  
b7E

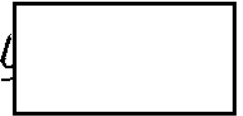
The FBI requests assistance from [REDACTED]

b7D  
b7E

updated LHM to Germany

LH120711.WPD

12/12/04



b6  
b7c



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No. 288A-NY-307369

New York, NY  
December 7, 2011

UNSUB(S); VICTIM - THE FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION

The New York Office of the Federal Bureau of Investigation (FBI) is investigating a possible computer intrusion into the computer network of a financial institution. The subject of the investigation is using a SQL injection to attempt to gain unauthorized access to the financial institution server.

Investigation was initiated by [REDACTED] which indicated a SQL vulnerability at THE FIRST NATIONAL BANK OF LONG ISLAND (FNBLI). According to open source information FNBLI has become a target of #OpRobinHood. #OpRobinHood is a joint venture between hacker groups "TeaMp0ison" and Anonymous to "take on the banks, steal money and donate it to charities and protests." TeaMp0ison, in a announcement on Pastebin.com, claimed responsibility for targeting FNBLI and for revealing the FNBLI's server vulnerability.

b7E

On November 28, 2011, the FBI contacted FNBLI who confirmed there was a SQLi attempt on one of FNBLI.COM's servers. FNBLI and their service provider confirmed, by viewing the web traffic logs, attacker IP address [REDACTED] made numerous attempts to gain access to FNBLI's server beginning on November 28, 2011, at 11:01 AM EDT. A WHOIS lookup revealed that IP [REDACTED] resolves to Internet Service Provider KABEL DEUTSCHLAND.

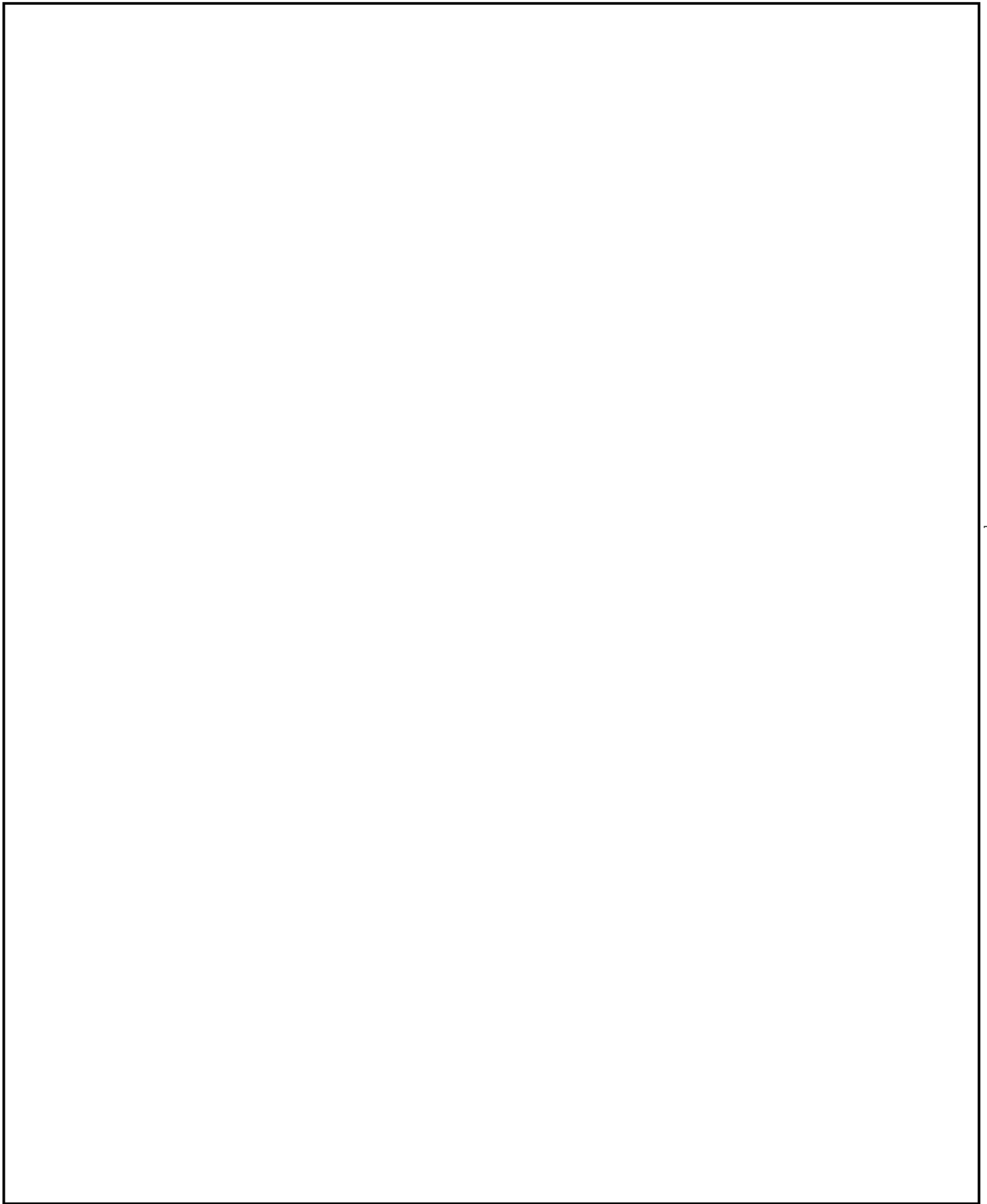
b6  
b7C  
b7E

The FBI requests assistance from [REDACTED]

b7D  
b7E

Attached to this letter are a copy of the #OpRobinHood statement made by TeaMp0ison [REDACTED] a copy of a web intelligence log and a host log provided by the FNBLI.

