Description of document:	Summary reports of investigations closed during 2012 (ROIs) produced by the Treasury Office of Inspector General (OIG)
Requested date:	2013
Released date:	25-March-2013
Posted date:	29-April-2013
Source of document:	FOIA Request Disclosure Services Department of the Treasury Washington, DC 20220 Fax: 202-622-3895

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

March 25, 2013

Re: Freedom of Information Act Request 2013-03-089

This responds to your letter addressed to the Department of the Treasury's Disclosure Services office, in which you requested, pursuant to the Freedom of Information Act, 5 U.S.C. § 552 (FOIA), copies of certain closed reports of investigation (ROIs) produced by the Treasury Office of Inspector General (OIG). Consistent with our pre-existing understanding, you are asking for just the summary reports, not the exhibits attached thereto. Similarly, you understand that names and other identifying information of subjects and witnesses are redacted, consistent with Exemption 7C of the FOIA, 5 U.S.C. § 552(b)(7)(C). With those understandings, I enclose a CD-ROM containing the responsive records.

You have the right to appeal under 5 U.S.C. § 552(a)(6)(A)(i) for full disclosure of the requested files. Pursuant to the Department's FOIA appeal process set forth in 31 C.F.R. § 1.5(i), an appeal must be submitted within 35 days from the date of this response to your request, signed by you and addressed to: Freedom of Information Act Appeal, DO, Disclosure Services, Department of the Treasury, Washington, D.C. 20020. The appeal should reasonably describe the records to which access has been denied and should specify the date of the initial request and the date of this determination. Please enclose copies of your initial requests and this letter.

Sincerely,

Mallory Johnson for

R.K. Delmar
Counsel to the Inspector General

Enclosures

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

December 3, 2012

MEMORANDUM FOR LAURA L. MCAULIFFE, SENIOR ADVISOR
OFFICE OF THE COMPTROLLER OF THE CURRENCY

FROM: [redacted] 12/4/12
Special Agent in Charge

SUBJECT: Closure of Investigative Case Support to Operation [redacted]

BANK-11-1174-I

A case investigation was initiated by the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG) to document case investigative support to the U.S. Attorney's Office (USAO) Minneapolis, MN and the Minnesota Financial Crimes Task Force (MNFCTF) in Operation [redacted]. The investigation originated by the U.S. Secret Service (USSS) in November 2009 when information was developed from separate ongoing investigations which indicated that a common group of individuals were involved in a significant criminal enterprise committing a variety of financial crimes in the Minneapolis, MN area and other regions of the U.S.

The offenses investigated in Operation [redacted] included conspiracy to commit bank fraud, mortgage fraud, money laundering, identity theft, and mail and wire fraud. In February 2012, two of the leaders of the enterprise were convicted and sentenced to over 22 years each of imprisonment. A total of 28 co-conspirators were prosecuted as a result of the investigation.

The evidence presented at trial proved that the leaders worked with numerous co-conspirators to buy and sell stolen bank-customer information that was ultimately used to open fraudulent bank and credit card accounts, apply for loans and obtain cash. Subsequently, these co-conspirators altered checks for deposit into fraudulent accounts and drafted checks against them. They also acquired cash from fraudulent credit card accounts they had established and used the false credit cards to purchase merchandise. They co-opted home equity lines of credit without the knowledge or consent of the true account holders, using the lines of credit for

their personal benefit. In addition to recruiting bank employees to assist in the scheme, co-conspirators regularly recruited other individuals to conduct fraudulent financial transaction, often transporting them to various banks around the country to commit their crimes.

The financial institutions victimized included [redacted]

The TOIG had been requested by the USAO Minneapolis to assist the investigation by contacting bank security officials and request their cooperation with the operation. TOIG worked with the Office of Comptroller of the Currency (OCC) in gaining the banks' cooperation, which included allowing confidential informants to make transactions and interact with employees who were complicit in providing access to financial accounts and funds. Agents from TOIG met with bank security and OCC officials to mitigate and allay concerns expressed by bank officers that their continued cooperation with law enforcement would not affect their regulatory oversight and compliance or their obligation to report of illegal conduct to the Treasury.

TOIG also conducted criminal history checks; database searches and FinCEN financial record checks for 15 additional bank employees and insiders who were identified as participating in the predicate criminal enterprise.

Accordingly, TOIG is closing its investigation into this matter. However, if you have any questions related to this investigation, please feel free to contact me at 202-927-[redacted].

REPORT OF INVESTIGATION
BEP-12-0128-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case #: BEP-12-0128-I

Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: October 31, 2011

Investigation Completed: MAY 21 2012

Conducted by: [redacted]
Special Agent

Origin: [redacted]
Product and Physical Safety Division
Office of Security
Bureau of Engraving and Printing

Approved by: [redacted]
Special Agent in Charge

Summary

On October 27, 2011 the Department of Treasury, Office of Inspector General, Office of Investigations (TOIG) received an allegation regarding the misuse of five Government computers at the Bureau of Engraving and Printing (BEP).

On October 26, 2011 the Global Security Operation Center (GSOC) notified the BEP Office of Security that internet traffic potentially linked to child pornography was monitored and linked to five BEP computers.

On October 27, 2011 the matter was referred from [redacted], BEP, [redacted], Office of Security to TOIG. TOIG responded to the BEP, seized the suspect computers and proceeded to conduct forensic examinations on each computer to determine which BEP employee may be linked to the computer misuse.

On March 20, 2011, Assistant United States Attorney (AUSA) for the District of Columbia, [redacted] declined criminal prosecution based upon lack of prosecutorial merit.

Basis and Scope of the Investigation

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted], Stock Control Recorder, BEP
- [redacted] Office of Security, BEP
- [redacted], Office of IT Operations, BEP
- [redacted], Manager, IT Security Division, Office of Critical Infrastructure and IT Security, BEP.

In addition, TOIG reviewed pertinent documents, including:

- Dell Optiplex GX280, Service Tag: [redacted]
- Dell Optiplex 960, Service Tag: [redacted]
- Dell Optiplex GX620, Service Tag: [redacted]
- Dell Optiplex 960 Dell Service Tag Number: [redacted]
- Gateway 507GR computer, serial number [redacted]

Investigative Activity

On October 26, 2011, the GSOC notified the BEP Office of Security that internet traffic potentially linked to child pornography was monitored and linked to five BEP computers.

On October 27, 2011, TOIG responded to the BEP at 14th and "C" Streets SW, Washington DC in regards to a referral alleging the misuse of the Government computers. TOIG met with [redacted], Office of Security; [redacted], Office of IT Operations; and [redacted], IT Security Division, Office of Critical Infrastructure and IT Security. (Exhibit 1)

[redacted] and [redacted] explained that all of the suspect computers may have been accessed with a unique log on password belonging to BEP employee [redacted] is employed by the BEP as a [redacted].

[redacted] further explained one of the suspect computers was named [redacted] because the primary user is BEP employee [redacted]. However, this particular computer was located in an engineering office and was shared by several employees. The four additional suspect computers were located in general purpose areas where numerous employees have potential access.

Continuing on the same date, TOIG seized three of the suspect general purpose computers for forensic examination. [redacted] told TOIG the fourth general purpose computer hard drive was reimaged and upgraded to Windows 7 prior to the notification of the incident by GSOC. Hedlund said the hard drive was reimaged with numerous other hard drives and placed back into

service. [redacted] further stated the hard drive was not recorded or tracked after the reimaging process and could not be identified.

Continuing on the same date, [redacted], BEP, Information Technology Specialist (ITS) retrieved and delivered the three general purpose computers into the custody of TOIG. TOIG transported, inventoried and secured the computers in the TOIG evidence vault. (Exhibit 2)

The three seized computers are identified as follows:

1. Dell Optiplex GX280, Service Tag: [redacted]
2. Dell Optiplex 960, Service Tag: [redacted]
3. Dell Optiplex GX620, Service Tag: [redacted]

[redacted] informed TOIG the seizure of the fifth suspect computer primarily used by [redacted] may disrupt the continuity of BEP operations. In an effort to accommodate the BEP and maximize the preservation of electronic evidence, TOIG Cyber Investigations was notified and tasked to seize the fifth computer hard drive on October 31, 2011.

On October 31, 2011, [redacted] provided TOIG Cyber Investigations with 80GB Seagate ST380815A5 Barracuda hard drive (Serial Number: [redacted]) that was installed in a BEP Dell Optiplex 960 (Dell Service Tag Number: [redacted]). TOIG Cyber Investigations imaged and secured the digital evidence related to hard drive (Serial Number: [redacted].

On December 16, 2011, TOIG Cyber Investigations reported, numerous images depicting nudity and/or sexual acts located in the data recovered from the hard drive that was installed in the BEP Dell Optiplex 960 (Dell Service Tag Number: [redacted]). TOIG Cyber Investigations also reported the pornographic images were associated with the [redacted] user profile. No evidence was found regarding images of minors or child pornography. (Exhibit 3 – also see the file [redacted]-Forensic_Analysis.zip)

On December 19, 2011, TOIG interviewed subject [redacted], regarding the misuse of government computers.

[redacted] told TOIG that he works in the "A-200" area of the BEP and has access to BEP computers. [redacted] stated he knows a colleague named [redacted] and uses [redacted]'s computer.

TOIG asked [redacted] if any other BEP employees may have used his logon to access [redacted]'s computer, [redacted] stated, "I don't let anyone use my site". TOIG asked [redacted] to clarify if "site" meant "logon", [redacted] stated "right".

TOIG asked [redacted] if he ever accessed pornography via a BEP computer. [redacted] became evasive and initially stated no. Agents presented digital evidence contradicting his statement and [redacted] admitted he searched for and viewed pornography by accessing the internet through BEP computers. [redacted] told TOIG that he accessed pornography primarily during breaks or downtime for approximately one hour per incident.

TOIG questioned [redacted] regarding search terms he used which potentially indicated he was searching for child pornography. [redacted] admitted he used the search terms but further stated, "I'm not into that". TOIG asked [redacted] what he expected to find using child pornography search terms. [redacted] told TOIG he did not know what he might find.

[redacted] agreed to provide TOIG with a written statement upon request. [redacted]'s written statement reiterates that he searched for and viewed pornography during his work breaks and that he used some search terms that suggest a search for child pornography. In regards to the child pornography search terms, [redacted]'s written statement further states, "I can't explain my reason for doing so, but I regret it".