b7E



b4  
b7E



b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E



b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

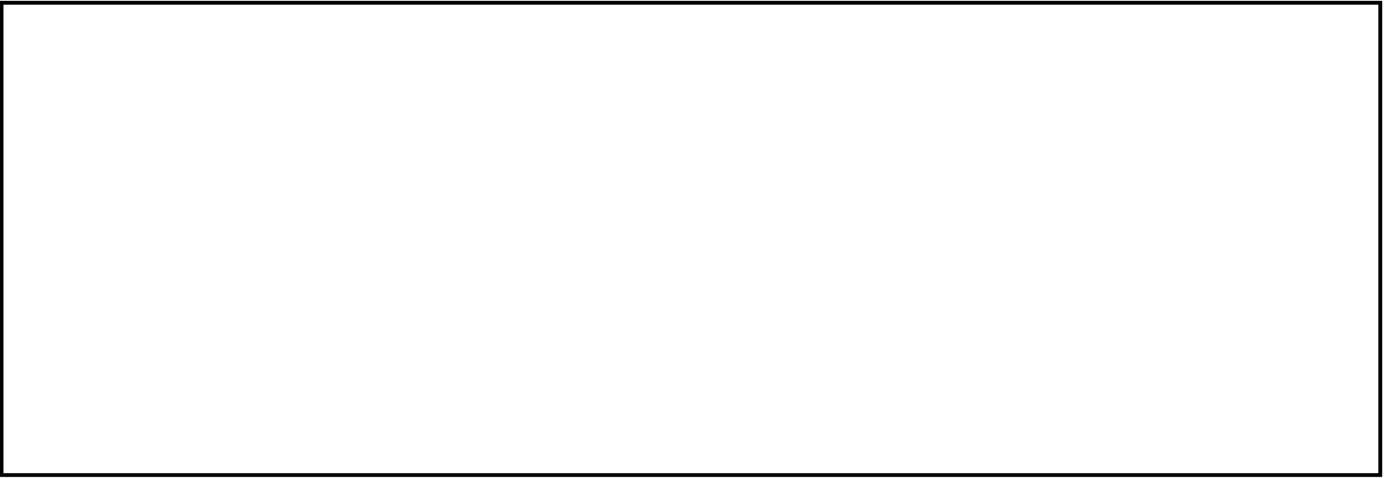
b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E





b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E



b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E



b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E



b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E



b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E

b4  
b7E



*U.S. Department of Justice*

**Federal Bureau of Investigation**

File No. 288A-NY-307369 -4  
Admin: 4HCD 7LCS.CY

Office of the Legal Attaché  
United States Consulate  
Frankfurt, Germany

9 December 2011


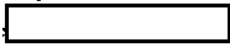

Re: #OpRobinHood/TeaMp0isoN and related German IP address



b6  
b7C  
b7D





Dear 

The New York Office of the Federal Bureau of Investigation (FBI) is investigating a possible computer intrusion into the computer network of a financial institution. The subject of the investigation used a SQL injection (SQLi) to attempt to gain unauthorized access to the financial institution server.

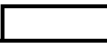

Investigation was initiated by  which indicated a SQL vulnerability at THE FIRST NATIONAL BANK OF LONG ISLAND (FNBLI). According to open source information, FNBLI has become a target of #OpRobinHood. #OpRobinHood is a joint venture between hacker groups "TeaMp0isoN" and Anonymous to "take on the banks, steal money and donate it to charities and protests." TeaMp0isoN,   claimed responsibility for targeting FNBLI and for revealing the FNBLI's server vulnerability.

b7E



b7E

On 28 November 2011, the FBI contacted FNBLI who confirmed there was a SQLi attempt on one of FNBLI.COM's servers. FNBLI and their service provider confirmed, by viewing the web traffic logs, attacker IP address  made numerous attempts to gain access to FNBLI's server beginning on November 28, 2011, at 11:01 AM EDT. On 29 November 2011, the FBI provided the above IP address to  FNBLI provided the FBI with a copy of a web intelligence log and a host log. On 9 December 2011, these logs were sent via email by SA  to .

b6  
b7C  
b7E

In addition, on 8 December 2011, ALAT  forwarded a copy of the #OpRobinHood statement made by TeaMp0isoN, .

b6  
b7C  
b7D  
b7E

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



The FBI requests assistance from [REDACTED]

[REDACTED] As always, thank you very much for your assistance. If  
you have any questions, then please contact ALAT [REDACTED]

b6  
b7C  
b7D  
b7E

[REDACTED]  
Legal Attaché

[REDACTED]  
Assistant Legal Attaché



b6  
b7C

919L I 1111. WPD

**FEDERAL BUREAU OF INVESTIGATION****Precedence:** ROUTINE**Date:** 01/18/2012**To:** New York**From:** New York

CY-2

**Contact:** SA [REDACTED]**Approved By:** [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** ✓ 288A-NY-307369 (Pending) - 5  
[REDACTED]**Title:** VICTIM NOTIFICATION FORM**Synopsis:** TEAMPOISON;  
VICTIM - FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION  
OO:NY**Reference:** 288A-NY-307369 Serial 1**Details:**

VnsCase#: 288A-NY-307369  
CAgtName: [REDACTED]  
PContact: Business  
BusName : FIRST NATIONAL BANK OF LONG ISLAND  
BuseIN : 000000000  
BusAcct : [REDACTED]  
VicFirN : [REDACTED]  
VicMidN : [REDACTED]  
VicLastN: [REDACTED]  
SSAN :  
VicDate : 20111128  
VicDOD :  
VicMinor:  
DOB :  
Race :  
Sex :  
Addr :  
Addr2 :  
City :  
State :  
Country :  
Zip :

b3  
b6  
b7C  
b7Eb6  
b7C  
b7Eb6  
b7C

To: New York From: New York  
Re: 288A-NY-307369, 01/18/2012

Email :  
HPhone :  
Fax :  
VWrkAddr: 18 Emerson Place  
VWrkadd2:  
VWrkCity: Valley Stream  
VWrkSt : NY  
VWrkCtry: US  
VWrkZip : 11580

WEmail :  
WPhone :  
WFax :

b7E

VicPager:  
NOKFirN :  
NOKMidN :  
NOKLastN:  
NOKRel :  
NOKAddr :  
NOKAddr2:  
NOKCity :  
NOKState:  
NOKCtry :  
NOKZip :  
NOKHEmal:  
NOKWEmal:  
NOKHPho :  
NOKWPho :  
NOKHFax :  
NOKWFax :  
NOKPager:  
GrdFirN :  
GrdMidN :  
GrdLastN:  
GrdRel :  
GrdAddr :  
GrdAddr2:  
GrdCity :  
GrdState:  
GrdCtry :  
GrdZip :  
GrdHEmal:  
GrdWEmal:  
GrdHPho :  
GrdWPho :  
GrdHFax :  
GrdWFax :  
GrdPager:  
PropRet : N  
TotLoss : 000000000

To: New York From: New York  
Re: 288A-NY-307369, 01/18/2012

Lang. :  
Disable :

♦♦

288A-NY-307369-6



b6  
b7c

b6  
b7c



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 02/21/2012

To: Cyber

International Operations  
New York

Attn: CCU-1

SSA [REDACTED]

Attn: Europe Unit

Attn: CY2

SSA [REDACTED]

SA [REDACTED]

b6  
b7C

From: Berlin

Frankfurt Sub-Office

Contact: ALAT [REDACTED]

b6  
b7C  
b7E

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-NY-307369 (Pending) -6

Title: TEAMPOISON;

VICTIM - FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION;  
OO:NY

Synopsis: To document investigation conducted by Legat Berlin.

Reference: 288A-NY-307369 Serial 3  
288A-NY-307369 Serial 4

Administrative: 4FBID

Enclosure(s): Enclosed for NYO is one (1) two-paged letter from [REDACTED] dated January 11, 2012.

b6  
b7C  
b7D  
b7E

Details: On November 29, 2012, FBI NYO requested Legat Berlin assistance in working with [REDACTED]

FBI NYO initiated the investigation after [REDACTED]

b7E

UNCLASSIFIED

b6  
b7C

4/9

4/5/2012

UNCLASSIFIED

To: Cyber From: Berlin  
Re: 288A-NY-307369 , 02/21/2012

[redacted] which indicated a SQL vulnerability at FNBLI. According to open source information, FNBLI had become a target of #OpRobinHood. #OpRobinHood is a joint venture between hacker groups "TeaMp0ison" and Anonymous to "take on the banks, steal money and donate it to charities and protests." TeaMp0ison, in an announcement on Pastebin.com, claimed responsibility for targeting FNBLI and for revealing the FNBLI's server vulnerability.

b7E

NYO contacted FNBLI and confirmed by viewing the web traffic logs that attacker IP address [redacted] made numerous attempts to gain access to FNBLI's server beginning on November 28, 2011, at 11:01 AM EDT.

b6  
b7C  
b7E

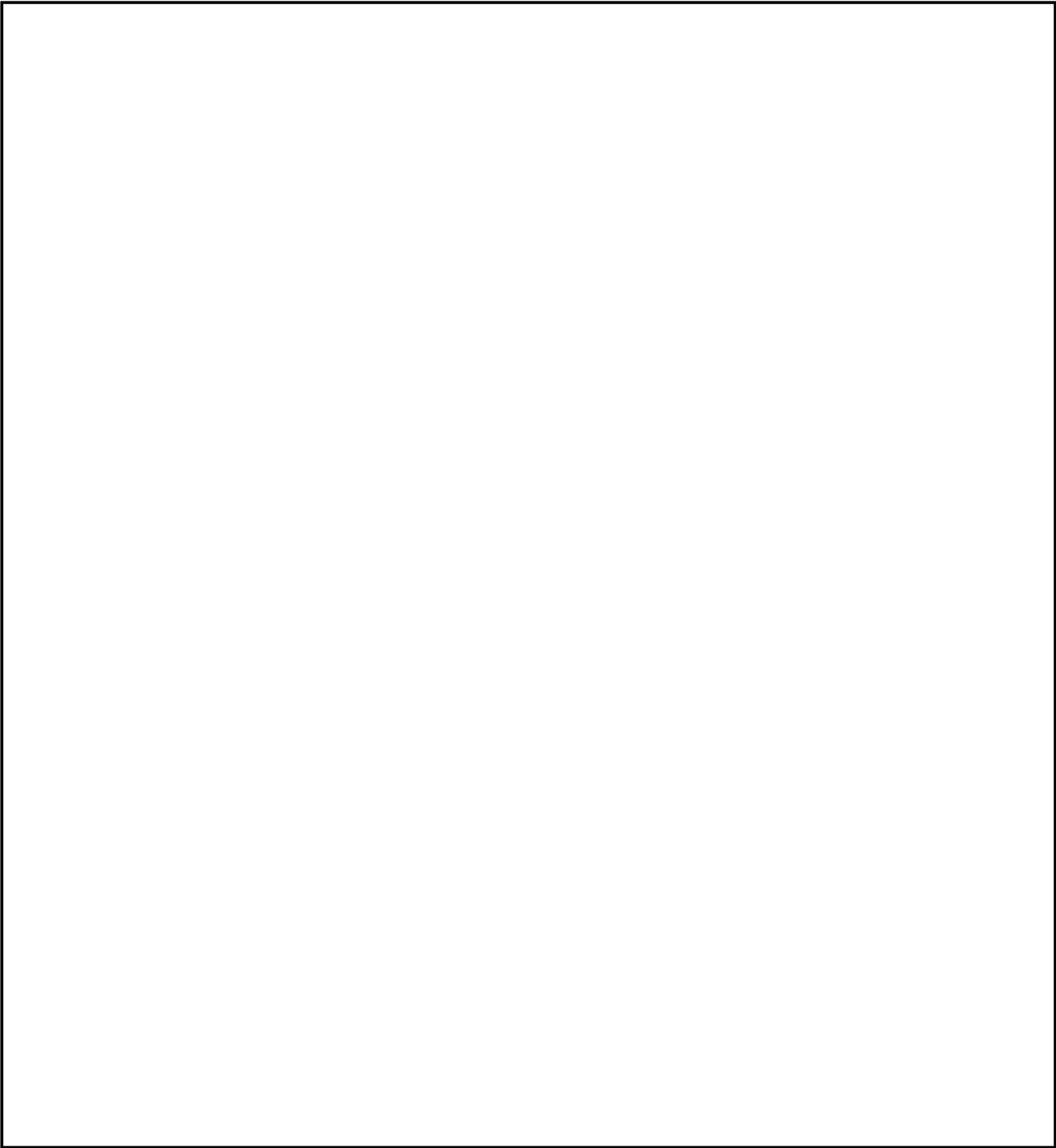
b6  
b7C  
b7D

UNCLASSIFIED



UNCLASSIFIED

To: Cyber From: Berlin  
Re: 288A-NY-307369 , 02/21/2012

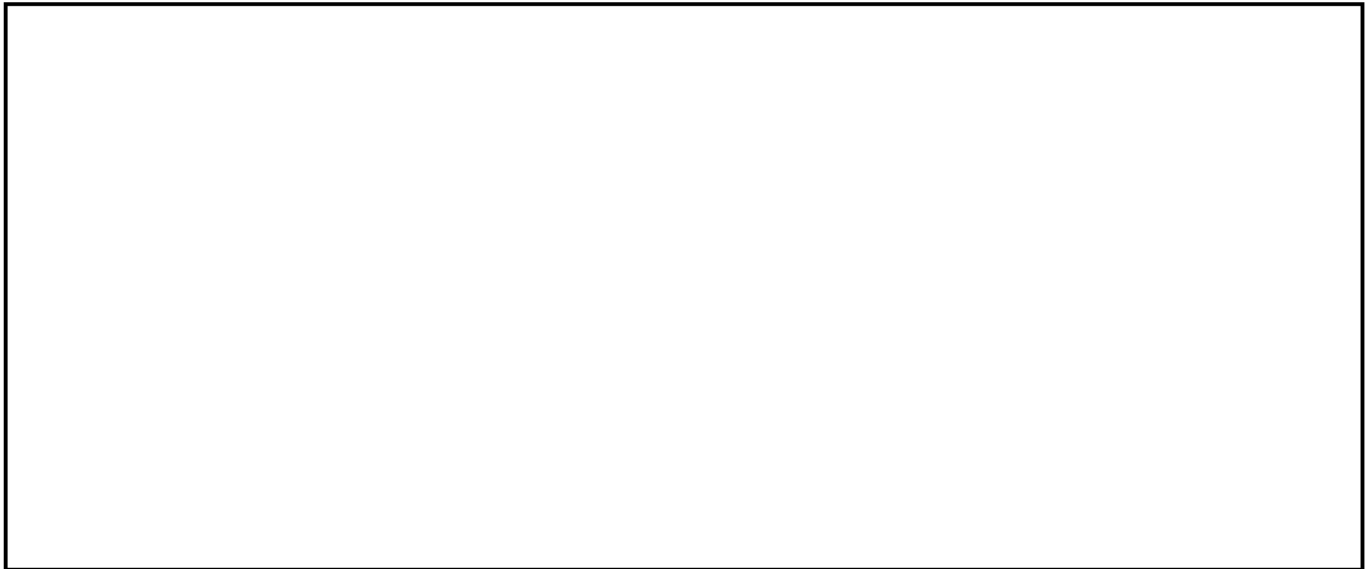


b6  
b7C  
b7D

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Berlin  
Re: 288A-NY-307369 , 02/21/2012



b6  
b7C  
b7D

Legat Berlin considers this matter covered.

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Berlin  
Re: 288A-NY-307369 , 02/21/2012

LEAD(s) :

Set Lead 1: (Info)

ALL RECEIVING OFFICES

For information. Read and clear.

52 ☐ 02.ec  
♦♦

b6  
b7c

UNCLASSIFIED

Date: 2/24/12

Doc: IC3 Complaint

3/15

--

b6  
b7c

From: [redacted] (IF) (FBI)  
Sent: Friday, February 24, 2012 9:48 AM  
To: [redacted] (F) (FBI)  
Cc: [redacted] (IF) (FBI); [redacted] (IF) (FBI)  
Subject: IC3 complaint on [redacted]

b6  
b7C

Classification: UNCLASSIFIED

=====

RECORD: 288A-HQ-C1610517-DD  
288A-NY-307369 -7

On 02/23/2012, the IC3 received a complaint from IP address [redacted] which provided the following contact information:

b6  
b7C  
b7E

Name: [redacted]  
Age: [redacted]  