TOIG requested consent to search [redacted]'s home computer. [redacted] agreed to let TOIG retrieve and conduct a forensic exam of his home computer. TOIG traveled to [redacted]'s residence, [redacted] and seized one Gateway 507GR computer, serial number [redacted]. (Exhibit 4)

On January 06, 2012, TOIG Cyber Investigations reported the results of [redacted]'s home computer examination. The analysis located 192 pornographic images, a pornographic web page and evidence that someone used that computer to view pornography in March 2007 and January 2008. No images depicting child pornography were located. (Exhibit 5 - also see the file [redacted]_Home_PC_ForensicReport.zip)

Between January 06, 2012 and February 16, 2012, TOIG Cyber Investigations completed the forensic examinations of BEP computers Dell Optiplex GX280, Service Tag: [redacted]; Dell Optiplex GX620, Service Tag: [redacted]; and a Dell Optiplex 960, Service Tag: [redacted]. TOIG Cyber Investigations analysis located evidence of pornography associated with the [redacted] user profile. No images depicting child pornography were located.
(Exhibit 6 - also see the file OptiplexGX280_ForensicReport.zip)
(Exhibit 7 - also see the file OptiplexGX620_ForensicReport.zip)
(Exhibit 8 - also see the file Optiplex960-Internet_History.html)

Referrals

On March 20, 2012, TOIG presented the case to AUSA [redacted] for the District of Columbia for possible criminal prosecution. AUSA [redacted] declined criminal prosecution due to lack of prosecutorial merit. (Exhibit 9)

Judicial Action

N/A

Findings

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policy(ies) were violated or could be applied to the case:

- 5 CFR 2635.101 – Basic obligation of Public Service
- 5 CFR 2635.704 – Use of Government property
- 31 CFR 0.210 – Conduct while on Official Duty or on Government Property

Distribution

Timothy Gerald, Manager
Product and Safety Division
Office of Security
Bureau of Engraving and Printing

Signatures

Case Agent:

[redacted], Special Agent — 05/18/2012 Date

Supervisor:

[redacted] Special Agent in Charge — 5-18-12 Date

Exhibits

1. Referral Memorandum, from [redacted], BEP to TOIG, dated October 27, 2011.
2. Memorandum of Activity, Evidence Obtained, draft dated November 04, 2011.
3. Memorandum of Activity, Cyber, draft date December 16, 2011.
4. Memorandum of Activity, [redacted], draft date December 20, 2011.
5. Memorandum of Activity, Cyber, draft date January 06, 2012.
6. Memorandum of Activity, Cyber, draft date January 06, 2012.
7. Memorandum of Activity, Cyber, draft date January 10, 2012.
8. Memorandum of Activity, Cyber, draft date February 16, 2012.
9. Memorandum of Activity, Case Presentation, draft date March 20, 2012.

REPORT OF INVESTIGATION
BEP-12-0485-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Bureau of Engraving and Printing
Washington, DC

Case #: BEP-12-0485-I

Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: December 20, 2011

Investigation Completed: JUN 19 2012

Conducted by: [redacted]
Special Agent

Origin: Anonymous Complaint

Approved by: [redacted]
Special Agent in Charge

Summary

On December 20, 2011, an anonymous complaint was received by the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), alleging improper handling of plates by Bureau of Engraving and Printing (BEP) personnel, creating creasing issues regarding the newly issued $100 Federal Reserve Note (FRN), and the reason for series changes in FRNs. Specifically, it was alleged that [redacted], Eastern Currency Facility (ECF), BEP, concealed plate cracking. (Exhibit 1)

The investigation determined that the allegations are unsubstantiated. It does not appear that [redacted] concealed the fact that plates were cracking. Additionally, TOIG determined that that there are several reasons why there would be a series change necessitating new plates, for example, design change, a change in the U.S. Treasurer or U.S. Treasury Secretary. The plates were changed in 2009 from 2009 to 2009A due to the personnel change of U.S. Treasurer Rosie Rios.

Basis and Scope of the Investigation

BEP began producing the NexGen $100 notes in January 2010, with an anticipated Federal Reserve Board (FRB) issuance in February 2011. During production, BEP noticed sporadic creasing of the notes in April 2010, and a more concentrated occurrence of creasing in June 2010. Shortly thereafter, in July 2010, BEP began working with the currency paper supplier to determine the cause of the creasing problem. BEP suspended production at Western Currency Facility (WCF) in September 2010 and conducted manual/visual inspections of individual notes to obtain data about the extent of the creasing problem. BEP and FRB officials stated that issuing flawed notes could cause the public to question note authenticity, particularly abroad where U.S. currency is scrutinized more closely. In October 2010, FRB announced a delay in the issuance of the NexGen $100 notes and has not accepted delivery of any of the finished notes. The research and tests performed show evidence of certain paper properties that have a strong correlation to creasing, but the tests have not identified the root cause of the problem.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted], Product and Investigations Branch, BEP
- [redacted] Office of Security, BEP
- [redacted], ECF, BEP

In addition, TOIG reviewed pertinent documents, including:

- KBA GIORI Technical Report, dated June 14, 2010.
- Fracture in Chromed Intaglio Plate: Microscopic Analysis, dated April 26, 2011.
- CAR-NC-2011-469 Intaglio Plate Cracking Timeline, dated November 2011.
- Summary of Premature Intaglio Plate Failures, no date.
- E-mail discussing KBA Report, dated May 13, 2011.
- Cracked Plates spreadsheet, no date.

Investigative Activity

In an interview with TOIG, [redacted] and [redacted] advised that the issue of the $100 FRN creasing has been resolved but the reason for the creasing is still unknown. [redacted] and [redacted] advised that there are several reasons why there would be a series change necessitating new plates including: Design change; a change in the U.S. Treasurer; or change in the U.S. Treasury Secretary. The plates were changed in 2009 from 2009 to 2009A, due to the personnel change of U.S. Treasurer Rosie Rios. (Exhibit 2)

In an interview with TOIG, [redacted] stated he never concealed the fact that plates were cracking and that the cracking problem has since been corrected as of November 2011 and is unaware of any cracking occurring since. Premature cracking was noticed in plates in March 2011. He explained that premature cracking occurs when the plate is attached to the cylinder and the press begins to run.

After the commencement of the process, the plates eventually crack. In 2010, a new plating line was created by KBA GIORI, the BEP contractor that manufactures the currency production machines. At that time, BEP switched from the old line of plates to the new. The plate cracking was noticed in March 2011 and continued through November 2011.

[redacted] continued that in April 2011, an independent laboratory, Laboratory Testing Incorporated (LTI), tested the hardness of the plates with specifications set by the check list for all KBA GIORI machines. KBA GIORI also looked at the hardness of the plates and plate hanging procedures on the cylinders and recommended to make the plates harder. BEP followed KBA GIORI's recommendation to harden plates and the result was additional plate cracking. In May 2011, an official BEP investigation was opened and a group of BEP employees from multiple offices led by [redacted] from the BEP plate printing department formed to review the plate cracking. Corrective Action Report (CAR). CAR-NC-2011-469 was generated by Corrective and Preventive Action Management System (CPAMS) that provides a synopsis from start to finish. The report includes a listing of cracked plates, the action taken, and what office took the action from March 2011 through November 2011.

In October 2011, BEP adjusted the system specifications to match those used with the older system prior to 2010, and the plates ceased cracking as of November 2011. Brent stated the premature cracking problem is resolved and now BEP is trying to determine why the cracking occurred in the first place. The plates that were cracking would have been destroyed with the exception of those stored in the vault for further review and testing. The cracked plates kept for testing were used by BEP employee, [redacted], to prepare an analysis report which concluded that he could not provide a definitive cause of plate cracking.

In October 2011, the ECF exchanged four plates with the BEP WCF to test the presses. The WCF has not yet tested the plates from ECF due to the Nexgen (2009A) testing. Plates are identified with a "W" for WCF or "E" for ECF. Approximately 82 plates had cracking issues. Of the approximate 82 problematic plates, the denominations were $1, $20, and $100 plates. [redacted] stated that of the 82 plates discussed, all but four of the plates have been destroyed. Plate numbers [redacted] and [redacted] are in the BEP plate vault. Plate [redacted] was listed incorrectly on the CPAMS report; the number should be [redacted]. Plate [redacted] has been destroyed. (Exhibits 3-5)

A TOIG review of documentation regarding the plate cracking at the BEP revealed:

- KBA GIORI Technical Report
  This report provides guidance on the mounting of plates, adjusting the registration of the intaglio plates, and the mounting of cardboard sheets and blanket. [redacted] of KBA GIORI visited BEP from May 10, 2011, through May 13, 2011, to diagnose the problem of the premature cracking and observe the production procedures used by BEP. [redacted] concluded that in his opinion, the cracking was due to the plates not being hard enough.

- Fracture in Chromed Intaglio Plate: Microscopic Analysis
  This report was prepared by [redacted] who was tasked to determine possible causes of plate

cracking. [redacted] used stereoscope light microscopy, reflected light microscopy (RLM), scanning electron microscopy (SEM) with energy dispersive spectrometry (EDS) to perform his analysis. [redacted] concluded that a definitive cause of plate cracking was unidentifiable.

- CAR-NC-2011-469 Intaglio Plate Cracking Timeline
  CAR-NC-2011-469 was generated by CPAMS that provides a synopsis from start to finish. The report includes details of the first two plates noticed to be cracked ([redacted] and [redacted]), as well as when plate cracking was noticed in other plates from March 2011 through November 2011 and what actions were taken by which offices within BEP. In October 2011, the ECF exchanged four plates with the BEP WCF to test the presses. The timeline provides that the WCF has not yet tested the ECF plating on the WCF system due to the Nexgen (2009A) testing. (Exhibit 6)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegations are unsubstantiated. It does not appear that [redacted] concealed the fact that plates were cracking. Additionally, TOIG determined that that there are several reasons why there would be a series change necessitating new plates, for example, design change, a change in the U.S. Treasurer or U.S. Treasury Secretary. The plates were changed in 2009 from 2009 to 2009A due to the personnel change of U.S. Treasurer Rosie Rios.

Distribution

[redacted], Product and Physical Safety Division, Office of Security, Bureau of Engraving and Printing

Signatures

Case Agent:

[redacted]

6/6/12
Date

Supervisor:

[redacted]

6-7-12
Date

Exhibits

1. Anonymous Complaint received by TOIG, dated December 20, 2011.
2. Memorandum of Activity, Interview of [redacted] and [redacted], dated March 7, 2012.
3. Memorandum of Activity, Interview of [redacted], dated April 13, 2012.
4. Memorandum of Activity, Interview of [redacted], dated April 23, 2012.
5. Memorandum of Activity, Interview of [redacted], dated May 2, 2012.
6. Memorandum of Activity, Document review of information provided by [redacted], dated April 13, 2012.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

NOV 20 2012

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM TO TIMOTHY GERALD, MANAGER, OFFICE OF SECURITY, BUREAU OF ENGRAVING AND PRINTING

FROM: John L. Phillips 11/19/12
Special Agent in Charge
Office of Investigations

SUBJECTS: [redacted]
Police Officers
Bureau of Engraving and Printing

Case Number: BEP-12-1688-I

Attached for your review is our Report of the Investigation (ROI) into allegations that Bureau of Engraving and Printing (BEP) Police Officers [redacted] misused National Criminal Information Center (NCIC) databases for personal use.

The investigation determined that the allegations are unsubstantiated. The allegation stems from an anonymous complaint alleging that [redacted] asked NCIC terminal operators to run NCIC for personal reasons.

The full Report and attached documentation are provided to your office for informational purposes only and any attachments that are referenced in the ROI exhibits can be made available upon your request.

If you have questions concerning this matter or, if you develop information that may indicate a need for additional or new investigative activity to assist you in resolving this matter, please contact me at (202) 927[redacted]. Staff requests for assistance should be directed to [redacted], Assistant Special Agent in Charge at (202) 927-[redacted].

REPORT OF INVESTIGATION
BEP-12-1688-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted] NCIC misuse (Treasury Employee)

Investigation Initiated: May 8, 2012

Investigation Completed:

Origin: Anonymous Complaint, TOIG Hotline

Case #: BEP-12-1688-I

Case Type: Criminal ___ Administrative x Civil ___

Conducted by: [redacted]
Special Agent

Approved by: [redacted]
Special Agent In Charge

Summary

On May 3, 2012, the Department of the Treasury, Office of the Inspector General, Office of Investigations (TOIG) received an anonymous complaint via the TOIG email hotline alleging Bureau of Engraving and Printing (BEP) Police Officers, [redacted] and [redacted] have been misusing the National Criminal Information Center (NCIC), querying criminal history information for their personal use. (Exhibit 1)

The allegations were unsubstantiated based on the review of NCIC/Washington Area Law Enforcement System (WALES) activity logs which revealed that no criminal history queries were conducted on the shift worked by Officer [redacted] nor did this investigation find that Officer [redacted] misused NCIC databases. Interview of other WALES operators supported the determination that the allegations are unsubstantiated.

Basis and Scope of the Investigation

On May 3, 2012, TOIG received an anonymous complaint via the TOIG email hotline alleging BEP Police Officers, [redacted] and [redacted] have been misusing NCIC, querying criminal history information for their personal use.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Investigator, BEP
- [redacted], Corporal, BEP
- [redacted] Corporal, BEP
- [redacted] Police Officer, BEP
- [redacted] Police Officer, BEP

In addition, TOIG reviewed pertinent documents, including:

- NCIC Activity Logs from Criminal Justice Information System (CJIS), Parkersburg, WV.
- WALES Activity Logs from Metropolitan Police Department (MPD), Washington, DC.

Investigative Activity

On June 25, 2012, TOIG received the NCIC logs for BEP's Originating Agency Indentifier (ORI) (DCBEP++) dated March 1, 2012 through May 31, 2012 from [redacted], Federal Bureau of Investigation (FBI), CJIS, Clarksburg, WV. A review of the documents revealed that there were no queries for criminal history (III) for the entire period by any terminal operator on the midnight shift. The only queries made were for lost/stolen access badges, lost computer equipment or test runs on fictional people. (Exhibit 2,3)

On July 12, 2012, TOIG received the written NCIC logs for BEP Central Police Operations Center (CPOC) for the dates August 6, 2010 through May 24, 2012, from Inspector [redacted] BEP, Washington, DC.

On July 18, 2012, TOIG interviewed [redacted], BEP Police. [redacted] is the NCIC coordinator for BEP. [redacted] said that all the terminals are in a secured area and that on the midnight shift, 11 Police Officers have access to the terminals. [redacted] said that when an NCIC III is queried, the terminal operator must enter the reason code, criminal or employment, and enter the name of the requestor, but for running a wants or warrants check (QW), the requestor is not required. [redacted] said that the only reason to run a III query would be for an arrest. He said that BEP Police have an MOU with the MPD regarding enforcement for several blocks surrounding BEP. This allows BEP Police federal and local jurisdiction within that several block radius. Officers requesting a NCIC query either call or radio in to the CPOC and request the

query. [redacted] said that all radio and phone communications with the CPOC are recorded. (Exhibit 4)

On August 10, 2012, TOIG received the WALES logs from [redacted] BEP. The logs are for all queries made by the midnight shift Officers in the CPOC for the last six months. [redacted] requested the information from [redacted], MPD. A review of the WALES logs for each midnight shift Terminal Operator revealed that there were no criminal history queries made during the entire period. The queries are all license plate checks or registration information, which would include wants/warrants. There are no criminal history queries. (Exhibit 5,6)

On September 26, 2012, TOIG interviewed [redacted], BEP. [redacted] is a NCIC and WALES Terminal Operator in BEP's CPOC on the midnight shift. [redacted] said that he has been with BEP for 24 years and has been assigned to the CPOC since approximately 1998. Since that time, he has been a NCIC/WALES Terminal Operator. [redacted] said that on the midnight shift there are about [redacted] people with NCIC/WALES terminal access; [redacted] terminal operators and [redacted] Sergeants.

[redacted] said that everything that he runs is related to traffic stops. He said that nearly everything is run through WALES and not NCIC because it is much easier and user friendly. The Officer on patrol will call in with a tag and he will run the tag for registration information. He said that when that is run, any wants/warrants will also come up on the screen. [redacted] said that he cannot recall ever running a criminal history check, either on NCIC or WALES. He said there is never a reason to run criminal history.

[redacted] said that all queries are automatically archived electronically; therefore, they do not need to keep a log. [redacted] says that there is a log in the CPOC where you can write down the requester and tag information, but it is not required because of the automatic log kept electronically by the computer. [redacted] said that some people keep the written log up to date, but it is not mandatory.

[redacted] said that he has never been asked to run anything that he thought was suspicious and nobody has ever come into the CPOC to ask him directly to run a query. He said that everything is traffic stops or individuals blocking money trucks.

[redacted] said that recently BEP has been assigned to be the Treasury Operations Center for all Treasury agencies requesting NCIC/WALES queries. He said they have been asked by the Internal Revenue Service to run registration information and tag information, but have never been asked to run criminal history. (Exhibit 7)

On September 26, 2012, TOIG interviewed [redacted] [redacted] Corporal, BEP. [redacted] is a NCIC/WALES Terminal Operator in BEP's CPOC on the midnight shift. [redacted] said that he has

been with BEP for 8 years and assigned to the CPOC for approximately the last three. Since that time, he has been a NCIC/WALES Terminal Operator.

[redacted] said that he runs tags through WALES related to traffic stops. He said that he does not recall ever running a criminal history query for any reason since he has been a Terminal Operator.

[redacted] said that he keeps his own notes daily on the back of the daily roster sheet. The roster sheet has the daily assignments for the posts around BEP. He said that if a request is made to run a tag, he will jot down the tag that is run and the start and ending time of the traffic stop on the back of his roster sheet. [redacted] said that the query is automatically logged electronically on the terminal that is being used for the query. [redacted] said that there are typically between 1 to 3 officers out on patrol at a time, 2 cars and 1 bike, and he knows who is calling in. He said that on occasion he will be asked to run wants/warrant information if patrol officers come across somebody on foot that needs to be run, but that is through WALES as a name check.

[redacted] said that he can't recall anybody ever having to run a criminal history. He said that he has never seen an officer come into the CPOC to run somebody or ask to have somebody run. (Exhibit 8)

On October 10, 2012, TOIG interviewed [redacted], BEP. [redacted] said that he has been with BEP for 15 years and assigned to the midnight shift since approximately 2000. [redacted] said that he has never requested a criminal history check. He said that there is no reason to do it. [redacted] said that he knows that people get in a lot of trouble using NCIC/Wales for unofficial reasons and he said that everything an officer does is recorded, both radio traffic and terminal usage. [redacted] said that he used to have NCIC/WALES terminal access when he was assigned to the CPOC, but that was over five years ago and all of his access has expired.

[redacted] said that when on patrol, he requests over the radio to have vehicle tags run and possibly the driver of the vehicle, but only for license information. He said that he will receive wants/warrants information through this type of query, but doesn't need anything else. [redacted] advised he has never asked for a criminal history. [redacted] said that everything he asks for is for traffic stops. He said that the terminal operators run the requested query. The terminal operator depends on who is available and answers his radio call. He said that he goes into the CPOC during his shift, but has not requested that criminal history information be queried.

The allegation suggested that [redacted] was running the boyfriends of his ex-wife to see who was coming in contact with his kids. [redacted] said that he has been divorced for over five years and does not have contact with his ex-wife. He said she is remarried and lives [redacted] He has [redacted] children, ages [redacted], who don't live in the area. (Exhibit 9)

On October 19, 2012, TOIG interviewed [redacted], BEP. [redacted] said that he has been with BEP since 2003 with a break in service from November 2007 to February 2010. From 2003 to 2007, [redacted] said he was assigned to evenings, from early 2007 to November 2007 he was assigned to midnights, then had his break in service, from February 2010 until June 2010 he was assigned evenings, and from June 2010 to present assigned to the day shift and assigned to the CPOC since April 2012.

[redacted] said that he doesn't use NCIC that often, and when he does it is only to enter lost control badge information. He said he has never run a tag or a criminal history through NCIC and has never been asked to run a criminal history. If he needs to run a tag, he said he used WALES because it is easier.

[redacted] said that he doesn't have knowledge of, or ever seen anybody run a criminal history for any reason. He said that he runs tag information through WALES when a patrol officer requests it via radio. [redacted] said that all WALES information is kept in an automated log through WALES and there is no written log.

[redacted] said that there are always at least two people in the CPOC and usually at least three. He said one officer monitors the alarms, one officer maintains the call log, and one officer monitors the fire management system. He said the officers on the alarms and call log usually handle the NCIC/WALES requests.

[redacted] said that he has been married [redacted], most recently [redacted] and has known her since February of 2010. [redacted] said that he has [redacted] children, [redacted] from first wife ([redacted]) who he has full custody, and [redacted] from second wife [redacted]) with whom he has split custody. [redacted] said that he has no issues with his ex-wives or their fiancées, and has no concerns about the safety of his kids with ex-wive's boyfriends or fiancée. (AGENT'S NOTE: questions were only asked because complaint specifically says names were run of ex-wive's boyfriends.) [redacted] said that he has never run, or asked anybody else to run the names of boyfriends of his ex-wives. (Exhibit 10)

Referrals

None

Judicial Action

None

Findings

TOIG's investigation of the misuse of NCIC/WALES by BEP officers [redacted] and [redacted] yielded no evidence that any Officer misused NCIC/WALES; therefore, the allegations are unsubstantiated.

Distribution

[redacted], Product and Physical Safety Division, Office of Security, Bureau of Engraving and Printing.