Telephone: [redacted]  
Email: [redacted]

The following subject information was reported:

Subject: [redacted]  
Address: [redacted]  
Email: [redacted]  
Nic: [redacted]  
Group: [redacted]  
Twitter: [redacted]

b6  
b7C

The complainant reported that [redacted] is [redacted] and is the leader of the hacktivist group TeaMp0ison. It was also reported that [redacted] released many databases from high profile websites, stolen tens of thousands of dollars in scams, and stolen credit cards.

b6  
b7C

The complainant reported that [redacted] "lured" him into thinking [redacted] worked for the FBI. He reportedly transferred over [redacted] via Western Union and PayPal to [redacted] over a seven month period and that [redacted] committed eBay scams using the complainant's PayPal account. The complainant reported he has chat logs, Western Union transfers, personal information, PayPal accounts, IP addresses, etc on [redacted] and that upon contact, he could provide "solid evidence."

b6  
b7C

No other complaints were found on [redacted] or email address [redacted]. On 01/17/2012, the IC3 received a complaint on TeaMp0ison member [redacted] for hacking a small webhosting company called host45.com. The complaint identified

b6  
b7C

[redacted] as [redacted] of [redacted]  
[redacted] email address [redacted] This information  
was initially forwarded to FBI Houston, San Diego, and  
Milwaukee, case ID 288A-HQ-C1610517-DD, serial 159. The  
complaint will also be forwarded to New York and Memphis.

b6  
b7C  
b7E

TeaMp0ison is affiliated with the hacktivist group Anonymous. A  
search of Sentinel and Cyber Criminal Division's [redacted]  
Intranet site did not indicate that an investigation was opened  
on [redacted] However, It appears New York has an open case  
on TeaMp0ison, case ID 288A-NY-307369. Therefore, New York is  
included on this dissemination.

b6  
b7C  
b7E

On 02/23/2012, the aforementioned summary and attached complaint  
was forwarded via email to Cyber Program Coordinators SSA  
[redacted] SSA [redacted] SSA [redacted] and New York  
Cyber SA [redacted]

b6  
b7C

Recipients were asked to advise the IC3 if a case is opened on  
[redacted] and/or if any action is taken on this information.