Signatures

Case Agent:

[redacted]

11/7/12
Date

Supervisor:

[redacted]

11/19/12
Date

Exhibits

1. Complaint document, Letter from Anonymous Complainant, dated May 4, 2012.
2. Memorandum of Activity, Receipt of NCIC user logs, dated June 26, 2012.
3. Memorandum of Activity, Review of NCIC user logs, dated October 23, 2012.
4. Memorandum of Activity, Interview of [redacted] dated July 19, 2012.
5. Memorandum of Activity, Receipt of WALES logs, dated August 23, 2012.
6. Memorandum of Activity, Review of WALES logs, dated October 23, 2012.
7. Memorandum of Activity, Interview of [redacted], dated October 1, 2012.
8. Memorandum of Activity, Interview of [redacted] dated October 1, 2012.
9. Memorandum of Activity, Interview of [redacted] dated October 16, 2012.
10. Memorandum of Activity, Interview of [redacted] dated October 22, 2012.

REPORT OF INVESTIGATION
BPD-11-0590-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case #: BPD-12-0590-I

Case Type: Criminal X
Administrative
Civil

Investigation Initiated: February 25, 2011

Investigation Completed: APR 19 2012

Conducted by: [redacted]
Special Agent

Origin: [redacted]
Bureau of the Public Debt

Approved by: [redacted]
Special Agent in Charge

Summary

On February 25, 2011, the Department of the Treasury Office of Inspector General (TOIG) opened an investigation into [redacted] and [redacted] unsuccessful attempts to fraudulently obtain money from the United Sates through the repeated submission of falsified documents to the Bureau of Public Debt (BPD).

TOIG's investigation coupled with complementary investigations conducted by the Department of Defense (DoD) Office of Inspector General (OIG) and the Department of Energy (DOE) OIG substantiated that [redacted] and [redacted] were attempting to defraud the United States; but no losses had been incurred by the United States. The lack of an actual monetary loss contributed to the declination for prosecution by the United States Attorney's Office (USAO) for the District of Columbia (TOIG's investigation) and the USAO for the Eastern District of Virginia (DoD OIG's investigation).

Basis and Scope of the Investigation

During the course of the investigation, the TOIG interviewed reviewed [redacted] and [redacted] submissions to the FMS and coordinated with DOE OIG and DoD OIG.

Investigative Activity

On February 1, 2011, BPD submitted a report to the TOIG hotline detailing [redacted] repeated attempts to defraud the United States via the submission of fraudulent documents to BPD. (Exhibit 1)

On March 23, 2011, TOIG reviewed the DOE OIG summary of their investigation into [redacted] and [redacted] unsuccessful attempts to fraudulently obtain money from the DOE through the repeated submission of falsified documents. DOE OIG's investigation included consensual telephone calls in which [redacted] and [redacted] claimed to be working for the government under a non-existent contract number. In addition, DOE OIG and DoD OIG executed a search warrant at [redacted] and [redacted] residence and collected evidence in May, 2010. On April 18, 2011, DOE OIG presented their investigation to the USAO for the Middle District of Tennessee. On December 2, 2011 DOE OIG informed TOIG that their investigation had been transferred to a new AUSA and that a decision was expected within a month. (Exhibit 2)

On July 25, 2011, TOIG completed the review of the fraudulent documents submitted by [redacted] to the Treasury Executive Office for Asset Forfeiture (TEOAF), BPD and the Financial Management Service (FMS). The review of the fraudulent documents showed that [redacted] were persistent in their attempts, but the nonsensical, inaccurate, and frequently hand written documents guaranteed that they would be rejected for payment. (Exhibit 3)

On September 17, 2011, DoD OIG contacted TOIG to coordinate each agency's investigation into [redacted] continued attempts to defraud the United States. It was decided that TOIG would concentrate on investigating the Treasury-specific attempts and work with the USAO for the District of Columbia while DoD OIG would work with the USAO for the Eastern District of Virginia and focus on attempts to defraud the DoD and the attempted impersonation of DoD personnel. On March 28, 2012, DoD OIG presented their investigation to USAO for the Eastern District of Virginia which declined to accept the case for prosecution citing the lack of loss to the government.

Referrals

On April 2, 2012, TOIG presented the investigation to the Financial Fraud and Public Corruption section of the USAO for the District of Columbia. Assistant United States Attorney [redacted] declined to accept the case, observing that absent a loss to the government, the case lacked prosecutorial merit. (Exhibit 4 and 5)

Judicial Action

Not Applicaable.

Findings

TOIG's investigation coupled with complementary investigations conducted by the DoD OIG and the DOE OIG substantiated that [redacted] were attempting to defraud the United States but the lack of an actual monetary loss contributed to the cases being declined for prosecution.

Distribution

[redacted], Acting Assistant Commissioner, BPD

Signatures

Case Agent:

[redacted]
Special Agent [redacted]

4/19/2012
Date

Supervisor:

[redacted]
Special Agent in Charge [redacted]

4-19-12
Date

Exhibits

1. BPD E-mail, dated February 1, 2011.
2. Memorandum of Activity, DOE OIG Investigative Summary, dated April 3, 2012.
3. Memorandum of Activity, Fraudulent Document Review, dated July 25, 2011.
4. Memorandum of Activity, Declination [redacted], dated April 2, 2012.
5. Memorandum of Activity, Declination [redacted] dated April 2, 2012.

REPORT OF INVESTIGATION
BPD-12-0650-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
(Non-Employee)

Case #: BPD-12-0650-I

Investigation Initiated: February 9, 2012

Case Type: Criminal X
Administrative ___
Civil ___

Investigation Completed:

Conducted by: [redacted]
Special Agent

Origin: [redacted] Attorney, Foley & Lardner, LLP

Approved by: [redacted]
Special Agent in Charge

Summary

On February 9, 2012, the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), initiated an investigation regarding members of the [redacted] family having trusts that fund the [redacted] foundation, of which an insider appeared to have embezzled monies from one (or more) of the Treasury Direct accounts. Specifically, it is alleged that [redacted] cashed out the bonds into the foundation's business investment account and transferred the funds to the linked checking account where she wrote checks to herself. The amount believed to have been embezzled is approximately $1.85 million. This investigation was conducted jointly with the Federal Bureau of Investigation (FBI) and Winter Garden Police Department (WGPD). (Exhibit 1)

The investigation determined that the allegation was substantiated. On July 24, 2012, [redacted] pled guilty in the U.S. District Court of the Middle District of Florida, to one count of Title 18 USC § 1343 – Wire Fraud and agreed to make full restitution to any victim or the offense, or to the community. On October 17, 2012, [redacted] was sentenced to 55 months incarceration and was ordered to pay restitution in the amount of $1,732,315.

Basis and Scope of the Investigation

On February 9, 2012, TOIG initiated an investigation regarding members of the [redacted] family having trusts that fund the [redacted] foundation, of which an insider appeared to have embezzled monies from one (or more) of the Treasury Direct accounts. Specifically, it is alleged that [redacted] cashed out the bonds into the foundation's business investment account and transferred the funds to the linked checking account where she wrote checks to herself. The amount believed to have been embezzled is approximately $1.85 million. (Exhibit 1)

Treasury Direct is a financial services website provided by the U.S. Department of the Treasury Bureau of Public Debt (BPD). Treasury Direct enables the purchase and redemption of securities directly from the U.S. Department of the Treasury in paperless electronic form. Financial portfolios are managed online and products offered include Treasury securities, from Series EE Savings Bonds to Treasury Notes. Treasury Direct accounts offer Treasury Bills, Notes, Bonds, Inflation-Protected Securities (TIPS), and Series I and EE Savings Bonds in electronic form in one convenient account.

During the course of the investigation, relevant interviews were conducted with:

- [redacted]

Investigative Activity

During a proffer session held at the United States Attorney's Office (USAO) of the Middle District of Florida, [redacted] confessed to the embezzlement exceeding $1 million from Treasury Direct funds in the names of [redacted] 1986 Revocable Trust, as well as the [redacted] 1986 Revocable Trust. When the Treasury notes from these trusts matured, the cash went into bank accounts and [redacted] never reinvested the funds. [redacted] and [redacted] are [redacted].

All of the [redacted] family's bank accounts were with Bank of America. [redacted] was the trustee and the signor on the [redacted] children's bank accounts. In addition to the [redacted] children's trust accounts, there was also an [redacted] 1989 Revocable Trust that [redacted] wrote checks from. [redacted] also had a money market account and a regular checking account. [redacted] took checks from [redacted] bank accounts and signed the checks, though she did not have signature authority to do so with respect to those bank accounts. [redacted] would sign [redacted] signature to the checks. [redacted] also had a personal bank account at Bank of America and [redacted] would do deposits per [redacted] request.

With regard to [redacted] son [redacted], there was somewhere between $160,000.00 and $200,000.00 in treasury notes in the [redacted] 1986 Revocable Trust. The bonds matured, and they went into a Federal Reserve account, called a Treasury Direct Account. [redacted] was the trustee on the account. [redacted] wrote a check from the account, as [redacted] was the signatory on the account. [redacted] actually wrote several checks out of the account and paid her own business expenses. They trusted [redacted] and they never asked her any questions.

[redacted] started with the [redacted] Foundation in 2004 or 2005. The most funds [redacted] took from any account were from the [redacted] Foundation. [redacted] was not part of the [redacted] Foundation, though he was the founder. [redacted] would write checks from the [redacted] Foundation's Bank of America account and she would sign the checks. While two signatures were required on the checks and the [redacted] Foundation would have preferred it to be that way, Bank of America did not recognize two signatures and did not require two signatures. There were six other people from the [redacted] Foundation whose names were on the account. (Exhibit 2)

Referrals

On February 16, 2012, AUSA [redacted] of the USAO Middle District of Florida accepted the case for prosecution.

Judicial Action

On July 24, 2012, [redacted] pled guilty to one count of Title 18 USC § 1343 – Wire Fraud and agreed to make full restitution to any victim or the offense, or to the community. (Exhibit 3)

On October 17, 2012, [redacted] was sentenced to 55 months of incarceration and ordered to pay restitution in the amount of $1,732,315. (Exhibit 4)

Findings

The investigation determined that the allegation was substantiated. On July 24, 2012, [redacted] pled guilty in the U.S. District Court of the Middle District of Florida, to one count of Title 18 USC § 1343 – Wire Fraud and agreed to make full restitution to any victim or the offense, or to the community. On October 17, 2012, [redacted] was sentenced to 55 months incarceration and was ordered to pay restitution in the amount of $1,732,315.

Based on the findings of our investigation, it appears the following pertinent statute(s), regulation(s), and/or policies were violated or could be applied to the case.

- Title 18 U.S.C § 656 – Theft Embezzlement
- Title 18 U.S.C § 1343 – Wire Fraud

Distribution

Signatures

Case Agent:

[redacted] 11/28/12
Date

Supervisor:

[redacted] 12-12-12
Date

Exhibits

1. Lead Initiation Document from [redacted], dated January 30, 2012.
2. Memorandum of Activity, Document Review of FBI 302 from proffer session held with [redacted] dated February 16, 2012.
3. Memorandum of Activity, Judicial Plea entered by [redacted] dated July 24, 2012.
4. Sentencing of [redacted] dated October 17, 2012.