IC3 Automatch case number [redacted]

b7E

[redacted]  
Thanks,

[redacted]  
Management & Program Analyst  
Cyber Division  
Internet Crime Complaint Center (IC3)  
[redacted]

b6  
b7C  
b7E

=====  
Classification: UNCLASSIFIED



## COMPLAINT REFERRAL FORM

Complaint ID:

b7E

*The following information was provided by the victim and may be forwarded to the appropriate law enforcement or regulatory agencies.*

Date: 02/23/2012 10:46:10

### Victim Information

Name:

b6  
b7C

Business Name:

Age:

Gender:

M

Address:

NA

City:

NA

Do you live within the city limits?:

No

County:

N/A

State:

Country:

Zip Code/Route:

Phone number:

Email Address:

b6  
b7C

Name of your local police or sheriff's office:

N/A

Is the complaint you are filing related to the Internet or an online service? Yes

Do you have pertinent documents in paper form? Yes

**Information about the Individual/Business that victimized you**

Business Name:

Name:

Gender:

Address:

City:

State:

Country:

Zip Code/Route:

Phone number:

Email Address:

b6  
b7c

**Other Identifiers**

Web Site:

IP Address:

IRC Server:

Chat Room Name:

Usenet Newsgroup:

Other:

**Monetary Loss**

If you lost money from the incident you are reporting, please specify the total dollar amount of your loss.

b6  
b7c

Please indicate the means of payment (select all that apply)

- ☒ Cash
- ☐ Cashier's Check
- ☐ Check/Debit Card
- ☐ Credit Card
- ☐ Money Order
- ☒ Wire Transfer
- ☒ Other (Specify) Western Union

Did you use a third party online payment service such as PayPal, BidPay, Escrow? Yes



### Description of the Incident

Describe in your own words how you have been victimized.

[redacted] as he is known on the online hacking side of things, is a leader of the  
hacktivist group 'TeaMp0isoN' and runs the hacking BBforum, Doxsters. He has released many databases  
from high profile websites around the globe, and stolen tens of thousands of dollars in scams, and stolen  
credit cards. Personally, he lured me into thinking he worked for the FBI, and over a period of 7 months I  
transferred over [redacted] to him through Western Union, and another [redacted] or so through PayPal. He  
committed eBay scams through my paypal account, which resulted in ARLcollect debt collectors to  
approach me about my negative balance. He has scammed many more like me. I have every single chat  
file, western union form, personal information, paypal accounts, IP addresses, and much, much more  
information. His twitter [redacted]

I prefer not to give out my details at this moment; however I can assure you contact with me will result in solid evidence against his name.

I can be contacted at

Thankyou.

Please indicate any medium used by the individual/business in the course of the incident.

- ☒ Bulletin board
- ☒ Chat room
- ☒ Email
- ☐ Fax
- ☐ In person
- ☒ Internet messaging
- ☒ Mail
- ☐ Newsgroup
- ☐ Telephone
- ☒ Web site
- ☐ Wire
- ☐ Other

Please indicate the initial means of contact with the individual/business that victimized you.

Bulletin board

Was this initial means of contact unsolicited/uninvited?

Yes

What was your relationship with the individual/business you are complaining about prior to the incident you are reporting?

online acquaintance

Did you conduct any research on the individual/business prior to the incident?

Yes

How much time has passed since you determined you were victimized?

4 - 5 months

### Contact Information

Are there witnesses or other victims to this crime?

Yes - contact me further please.

Have you reported this crime to any law enforcement or government agencies?

- ☐ Better Business Bureau
- ☐ Consumer protection agency
- ☐ Individual/business that victimized you
- ☐ Police/other law enforcement
- ☐ Private attorney

Provide the specific name of each organization, contact name, contact phone number, email address, date reported, and report number (if known).

[left blank]

### Digital Signature

By digitally signing this document, I affirm that the information I provided is true and accurate to the best of my knowledge. I have read the IC3's Privacy Policy, and understand that this information may be provided to law enforcement and regulatory agencies. If available, I will provide additional documentation not included in this complaint, such as email correspondence, payment receipts, or electronic logs, upon request to the best of my ability. I authorize the dissemination of the complaint, or information in the complaint, to appropriate federal, state, local, tribal or international Law Enforcement Agencies (LEAs) for purposes of investigating the complaint.

b6  
b7c

3/1/70

--

b6  
b7c

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 03/15/2012

To: New York

From: New York

CY-2

Contact: SA

[Redacted]

Approved By:

[Redacted]

Drafted By:

Case ID #: 288A-NY-307369 (Pending) - 8

Title: TEAMPOISON;  
VICTIM - FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION  
OO:NY

**Synopsis:** To document statistical accomplishments for captioned case.

**Details:** The following accomplishments are associated with the above-captioned case.

b6  
b7C  
b7E

UNCLASSIFIED

UNCLASSIFIED

To: New York From: New York  
Re: 288A-NY-307369, 03/15/2012

Accomplishment Information:

Number: [REDACTED]  
Type: [REDACTED]  
ITU: [REDACTED]  
Claimed By:  
SSN: [REDACTED]  
Name: [REDACTED]  
Squad: [REDACTED]

b6  
b7C  
b7E

Number: [REDACTED]  
Type: [REDACTED]  
ITU: [REDACTED]  
Claimed By:  
SSN: [REDACTED]  
Name: [REDACTED]  
Squad: [REDACTED]

b6  
b7C  
b7E

Number: [REDACTED]  
Type: [REDACTED]  
ITU: [REDACTED]  
Claimed By:  
SSN: [REDACTED]  
Name: [REDACTED]  
Squad: [REDACTED]

b6  
b7C  
b7E

Number: [REDACTED]  
Type: [REDACTED]  
ITU: [REDACTED]  
Claimed By:  
SSN: [REDACTED]  
Name: [REDACTED]  
Squad: [REDACTED]

b6  
b7C  
b7E

UNCLASSIFIED

UNCLASSIFIED

To: New York From: New York  
Re: 288A-NY-307369, 03/15/2012

LEAD(s) :

Set Lead 1: (Info)

NEW YORK

AT NEW YORK

Read and clear.

♦♦

UNCLASSIFIED

Date: 12/16/2011

Doc: Email from

to

2

b6  
b7C  
b7D



Date: 12/14/2011

Doc: 

3 



b6  
b7C  
b7D

See 1A1  
Ⓢ

ECC31512.WPD

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 03/15/2012

To: New York

From: New York  
CY-2

Contact: SA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-NY-307369 (Pending) -//

Title: TEAMPOISON;  
VICTIM - FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION  
OO:NY

Synopsis: To provide update to captioned investigation.