REPORT OF INVESTIGATION
BPD-12-1652-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Bureau of Public Debt
Washington, DC

Case #: BPD-12-1652-I

Case Type: Criminal ___
Administrative X
Civil ___

Conducted by: [redacted]
Special Agent

Investigation Initiated: May 1, 2012

Investigation Completed:

Approved by: [redacted]
Special Agent in Charge

Origin: Bureau of Public Debt

Summary

On May 1, 2012, the U.S. Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG), initiated an investigation based on information received from the Bureau of Public Debt (BPD). The allegation was that [redacted], BPD, had viewed pornographic images, including pornographic videos on his government computer during government time. There was also a sexual harassment allegation that [redacted] made sexual comments to [redacted], Financial Systems Analyst, BPD.

The investigation determined that the allegation regarding [redacted] viewing pornography is substantiated. A TOIG review and analysis of [redacted] government computer found that between March 3, 2011 and April 26, 2012, [redacted] viewed a total of 861 different pornographic images and 9 pornographic videos, which were viewed 13,224 times during this time period. In addition, [redacted] admitted to the viewing of these images during government time.

Additionally, the investigation determined that the sexual harassment allegation was unsubstantiated. Both [redacted] and [redacted] denied that sexual harassment ever occurred.

Basis and Scope of the Investigation

It was alleged that [redacted] viewed pornographic images on his government computer during work hours, in violation of BPD policies.

Treasury Directive 85-01 regarding BPD IT Systems Users, dated January 23, 2006, states the user will, "...not view, send, retain, or reproduce content that is fraudulent, harassing, or obscene in nature."

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted], Management and Program Assistant, BPD
- [redacted], Human Resources, BPD
- [redacted], Human Resources, BPD
- [redacted], Policy and Program Analyst, BPD
- [redacted], Program and Management Analyst, BPD
- [redacted], Financial Management Analyst, BPD

During the course of the investigation, TOIG reviewed pertinent documents, including:

- BPD's regulations regarding use of government computers
- [redacted] Internet history on his government computer

Investigative Activity

In an interview with TOIG, [redacted] and [redacted] stated that they had been sent by BPD to conduct interviews regarding the misuse of a government computer by [redacted]. Specifically, that [redacted] had viewed pornography on his government computer. They had been made aware of the allegation on April 24, 2012, by [redacted] supervisor, [redacted]. [redacted] also told them that she had heard [redacted] made sexual advances to [redacted].

Smith contacted BPD's Information Technology Office and had them conduct a review of [redacted] internet usage from his government computer for April 11, 2012 to April 25, 2012. The review found that [redacted] viewed inappropriate sites 101 times during this time period including "Hornyjock.tumblr.com," "Dickaddict.tumblr.com," and "Hotboysforall.tumblr.com."

[redacted] and [redacted] provided the BPD guidance on government computers which allow "limited personal use" of government computers, but does not allow computers to be used for gambling or to access "sexually oriented or explicit material." They also provided the BPD IT Security Rules of Behavior dated January 23, 2006, signed by [redacted] May 1, 2006, and an ethics orientation form signed by [redacted] March 22, 2004. (Exhibit 2)

In an interview with TOIG, [redacted] stated that she began supervising [redacted] in March 2012. On approximately April 24, 2012, [redacted] Public and Legislative Affair employee, BPD, asked [redacted] if she had heard the allegations that [redacted] was viewing pornography from his government computer. She also heard that [redacted] made sexual comments and 'came on" to

[redacted]. [redacted] stated that [redacted] is "openly gay" and he likes to discuss his relationships to anyone who will listen, but had never heard allegations of him making advances toward an employee before. [redacted] informed [redacted] that she had not heard these allegations. (Exhibit 2)

In an interview with TOIG, [redacted] stated that she has known [redacted] for approximately six years when [redacted] began at the BPD. On approximately April 24, 2012, [redacted] informed her that he heard sexual sounds and language coming from [redacted] computer. [redacted] told [redacted], Administrative Assistant to the Commissioner, who informed [redacted] that BPD management found pornographic material on a computer [redacted] was using in the BPD Auction Room in 2007, and he was counseled. (Exhibit 3)

In an interview with TOIG, [redacted] stated that he has limited work contact with [redacted], but sits in a cubicle next to him. On various occasions, [redacted] has heard sexual sounds like groaning and panting coming from [redacted] cubicle. This would last for a few minutes at a time. One day in mid April 2012 (he could not recall the date), he heard the sounds of moaning and panting, but also heard explicit sexual language. As usual, it lasted a few minutes. He informed coworkers [redacted], and [redacted].

[redacted] stated that [redacted] has never made sexual comments to him, propositioned him, or "come on" to him. (Exhibit 4)

A TOIG cyber analysis of the government computer used by [redacted] found that between March 3, 2011 and April 26, 2012, [redacted] viewed a total of 861 different pornographic images and 9 pornographic videos. These images and videos were viewed 13,224 times during this time period. Most of these images were from the Tumblr.com website. (Exhibit 5)

In an interview with TOIG, [redacted] admitted that he views pornographic images (photos and videos) from his BPD computer during government time several times per week. He stated that he is aware that it is against BPD and government rules and regulations, but he often does not have enough work to do and has free time. He finds these images off of Tumblr.com. He stated that some days he views this site for several minutes, but other days he does not get on the site at all. It depends on his workload. [redacted] stated that he has never viewed child pornography. He apologized for viewing pornography on government time.

[redacted] stated [redacted] advised him that BPD was investigating the allegation of misuse of his computer. He did not deny that he misused his computer during the meeting. However, she stated that there were allegations that he made sexual advances to an employee. He stated to her and to TOIG that he has never "come on" or made sexual advances to any employee. (Exhibit 6)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegation regarding [redacted] viewing pornography is substantiated. A TOIG review and analysis of [redacted] government computer found that between March 3, 2011 and April 26, 2012, [redacted] viewed a total of 861 different pornographic images and 9 pornographic videos, which were viewed 13,224 times during this time period. In addition, [redacted] admitted to the viewing of these images during government time.

Additionally, the investigation determined that the sexual harassment allegation was unsubstantiated. Both [redacted] and [redacted] denied that sexual harassment ever occurred.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policies were violated or could be applied to the case:

- C.F.R. 2635.101 - Basic obligation of public service, misuse of position
- Treasury Directive 85-01 regarding BPD IT Systems Users, dated January 23, 2006
- BPD "Limited Personal Use" of Government Office Equipment (undated)

Distribution

[redacted] (Acting) Assistant Commissioner, Bureau of Public Debt

Signatures

Case Agent:

[redacted] _____ 5-23-12
Date

Supervisor:

[redacted] _____ 5-24-12
Date

Exhibits

1. Memorandum of Activity, Interview of [redacted] and [redacted], dated May 4, 2012.
2. Memorandum of Activity, Interview of [redacted], dated May 4, 2012.
3. Memorandum of Activity, Interview of [redacted], dated May 4, 2012.
4. Memorandum of Activity, Interview of [redacted], dated May 4, 2012.
5. Memorandum of Activity, Cyber Analysis, dated May 10, 2012.
6. Memorandum of Activity, Interview of [redacted] dated May 10, 2012.

REPORT OF INVESTIGATION
BPD-12-2054-I

Office of Inspector General

United States Department of the Treasury

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

= DEC 3 2012

MEMORANDUM FOR DAVID AMBROSE, ACTING CHIEF SECURITY OFFICER, BUREAU OF FISCAL SERVICE

FROM: [redacted] 12-3-12
Special Agent in Charge

SUBJECT: [redacted]
Bureau of Public Debt
Case Number: BPD-12-2054-I

Attached for your review is our Report of Investigation (ROI) into allegations that [redacted] was involved in the possession and distribution of child pornography.

The investigation determined that the allegations are unsubstantiated. The full report and attached documentation are provided to your office for informational purposes only and any attachments that are referenced in the ROI exhibits can be made available upon your request.

If you have any questions concerning this matter, or if you develop information that may indicate a need for additional or new investigative activity to assist you in resolving this matter, please contact me at (202) 927-[redacted]. Staff requests for assistance should be directed to [redacted], Assistant Special Agent in Charge, Mission Support Branch at (202) 927-[redacted].

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Specialist
Bureau of Public Debt

Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: June 25, 2012

Conducted by: [redacted]
Special Agent

Investigation Completed: DEC 3 2012

Approved by: [redacted]
Special Agent in Charge

Origin: [redacted], BPD

Case #: BPD-12-2054-I

Summary

On June 25, 2012, the United States Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), received information from Lead Investigator [redacted], Bureau of Public Debt (BPD), informing TOIG that the West Virginia State Police (WVSP) conducted a search warrant on BPD employee [redacted] residence, based on allegations of the possession and distribution of child pornography. [redacted] is an [redacted] Specialist with BPD. (Exhibit 1)

The investigation determined the allegations are unsubstantiated. The Parkersburg Police Department (PPD) conducted a forensic analysis of the personal items seized during the search warrant on [redacted]' residence. TOIG conducted a forensic analysis of [redacted]' government-issued laptop. Forensic analysis of all the seized items revealed no evidence of child pornography.

Basis and Scope of the Investigation

This case was initiated on June 25, 2012, based upon a referral from Lead Investigator [redacted], BPD, informing TOIG of a search warrant conducted by WVSP on [redacted] residence. The WVSP believed [redacted] was involved in the possession and distribution of child pornography.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted], IT Specialist, BPD

In addition, TOIG reviewed pertinent documents, including:

- West Virginia State Police Report number 0210-[redacted], dated June 1, 2012
- OI Form- 30C (Chain of Custody) for Dell Model D360, service tag [redacted], dated September 5, 2012
- TOIG Cyber Report for [redacted] Government-issued Laptop, dated September 11, 2012
- OI Form-27 (Advice of Rights – Beckwith/Garrity) for [redacted], dated October 16, 2012
- OI Form- 13 (Personal History Information) for [redacted], dated October 16, 2012

Investigative Activity

On June 25, 2012, TOIG obtained BPD laptop, Dell Model D630, service tag [redacted], from Detective [redacted] PPD. The BPD laptop was obtained during a search warrant executed by the WVSP on [redacted] residence. The WVSP seized several electronic media items including [redacted] government-issued laptop during the execution of the search warrant. PPD requested TOIG's assistance with decrypting, analyzing and imaging [redacted] government-issued laptop. (Exhibit 2)

On September 11, 2012, TOIG analyzed a copy of the original hard drive found in [redacted] government-issued laptop. The analysis did not find any evidence of child pornography, and minimal evidence was found indicating that [redacted] used the laptop for any significant amount of time. (Exhibit 3)

On October 15, 2012, TOIG received WVSP Complaint Report number 0210-[redacted] regarding [redacted]. According to the report, the PPD conducted a search of the Internet Crimes Against Children (ICAC) database for Internet Protocol (IP) addresses, that were previously identified as being involved in the possession and distribution of digital media files involving child pornography. The search resulted in the identification of [redacted] IP address. The report stated that [redacted] IP address was involved in the possession and distribution of one hundred and nineteen unique digital media files involving child pornography from November 11, 2011 through December 6, 2011. The report stated that on April 6, 2012, Suddenlink Communications replied to a WVSP Administrative subpoena for subscriber information for IP address [redacted]. The results identified the IP address [redacted] belonged to [redacted] at [redacted]. The report also included the negative results for evidence of child pornography for [redacted] forensic exams on the other seized items. (Exhibit 4)

On October 16, 2012, TOIG interviewed [redacted]. [redacted] confirmed that the WVSP conducted a search warrant on his residence in June 2012. During the search warrant [redacted] was questioned regarding his alleged possession and distribution of child pornography. [redacted] said

the WVSP seized several electronic devices including computers, cell phones, compact disks (CDs), and a Universal Serial Bus (USB) hub. [redacted] noted that the WVSP did not seize all electronic devices in the residence. [redacted] said the next time he spoke with or saw the WVSP was when they returned his belongings, stating that they found no evidence of child pornography. [redacted] advised he was on annual leave from BPD during the period the child pornography was downloaded and distributed. The dates ranged from November 11, 2011 through December 6, 2011.

[redacted] said his home network is password protected with a Wired Equivalent Privacy (WEP) encryption. In addition, [redacted] informed TOIG that he has multiple private networks at his residence. One network connects his computer devices including [redacted] personal computer, iPhone, and iPad. The other network is set up for internet access only. [redacted] advised he only connected his government- issued laptop to his home network twice to confirm the connection. [redacted] noted that the dates on the affidavit presented to him by the WVSP, regarding the subpoena for IP subscriber information, did not correlate with the dates the alleged activity took place. The affidavit listed the dates for the subpoena as March 3, 2012 through March 27, 2012. (Exhibit 5)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegations are unsubstantiated. No evidence was found on any of the digital media seized by the WVSP.

Distribution

[redacted], Acting Chief Security Officer, BFS

Signatures

Case Agent:

[redacted] 11/2/2012
Date

Supervisor:

[redacted] 11/28/12
Date

Exhibits

Number	Description
1.	Original Allegation, Correspondence from [redacted], dated June 22, 2012.
2.	Memorandum of Activity, Evidence Obtained from Parkersburg Police Department, dated June 22, 2012.
3.	Memorandum of Activity, Forensic Analysis of [redacted] Laptop, dated September 11, 2012.
4.	Memorandum of Activity, Record Review of West Virginia State Police Report number 0210-[redacted], dated October 15, 2012.
5.	Memorandum of Activity, Interview of [redacted] dated October 16, 2012.

REPORT OF INVESTIGATION
BPD-12-2069-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Parkersburg, WV
Bureau of Public Debt

Case #: BPD-12-2069-I
Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: June 27, 2012

Investigation Completed: AUG 14 2012

Conducted by: [redacted]
Special Agent

Approved by: [redacted]
Special Agent in Charge

Origin: [redacted], Lead Investigator,
Bureau of Public Debt

Summary

On June 25, 2012, a complaint was received by the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG) from [redacted], Lead Investigator, Bureau of Public Debt (BPD), alleging that [redacted] Specialist, BPD made unwanted sexual advances toward [redacted] Specialist, BPD, on three occasions during official travel. (Exhibit 1)

The investigation determined that the allegations are unsubstantiated. There was no evidence discovered that corroborated [redacted] made unwanted sexual advances toward [redacted]. [redacted] denied making any unwanted sexual advances toward [redacted] and stated the two shared several kisses that were consensual. [redacted] reiterated that [redacted] made unwanted sexual advances toward her. TOIG advised [redacted] to file an Equal Employment Opportunity Commission (EEOC) complaint if she believed she was a victim of sexual harassment.

Basis and Scope of the Investigation

On June 25, 2012, a complaint was received by TOIG from [redacted], alleging [redacted], made unwanted sexual advances toward [redacted], on three occasions during official travel to Washington, DC. (Exhibit 1)

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Fiscal Services, BPD
- [redacted] Specialist, BPD
- [redacted] Specialist, BPD
- [redacted] Specialist, BPD
- [redacted] Specialist, BPD
- [redacted] Specialist, BPD

In addition, TOIG reviewed pertinent documents, including:

- Sensitive but Unclassified report, prepared by [redacted] in regard to the allegation of [redacted] making unwanted sexual advances toward [redacted] on work travel, dated June 26, 2012.

Investigative Activity

In an interview with TOIG, [redacted] stated he has supervised [redacted] and [redacted] since November 2011. [redacted] and [redacted] are both IT Specialists who work on the same team and traveled often together for work. [redacted] stated he only observed a professional working relationship between [redacted] and [redacted] and never witnessed anything inappropriate between the two. [redacted] was unaware if the two had any contact outside of work.

On March 16, 2012, [redacted] received an e-mail from [redacted] in regard to her telework schedule and a request to work solely with [redacted] and no longer with [redacted]. [redacted] continued to explain her reasoning for wanting to work solely with [redacted] was due to [redacted] behaving inappropriately toward her on past work trips together. [redacted] did not explain any further details in the e-mail. [redacted] never requested to be re-assigned before making the allegation. [redacted] told [redacted] she did not want to cause any problems by making the allegation and only wanted to work with [redacted] and no longer work with [redacted].

[redacted] called [redacted] and the EEOC immediately. [redacted] did not want to make an EEOC complaint or take any other action against [redacted]. [redacted] received EEOC guidance from [redacted] who informed [redacted] that unless [redacted] made a complaint with EEOC, no documentation or investigation would be done by EEOC. Also, [redacted] contacted [redacted]

at Franchise Labor and Employee Relations Branch (FLERB) who took over the situation around March 20, 2012 along with BPD investigator, [redacted].

On March 16, 2012, [redacted] re-assigned [redacted] and to the present she has not traveled or worked directly with [redacted]. [redacted] stated currently both employees have little to no interaction at work. Since [redacted] was reassigned, [redacted] has not received any further complaints. [redacted] stated a conversation with the team in February 2012, revealed that multiple team members believed [redacted] was not pulling her weight on the team. (Exhibit 2)

In an interview with TOIG, [redacted] stated he was assigned to a 6-month temporary team lead in March 2011. [redacted] lead a team of four other [redacted], and [redacted]. Prior to [redacted] leading the team, [redacted] was the team lead for 6 months from September 2010 to March 2011. [redacted] was not aware of any issues, sexual or otherwise, between [redacted] and [redacted] and was unaware of the allegation. (Exhibit 3)

In an interview with TOIG, [redacted] stated he was Lead IT Specialist of the team including [redacted], [redacted], and [redacted] until November 2011. Throughout his time as team lead, [redacted] traveled with [redacted] extensively on business trips and once with [redacted] and [redacted] in October 2011. [redacted] stated [redacted] was ill throughout this trip. [redacted] did not witness any issues between [redacted] and [redacted], sexual or otherwise, on the trip or in the office. [redacted] was surprised to hear about the allegation and is unaware of any inappropriate behavior between [redacted] and [redacted] throughout the time he has worked with them on the team. (Exhibit 4)

In an interview with TOIG, [redacted] stated he is a team member of [redacted] and [redacted] and has worked with both throughout the last two years. [redacted] has worked and traveled with [redacted] and [redacted] on several occasions for work and has never witnessed any sexual or otherwise inappropriate behavior between them.

On a work trip to Washington, DC in May 2011, [redacted] witnessed [redacted] give [redacted] a ride on his back while sightseeing and [redacted] sitting on [redacted] lap in a taxi. [redacted] never witnessed any other physical contact between [redacted] and [redacted] while on work travel or at the office. (Exhibit 5)

In an interview with TOIG, [redacted] stated she did not want to make a big deal out of the allegation and she solely wanted to be reassigned from traveling with [redacted]. [redacted] began working in the Office of [redacted] in January 2011 and had a good working relationship with [redacted].

In May 2011, [redacted] and [redacted] traveled to Washington, DC for a work trip along with coworkers [redacted] and [redacted]. The teammates drank at a happy hour at their Embassy Suites hotel and proceeded to go sightseeing. [redacted] gave [redacted] a ride on his back while sightseeing. When asked by TOIG about the taxi ride [redacted] took with [redacted] and the

other teammates, [redacted] stated she was intoxicated and did not remember the taxi ride or sitting on [redacted] lap in the taxi. The sightseeing group split up and [redacted] and [redacted] were left alone when [redacted] stated [redacted] kissed her outside of a hotel, of which [redacted] did not recall the name because she was intoxicated. [redacted] stated the kiss was not mutual and [redacted] apologized. [redacted] and [redacted] continued to walk back to their hotel and discussed [redacted] marital problems.

[redacted] permitted [redacted] into her hotel room to continue to discuss [redacted] marital problems because she felt bad for him. Once in the room, [redacted] stated [redacted] kissed her again and continued to attempt to convince her to pursue a sexual relationship with him. [redacted] stated [redacted] climbed on top of her and she told him she was not interested, but she did not resist or fight for fear of the situation escalating. [redacted] eventually left after [redacted] kept insisting he do so, and the two did not have sexual relations that evening.

During the same trip in May 2011, the team was working in [redacted] room and when left alone, [redacted] stated [redacted] pushed her up against a wall and proceeded to kiss her when [redacted] re-entered the room, [redacted] backed off. [redacted] stated [redacted] did not see the situation. Upon return from Washington, DC, [redacted] and [redacted] resumed their working relationship and continued on as though the situation had never occurred. [redacted] did not make a complaint because she believed the situation was resolved and did not want to cause problems at work.

During a work trip in October 2011, [redacted], [redacted], and [redacted] traveled back to Washington, DC. [redacted] was sick throughout the trip and returned to the hotel before [redacted] and [redacted] on the first day of travel. [redacted] continued to feel sick on the second day and stayed at the hotel while [redacted] and [redacted] worked. After completing work on the second day, [redacted] came to [redacted] room to check on her and [redacted] stated [redacted] felt her head and [redacted] told her she was very hot and should take off her shirt to cool down. [redacted] refused to take her shirt off and [redacted] continued to attempt to take [redacted] shirt off until [redacted] ran to the bathroom saying she was going to be sick and locked herself in the bathroom until [redacted] left approximately 15 minutes later. The next day, the team finished their job and returned to Parkersburg, WV. [redacted] and [redacted] never discussed the incident and [redacted] did not report it because she did not want to get [redacted] in trouble and still liked him as a friend and coworker.

[redacted] stated [redacted] never displayed unwanted sexual behavior toward her while in the office or after the trip in October 2011. [redacted] stated she has never had sexual relations with [redacted]. [redacted] called [redacted] to pick her up after her car had a flat tire in February 2012 and the two continued to act like prior unwanted sexual behavior on work trips in the past did not occur.