Enclosure(s): CD-ROM: Titled FNBLI containing images of  
#opRobinHood bulletin from [REDACTED] images from [REDACTED]  
[REDACTED] and web logs from FIRST NATIONAL BANK OF LONG  
ISLAND.

Details: From November 29, 2011 to December 13, 2011, writer  
received logs from FIRST NATIONAL BANK OF LONG ISLAND (FNBLI).  
FISERV is FNBLI's service provider who handles FNBLI's network  
and IT infrastructure. Writer reviewed the web intelligence logs  
from the SQL injection attempts.

Investigation in New York continues.

♦♦

UNCLASSIFIED

b6  
b7C  
b7E

b6  
b7C  
b7E

b7D

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/09/2011

To: New York

From: New York

CY-2

Contact: SA [REDACTED]

b6  
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-NY-307369 (Pending) - 12

Title: TEAMPOISON;  
VICTIM - FIRST NATIONAL BANK OF LONG ISLAND;  
COMPUTER INTRUSION  
OO:NY [REDACTED]

b6  
b7C

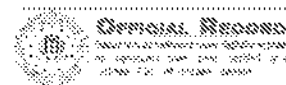
Synopsis: Request removal of co-case agent on captioned case.

Details: Writer requests removal of himself as co-case agent for the above-captioned investigation due to a forthcoming transfer to FBI NY squad CY-1.

♦♦

UNCLASSIFIED

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication****Title:** (U) To provide update to captioned case.**Date:** 12/28/2012**From:** NEW YORK

NY-CY03

**Contact:** [REDACTED]**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 288A-NY-307369(U) TEAMPOISON FIRST NATIONAL BANK OF  
LONG ISLAND**Synopsis:** (U) To provide update to captioned case.**Full Investigation Initiated:** 12/05/2011**Details:**

From April 8, 2012, to October 7, 2012, Special Agent [REDACTED]  
[REDACTED] was the Acting Coordinating Supervisor Special Agent  
(A/CSSA) for the Cyber branch. During this time period her case work  
was pending inactive.

On December 28, 2012, SA [REDACTED] contacted [REDACTED]  
[REDACTED]  
[REDACTED] to discuss captioned case.

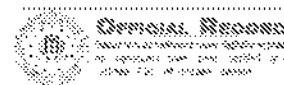
Investigation in New York continues.

◆◆

UNCLASSIFIED

b6  
b7C  
b7Eb6  
b7Cb6  
b7C

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication****Title:** (U) To provide update to captioned case.**Date:** 12/28/2012**From:** NEW YORK

NY-CY03

**Contact:** [REDACTED]b6  
b7C  
b7E**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 288A-NY-307369

(U) TEAMPOISON;

FIRST NATIONAL BANK OF LONG ISLAND

**Synopsis:** (U) To provide update to captioned case.**Full Investigation Initiated:** 12/05/2011**Details:**

On 12/28/2012, SA [REDACTED]

contacted [REDACTED]

b6  
b7C

[REDACTED] advised the following:

- Since the November 2011 intrusion attempts there have been no further attempts to access the FNBLI computer network by the hactivist group TeaMp0ison or Operation Robin Hood.
- FNBLI did not encounter any unauthorized intrusions into their computer network. During November 2011, the incidents were attempts to access the network, however no successful penetration occurred.

From 2/14/2013 to 5/10/2013 Special Agent [REDACTED] was the Acting Supervisory Special Agent (A/SSA) for Squad CY-3. During this time period her case work was pending inactive.

b6  
b7C

Writer will contact Southern District of New York (SDNY) during next file review period to confirm SDNY concurrence with closing captioned case.

UNCLASSIFIED

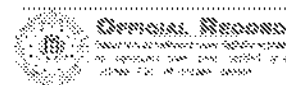
UNCLASSIFIED

Title: (U) To provide update to captioned case.  
Re: 288A-NY-307369, 12/28/2012

◆◆

UNCLASSIFIED

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication****Title:** (U) To document SDNY attempted contact.**Date:** 10/01/2013**From:** NEW YORK

NY-CY03

**Contact:** [REDACTED]b6  
b7C  
b7E**Approved By:** SSA [REDACTED]**Drafted By** [REDACTED]**Case ID #:** 288A-NY-307369

(U) TEAMPOISON;

FIRST NATIONAL BANK OF LONG ISLAND

**Synopsis:** (U) To document attempt to contact Deputy Chief [REDACTED]  
[REDACTED]b6  
b7C**Full Investigation Initiated:** 12/05/2011**Details:**

On September 26, 2013, writer sent an e-mail to Deputy Chief [REDACTED]  
[REDACTED] Southern District of New York (SDNY), in regards to SDNY's  
concurrence to close captioned case. All investigative steps have been  
taken and no further investigation is warranted at this time.

b6  
b7C

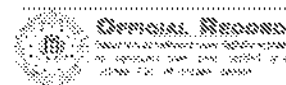
Writer is currently waiting on a response and call back from SDNY.

◆◆

UNCLASSIFIED



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication**

Title: (U) Closing EC.

Date: 12/31/2013

From: NEW YORK

NY-CY03

Contact: [REDACTED]

b6  
b7C  
b7E

Approved By: SSA [REDACTED]

Drafted By [REDACTED]

Case ID #: 288A-NY-307369

(U) TEAMPOISON;

FIRST NATIONAL BANK OF LONG ISLAND

Synopsis: (U) To document case summary and case closing to captioned case.

Full Investigation Initiated: 12/05/2011

## Details:

On November 28, 2011, investigation was predicated upon information received from Squad ID-24 who notified Squad CY-2 of [REDACTED] that indicated an SQL injection (SQLi) vulnerability at THE FIRST NATIONAL BANK OF LONG ISLAND (FNBLI).

b7E

According to open source information FNBLI had become a target of #OpRobinHood. #OpRobinHood was a joint venture between hacker groups "TeamP0ison" and Anonymous to "take on the banks, steal money and donate it to charities and protests." TeamP0ison, [REDACTED] claimed responsibility for targeting FNBLI and for revealing the FNBLI's server vulnerability.

b7E

On November 28, 2011, writer contacted [REDACTED] and advised him of the SQLi vulnerability and the possible intrusion into their computer network. Subsequent to the initial contact, [REDACTED] contacted writer and confirmed there were SQLi attempts on one of FNBLI.COM's web

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Closing EC.