In February 2012, [redacted] complained to supervisors that [redacted] was responsible for a project being messed up. [redacted] requested that her supervisor reassign her to travel solely with [redacted] in March 2012, because of how differently [redacted] behavior toward her was on work travel and to avoid future inappropriate unwanted sexual behavior from [redacted]. [redacted] stated she did not want to be discriminated against and/or retaliated against for filing a complaint and she also did not want to lose her job over it. (Exhibit 6)

In an interview with TOIG, [redacted] stated he had a working relationship with [redacted] with mutual playful flirting at the office. [redacted] stated he has worked on a team with [redacted] since 2011, and traveled with [redacted] to Washington, DC three times for work trips.

In May 2011, [redacted] and [redacted] traveled to Washington, DC for a work trip along with coworkers [redacted] and [redacted]. The teammates drank at a happy hour at their Embassy Suites hotel and proceeded to go sightseeing. [redacted] gave [redacted] a ride on his back while sightseeing and [redacted] sat on [redacted] lap in a taxi cab with the other teammates. [redacted] stated he and [redacted] got split up from the group after the taxi ride and the two were alone for the remainder of the night. [redacted] stated there was mutual flirting on the same night followed by a first kiss that led to consensual kissing throughout the evening while walking in Washington, DC and when [redacted] and [redacted] returned to [redacted] hotel room alone.

[redacted] stated [redacted] told him to stop kissing her once back in her room and he stopped and returned to his room. [redacted] stated he never held down [redacted] or climbed on top of her in her hotel room. [redacted] stated there were no additional intimate moments between the two on the first trip to Washington, DC or the remaining two trips. [redacted] and [redacted] never discussed their kissing on the first trip once they returned to the office. [redacted] and [redacted] remained teammates with a good working relationship after the first trip to Washington, DC in May 2011.

[redacted] stated he never forced himself on [redacted] and that he also never made any advances toward her following the trip to Washington, DC in May 2011. [redacted] stated he never had a sexual relationship with [redacted] and the multiple occurrences of kissing on the work trip to DC in May 2011 were the only intimate relations they ever shared. [redacted] stated the only outside of work activity he has had with [redacted] was in February 2012 when [redacted] called [redacted] to pick her up after her car had a flat tire.

In February 2012, [redacted] complained to the team's supervisor, [redacted], that [redacted] was not pulling her share of the work on the team. [redacted] spoke with [redacted] and [redacted] is unsure if [redacted] holds the complaint against her. (Exhibit 7)

A TOIG review of documentation regarding the BPD investigation conducted by [redacted] revealed the following:

This report contains statements from several employees and other documents associated the [redacted] allegation of improper behavior from [redacted] while on government travel including:

- Copy of [redacted] E-mail to her manager, [redacted], requesting reassignment, dated March 16, 2012.
- Statement from [redacted] dated June 21, 2012.
- Statements from [redacted], dated April 27, 2012 and June 20, 2012.
- Statements from [redacted], dated March 27, 2012 and June 19, 2012.
- Statement from [redacted], dated June 25, 2012.
- Statement from [redacted], dated June 20, 2012.

[redacted] concluded that there were no independently verified statements or evidence for either [redacted] or [redacted]. The biggest discrepancy between [redacted] and [redacted] statements were the extent of kissing and flirting that was consensual. (Exhibit 8)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegations are unsubstantiated. There was no evidence discovered that corroborated [redacted] made unwanted sexual advances toward [redacted]. [redacted] denied making any unwanted sexual advances toward [redacted] and stated the two shared several kisses that were consensual. [redacted] reiterated that [redacted] made unwanted sexual advances toward her. TOIG advised [redacted] to file an EEOC complaint if she believed she was a victim of sexual harassment.

Distribution

[redacted], (Acting) Assistant Commissioner, Bureau of the Public Debt

Signatures

Case Agent:

[redacted]

8/14/12
Date

Supervisor:

[redacted]

8-14-12
Date

Exhibits

1. Complaint received by TOIG, dated June 25, 2012.
2. Memorandum of Activity, Interview of [redacted], dated July 6, 2012.
3. Memorandum of Activity, Interview of [redacted], dated July 9, 2012.
4. Memorandum of Activity, Interview of [redacted], dated July 9, 2012.
5. Memorandum of Activity, Interview of [redacted], dated July 10, 2012.
6. Memorandum of Activity, Interview of [redacted], dated July 10, 2012.
7. Memorandum of Activity, Interview of [redacted], dated July 10, 2012.
8. Memorandum of Activity, Document review of case synopsis provided by [redacted], dated June 6, 2012.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 16, 2012

MEMORANDUM FOR THE OFFICE OF INVESTIGATIONS

FROM: [redacted] 10/22/12
Special Agent in Charge

SUBJECT: Notification of Preliminary Inquiry Closure

OIG Project Number: CFIF-12-0024-I

In August 2010, the Office of Investigations (OI) embarked on an initiative surrounding fraud related to the Check Forgery Insurance Fund (CFIF). The CFIF is managed by the Financial Management Service (FMS) and creates a mechanism for FMS to send victim payees replacement checks related to suspected fraud. As such OI receives information from FMS monthly related to the investigative leads involving CFIF. OI will open a case number in the case management system to allow agents to utilize it for case development, and to document agent activities.

In December 2011, TOIG opened an investigative case number for Fiscal Year (FY) 2011 to allow agents to utilize for case development and to document agent activities in relation to the initiative. TOIG has received more than 62,000 potential leads concerning fraud related to the CFIF. A number of the leads conducted to date have been converted into active investigations with many leading to the prosecution and conviction of the subjects involved and restitution being ordered to repay the U.S. Treasury or victim financial institution.

Therefore, with the ending of FY 2012, it is recommended that with the approval of this memorandum, this project be administratively closed and a new project initiative to document agent activities and case development will be opened for FY 2013.

REPORT OF INVESTIGATION
DO-11-0536-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case #: DO-11-0536-I
Case Type: Criminal X
Administrative ____
Civil ____

Conducted by: [redacted],
Special Agent

Approved by: [redacted],
Special Agent in Charge

Investigation Initiated: January 24, 2011

Investigation Completed: JUN 06 2012

Origin: Regus, Inc.

Summary

On January 19, 2011, the U.S. Department of Treasury (Treasury), Office of Inspector General (TOIG) received information from Regus, a local Washington D.C. business that leases office space and support services that they were the victims of fraud. Regus rented office space and support services to [redacted] and his company [redacted]. [redacted] entered into an agreement for services by representing himself as being on the General Services Administration's (GSA) Multiple Award Schedule as well as receiving funding from Treasury. The complainant also reported this matter to the GSA, Office of Inspector General (GSA/OIG) and the Washington Metropolitan Police Department (MPD) and was conducted jointly with these agencies. (Exhibit 1)

The investigation determined that the allegations are substantiated. On October 20, 2010, [redacted] entered into a one year lease with Regus verbally providing the GSA/Treasury information to Regus. [redacted] did not provide any written documentation which enabled him to avoid paying a security deposit of $21,800 that Regus waived because of his alleged affiliation with GSA and Treasury. [redacted] did not pay any rent during the period of occupancy and Regus estimated they lost over $66,000 for services rendered prior to [redacted] eviction. Additionally, [redacted] defrauded a security guard company retained to provide services at the leased office space for over $18,000. [redacted] also purchased large orders of supplies and equipment through Staples for the leased facilities totaling $9,543.

On March 10, 2011, an arrest warrant was obtained charging [redacted] with First Degree Theft. On March 22, 2011, [redacted] surrendered to local authorities. On April 10, 2012, the United States Attorney's Office (USAO), Washington, DC notified TOIG the case was dismissed.

Basis and Scope of the Investigation

This investigation was initiated on January 24, 2011, based upon information that [redacted] defrauded a local business by claiming he was on the GSA Multiple Award Schedule and his company was receiving funding from Treasury.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Center Manager, Regus
- [redacted], Deputy Director, Treasury Office of the Procurement Executive
- [redacted] Director, Treasury, Real Estate Management
- [redacted], Office of Security, Staples Inc.
- [redacted], Owner, S & K Security

In addition, TOIG reviewed pertinent documents, including:

- GSA Databases
- Regus Business Records
- Staples, Inc. Business Records

Investigative Activity

In an interview with TOIG, Ball stated in October 2010, [redacted] came to Regus to lease office space and support services at [redacted] Washington, D.C. [redacted] stated his company was known as [redacted] and was involved with health care programs involving elementary through high school children. [redacted] signed a one year office service agreement. The agreement was for three rooms, ten telephones, and parking. During the meeting, [redacted] stated he was working with Treasury and GSA regarding payment for the office space. [redacted] verbally provided a GSA/ Treasury "P.O." number, [redacted] but did not provide any written documentation of proof. Regus was under the assumption [redacted] had a government contract so they did not charge [redacted] for a security deposit of $21,800.00 ($10,900 monthly rent x's 2). (Exhibit 2)

In an interview with TOIG, [redacted] stated there was no record of Treasury P.O. [redacted] or a contract issued to [redacted] or [redacted]. (Exhibit 3)

GSA databases searched by GSA/OIG did not identify any records, company information or payments to [redacted] or [redacted]. (Exhibit 4)

In an interview with TOIG, [redacted] stated her office coordinates the acquisition of property for anyone with Treasury and she had never heard of [redacted] or [redacted]. (Exhibit 5)

In an interview with TOIG, [redacted] stated from approximately November 29, 2010 through January 6, 2011, he provided security services for [redacted] at the Pennsylvania Ave. location. [redacted] recalled [redacted] stating he either had a Federal grant or was obtaining funding from a grant program

under the President's Health Care Program. [redacted] was never paid and is owed over $18,000. (Exhibit 6)

In an interview with GSA, [redacted] stated Staples shipped $9,543 in supplies and equipment to the Washington, D.C. address for [redacted] Health Care Administration from November 4, 2010 through December 21, 2010 and their account had an outstanding balance of $21, 798. (Exhibit 7)

Referrals

On February 25, 2011, the facts of the joint investigation were presented to Assistant United States Attorney (AUSA) [redacted], USAO, Washington, D.C.

Judicial Action

On March 10, 2011, an Arrest Warrant was obtained for [redacted] for violation of First Degree Theft, 22 D.C. Code; Section 3211 and 3212 (a). (Exhibit 8)

On March 22, 2011, [redacted] surrendered to MPD. (Exhibit 9)

On April 10, 2012, AUSA [redacted] notified TOIG the charges were dismissed in Superior Court. AUSA [redacted] explained their office made a decision that based upon the strengths and weaknesses the case could not justify the large amount of resources necessary to indict and try the case. (Exhibit10)

Findings

The investigation determined that the allegations are substantiated. On October 20, 2010, [redacted] entered into a one year lease with Regus verbally providing the GSA/Treasury information to Regus. [redacted] did not provide any written documentation which enabled him to avoid paying a security deposit of $21,800 that Regus waived because of his alleged affiliation with GSA and Treasury. [redacted] did not pay any rent during the period of occupancy and Regus estimated they lost over $66,000 for services rendered prior to [redacted] eviction. Additionally, [redacted] defrauded a security guard company retained to provide services at the leased office space for over $18,000. [redacted] also purchased large orders of supplies and equipment through Staples for the leased facilities totaling $9,543.