Re: 288A-NY-307369, 12/31/2013

servers. FNBLI and their service provider FISERV confirmed attacker internet protocol (IP) address [REDACTED] made numerous attempts to gain access to FNBLI's server beginning on November 28, 2011, at 11:01 AM EDT. A WHOIS lookup revealed that IP [REDACTED] resolves to KABEL DEUTSCHLAND.

b7E

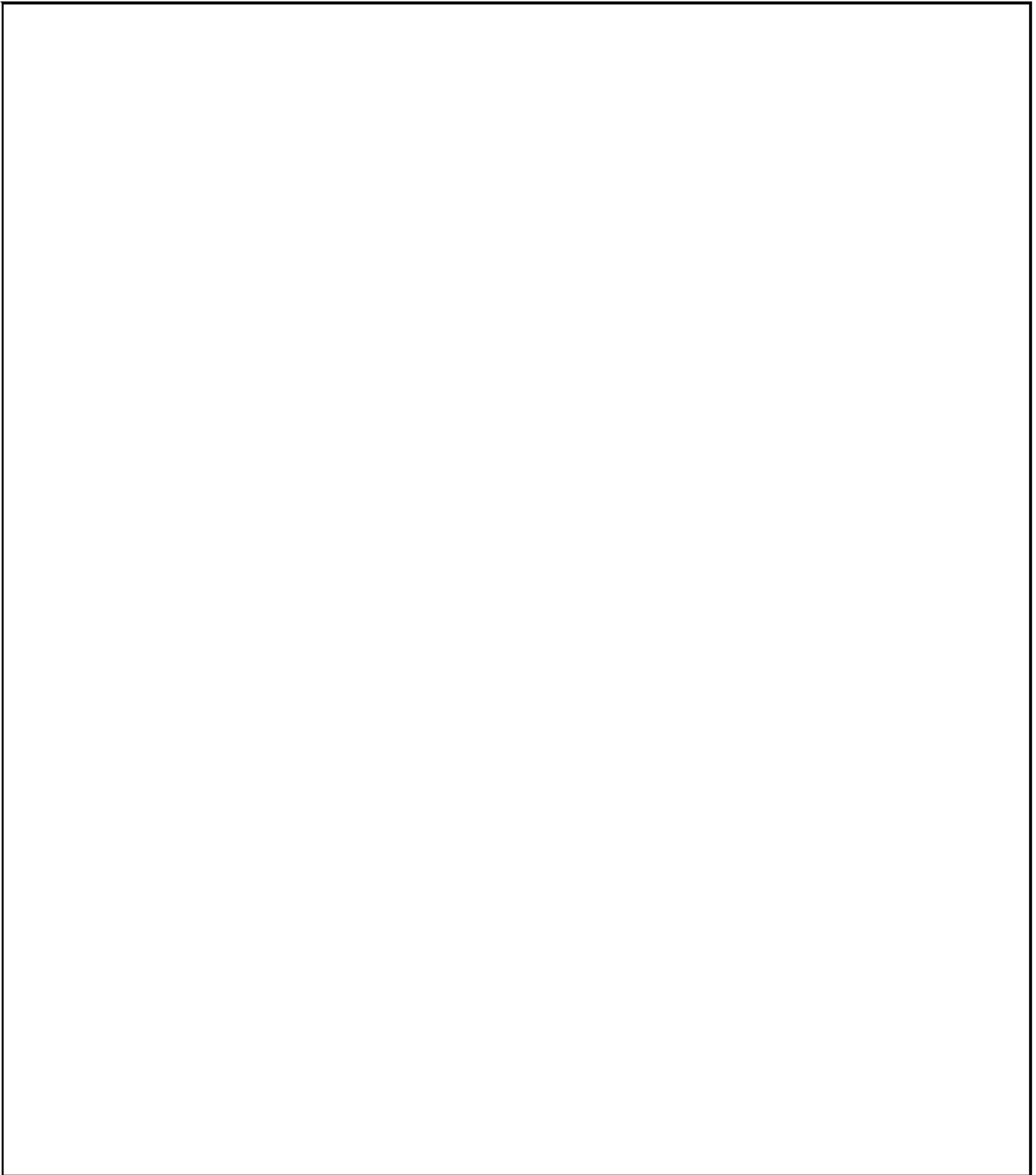
b6  
b7C  
b7D

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Closing EC.

Re: 288A-NY-307369, 12/31/2013



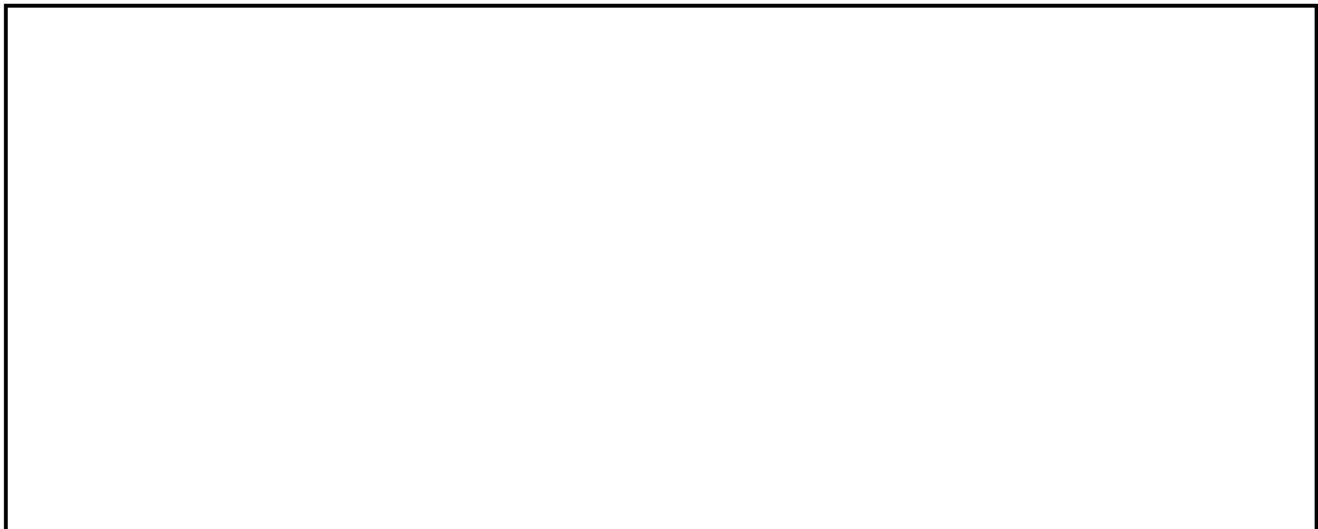
b6  
b7C  
b7D

UNCLASSIFIED

## UNCLASSIFIED

Title: (U) Closing EC.

Re: 288A-NY-307369, 12/31/2013



b6  
b7C  
b7D

Writer further analyzed web intelligence logs and web traffic logs that FNBLI provided. Additional SQLi attempts were made from IP addresses from overseas. No successful intrusion occurred during the #OpRobinHood attack.

On 12/28/2012, writer contacted [redacted] advised the following:

b6  
b7C

- Since the November 2011 intrusion attempts there have been no further attempts to access the FNBLI computer network by the hacktivist group TeaMp0isoN or #OpRobinHood.
- FNBLI did not encounter any unauthorized intrusions into their computer network. During November 2011, the incidents were attempts to access the network, however no successful penetration occurred.

On or about November 1, 2013, SSA [redacted] concurred with closing captioned investigation administratively due to; [redacted]

b6  
b7C  
b7E

[redacted] All leads and evidence have been cleared.

New York considers this investigation closed.

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Closing EC.

Re: 288A-NY-307369, 12/31/2013

◆◆

UNCLASSIFIED

(Overall Document Classification Required)

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication**

Title: (?) [REDACTED]

Date: 09/21/2020

Drafted By: [REDACTED]

Case ID #: 288A-PG-79338-[REDACTED]

(U) ANONYMOUS [REDACTED]

Details: 03/23/2012 [REDACTED] date of birth [REDACTED]  
social security account number [REDACTED] home address [REDACTED]

[REDACTED] was

interviewed at the Texas City office of the Federal Bureau of Investigation (FBI) located at 600 Gulf Freeway, Suite 211, Texas City, TX. Also present during the interview was Texas Department of Public Safety (DPS) Agent [REDACTED]. After being advised of the interviewing Agents' identity, [REDACTED] stated that he had graduated from High School and attended ITT Technical Institute, but had quit before getting a certificate. He further stated he was able to read and write English. [REDACTED] was then presented FBI form FD-395, advice of rights. It was requested that he read the form and sign it if he agreed and did not have any questions. [REDACTED] read the form, stated that it was a standard form, and then signed the bottom. Special Agent (SA) [REDACTED] signed the bottom of the form as did Agent [REDACTED]. The FD- 395 will be maintained in the 1A section of the file. After signing this form, [REDACTED] provided the following information: [REDACTED]

b3  
b6  
b7C  
b7Eb6  
b7Cb6  
b7Cb6  
b7C

(Overall Document Classification Required)

(Overall Document Classification Required)

Title: (?) [REDACTED]

Re: 288A-PG-79338-[REDACTED] 09/21/2020

b3  
b6  
b7C  
b7E

[REDACTED]

[REDACTED] is working with [REDACTED] Team Poison and [REDACTED]

b6  
b7C  
b7E

[REDACTED]

b6  
b7C  
b7E

(Overall Document Classification Required)

08/23/2011

[redacted] who is known to the writing agent through previous contact, sent five email messages to the writing agent between the dates of August 14, 2011 and August 16, 2011. These emails messages are attached and made part of this communication.

b6  
b7C  
b7D

In the email dated August 14, 2011 at 6:49 AM, [redacted] provided the following information:

b6  
b7C  
b7D

---Begin Email Message---

Subject: [redacted]  
From: [redacted]  
Sent: Sunday, August 14, 2011 6:49 AM  
To: [redacted]

b6  
b7C  
b7D

I have below, [redacted]

[redacted]

b6  
b7C  
b7D

"TeaMp0isoN\_", and more [redacted]

[redacted]



(Overall Document Classification Required)

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication**

Title: (U//~~FOUO~~) [REDACTED] SENT FIVE  
EMAIL MESSAGES TO AGENT

Date: 09/30/2020

Drafted By: [REDACTED]

Case ID #: 288A-SD-NEW

(U) [REDACTED]  
[REDACTED]

INTRUSION INFO SYSTEMS

Details: 08/23/2011 [REDACTED] who is known to the writing agent through previous contact, sent five email messages to the writing agent between the dates of August 14, 2011 and August 16, 2011. These emails messages are attached and made part of this communication. In the email dated August 14, 2011 at 6:49 AM, [REDACTED] provided the following information: ---Begin Email Message---

Subject: [REDACTED]

From: [REDACTED]

[REDACTED] Sent: Sunday, August 14, 2011 6:49 AM To:

[REDACTED] I have below, [REDACTED]

[REDACTED]

[REDACTED] "TeaMp0ison ", and more. [REDACTED]

[REDACTED]

(Overall Document Classification Required)

b6  
b7C  
b7Db6  
b7C  
b7Db3  
b6  
b7C  
b7D  
b7E

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1475926-000

Total Deleted Page(s) = 1  
Page 4 ~ b6; b7C; b7D; b7E;

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

UNCLASSIFIED//~~FOUO~~**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication**Title: (U//~~FOUO~~) To document email from CHS

Date: 07/01/2013

b6  
b7C  
b7D  
b7E

From: SAN JUAN

SJ-CY

Contact:

Approved By: A/SSA

Drafted By:

b3  
b6  
b7C  
b7E

Case ID #: 288A-SJ-42309

Synopsis: (U//~~FOUO~~) To document email from CHSb6  
b7C  
b7D  
b7E

Full Investigation Initiated: 07/07/2011

Enclosure(s): Enclosed are the following items:

1. (U//~~FOUO~~)

Details:

On 6/27/2013, CHS

b6  
b7C  
b7D  
b7EUNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1475926-000

Total Deleted Page(s) = 5  
Page 1 ~ b6; b7C; b7D; b7E;  
Page 2 ~ b6; b7C; b7D; b7E;  
Page 3 ~ b6; b7C; b7D; b7E;  
Page 4 ~ b6; b7C; b7D; b7E;  
Page 5 ~ b3; b6; b7C; b7D; b7E;

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