On March 10, 2011, an arrest warrant was obtained charging [redacted] with First Degree Theft. On March 22, 2011, [redacted] surrendered to local authorities. On April 10, 2012, the USAO, Washington, DC notified TOIG the case was dismissed.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policies were violated or could be applied to the case:

- First Degree Theft, District of Columbia Code, Section 22-3211, 22-3212 (a).

Distribution

N/A

Signatures

Case Agent:

[redacted]

[redacted]

6/4/2012
Date

Supervisor:

[redacted]

6-4-12
Date

Exhibits

1. Initial Complaint document, dated January 19, 2011.
2. Memorandum of Activity, Interview of [redacted] dated January 25, 2011.
3. Memorandum of Activity, Interview of [redacted], dated January 25, 2011.
4. Memorandum of Activity, Document review of GSA Database Searches, dated January 25, 2011.
5. Memorandum of Activity, Interview of [redacted], dated January 31, 2011.
6. Memorandum of Activity, Interview of [redacted], dated February 2, 2011.
7. Memorandum of Activity, Interview of [redacted], dated February 8, 2011.
8. Memorandum of Activity, Arrest Warrant and Affidavit for Arrest Warrant, dated March 11, 2011.
9. Memorandum of Activity, Interview of [redacted], dated March 22, 2011.
10. Memorandum of Activity, Interview of [redacted], dated April 10, 2012.

REPORT OF INVESTIGATION
DO-11-1241-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: Treasury Securities Breach

Case #: DO-11-1241

Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: July 6, 2011

Investigation Completed: OCT 22 2012

Conducted by: [redacted]
Special Agent

Origin: Federal Bureau of Investigation

Approved by: [redacted]
Special Agent in Charge

Summary

On June 28, 2011, The Department of Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG) received information from the Federal Bureau of Investigation (FBI) concerning an espionage investigation potentially involving Treasury securities. The FBI investigation involved individuals leaking economic data from "lockdown rooms." This information was leaked to news media outlet, Need To Know News, owned by [redacted], where once reported, people traded securities based on the leaks. It was believed that individuals were attempting to obtain sensitive U.S. economic data for malicious and/or fraudulent purposes. In addition, there were numerous potential subjects that sought employment with various Government agencies to potentially gain access to this sensitive data. This investigation was worked jointly with the OIG's for the U.S. Departments of Commerce, Labor, Agriculture, and the FBI. (Exhibit 1)

The investigation determined the allegations are unsubstantiated. There were five individuals who had accounts in Career Connector; however, only [redacted] applied for positions with Treasury. [redacted] was not hired by Treasury. Furthermore, the Treasury lockdown room was rarely utilized other than once a quarter when the Federal Reserve Board of Governors (FRB) issued their Federal Open Market Committee (FOMC) report. None of the press personnel with access to the Treasury "lockdown room" were affiliated with Need to Know News, nor other [redacted] affiliated companies.

Basis and Scope of the Investigation

The FBI investigation involved individuals leaking economic data from "lockdown rooms." This information was leaked to news media outlet, Need To Know News, owned by [redacted], where once reported, people traded securities based on the leaks. It was believed that individuals were attempting to obtain sensitive U.S. economic data for malicious and/or fraudulent purposes. In addition, there were numerous potential subjects that sought employment with various Government agencies to potentially gain access to this sensitive data. The Treasury "lockdown room" is the Treasury Press Room which allows members of news organizations assigned to report on Treasury activities, a place to work.

When the lockdown is in effect at Treasury, there is at least one person who oversees the room. Members of the press are told what time they can file their story and when the time elapses the lockdown is over. Unlike other Government agencies, there are no securities trading issues, only Federal news issues.

Career Connector, an online hiring system that is part of the Office of Personnel Management's (OPM), USAJobs Website, allows individuals to create accounts to store resumes and other hiring documentation, in order to apply for Federal government job vacancies. The Bureau of Public Debt (BPD) is contracted to handle the Human Resources components for the majority of Treasury, therefore having access to Career Connector.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted], Special Agent, FBI
- [redacted], Special Agent, Office of Personnel Management, OIG
- [redacted], Senior Advisor for Public Affairs, Treasury
- [redacted], Senior Advisor for Public Affairs, Treasury

In addition, TOIG reviewed pertinent documents, including:

- Job Announcements, Applications and Resumes of [redacted] obtained from BPD
- Spreadsheets with names of [redacted] Employees provided by the FBI
- Spreadsheets with names and employers of Press Personnel with access to Treasury Lockdown Room

Investigative Activity

A TOIG review of job application documents obtained from the BPD in connection to their queries of potential suspects: [redacted]; revealed that only [redacted] applied for Treasury positions. [redacted] applied for the following positions with Treasury: [redacted]

[redacted]. [redacted] was found to be qualified; however, [redacted] was not hired for any of the three positions. (Exhibit 2)

In an interview with TOIG, Special Agent [redacted] stated as a result of her queries in OPM Databases on [redacted] who had account profiles in Career Connector, only [redacted] had applications with the Treasury. (Exhibit 3)

In an interview with TOIG, [redacted] stated the Treasury lockdown room is located within the Press Room of the Main Treasury building on the first floor. The lockdown room does not operate like many of the other Federal agencies similar rooms. The lockdown room is utilized quarterly and is used when the FRB issues their FOMC report on interest rate changes. The FOMC report does not contain trading issues, only federal news issues. [redacted] further explained the FRB will fax over their report for distribution to the press; however, FRB will hold their press conference at their office. The lockdown room is rarely utilized for other than the quarterly report. (Exhibit 4)

In an interview with TOIG, [redacted] provided the procedures for the Treasury lockdown room and the list of press personnel who have access to the Treasury Press Room. [redacted] stated Treasury does not have formal lockdown procedures for the public release of economic or financial information. Information is provided to the reporters in the Treasury press room of the under embargo, with the embargo lasting 30 minutes to one hour. Treasury does not take any technological steps to block outside communications or bar reporters from exiting the press room. A member of the Treasury press staff oversees the embargo period for the FOMC statement by: (1) shutting the exit of the Treasury press room (though phone and communications are not blocked through any technological means); (2) counting down the embargo (e.g. "five-minutes left," "four minutes left,"), and (3) ringing a large bell when the embargo is lifted and reporters can file their stories. One-minute before the embargo lifts, reporters are permitted to open their telephone lines and speak with their producers and editors, but are not permitted to file their stories until the bell rings. (Exhibit 5)

A TOIG review of the Treasury Press Room personnel, determined that none of the 39 names of the press personnel who have access to the Treasury Lockdown room were on the master list of [redacted] associated individuals provided by the FBI. (Exhibit 6)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined the allegations are unsubstantiated. There were five individuals who had accounts in Career Connector; however, only [redacted] applied for positions with Treasury. [redacted] was not hired by Treasury. Furthermore, the Treasury lockdown room was rarely utilized other than once a quarter when the FRB of Governors issued their FOMC report. None of the press personnel with access to the Treasury "lockdown room" were affiliated with Need to Know News, nor other [redacted] affiliated companies.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policy(ies) were violated or could be applied to the case:

- N/A

Distribution

N/A

Signatures

Case Agent:

[redacted] 10/19/2012
Date

Supervisor:

[redacted] 10/19/12
Date

Exhibits

1. Initial Complaint document, dated June 28, 2011.
2. Memorandum of Activity, Document Review, [redacted] for Employment, dated July 27, 2011.
3. Memorandum of Activity, Interview of [redacted] dated August 2, 2011.
4. Memorandum of Activity, Interview of [redacted] dated November 9, 2011.
5. Memorandum of Activity, Interview of [redacted] dated February 28, 2012.
6. Memorandum of Activity, Document Review, Press Personnel Assigned to Treasury Press Room, dated March 6, 2012.

REPORT OF INVESTIGATION
DO-11-1411-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case Type: Criminal X
Administrative ____
Civil ____

Investigation Initiated: July 28, 2011

Investigation Completed: FEB 17 2012

Conducted by: [redacted]
Special Agent

Origin: Treasury Inspector General for Tax Administration (TIGTA)

Approved by: [redacted]
Special Agent in Charge

Case #: DO-11-1411-I

Summary

A preliminary inquiry was initiated by the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), after receiving information from the U.S. Attorney's Office (USAO) and the Treasury Inspector General for Tax Administration (TIGTA), Miami, FL on July 28, 2011 that [redacted] Sr. of Vero Beach, FL had represented that he was a Treasury Special Agent. [redacted] told the U.S. Attorney's secretary that he needed to meet with the U.S. Attorney and give him some documents. [redacted] entered the building and provided a business card which described him as being employed by the "U.S.Treasury, Federal Notary Agency" and his title as a Special Agent.

Subsequent investigation by the TOIG and TIGTA determined that [redacted] did attempt to gain access to the U.S. Attorney in Miami to pass a report he had written regarding a special operation that he said he had been involved in for the past 20 years and which was to be given to Secretary of State Hillary Rodham Clinton. [redacted] denied any mental diagnoses or issues.

The USAO declined criminal prosecution of [redacted] on January 5, 2012.

Basis and Scope of the Investigation

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted]
- SA [redacted], Treasury Inspector General for Tax Administration (TIGTA)
- [redacted], [redacted] spouse
- [redacted] [redacted] physician
- [redacted] landlord
- [redacted] brother

In addition, TOIG reviewed pertinent documents, including:

- Court Facility Incident Report, U.S. Attorney's Office, Miami, FL
- Written statements of Court Security Officers
- Documents provided by [redacted] Sr.
- Incident reports

Investigative Activity

On July 29, 2011, TIGTA advised the TOIG that it had received a complaint regarding [redacted] who allegedly impersonated a U.S. Treasury Agent. [redacted] had contacted the U.S. Attorney's Office in Miami, FL and advised the USAO's secretary that he was a Treasury agent and needed to meet with him and give him some documents. [redacted] entered the building and provided a business card which stated "U.S. Treasury, Federal Notary Agency" and his title as "Special Agent". The USAO contacted TIGTA's field office in Miami and requested that it interview [redacted] (Exhibit 1)

On August 1, 2011, the TOIG and TIGTA interviewed [redacted] [redacted] stated that he had dropped off a document at the USAO in Miami on July 28, 2011. The document was a report regarding a special operation that he has been involved in for the past 20 years. The report concerned financial threats to the U.S. economy and how to address the threats. The report was addressed to U.S. Secretary of State Hillary Rodham Clinton. He told interviewing agents that he works under the direction of the State Department and operates under encrypted codes. (Exhibit 2)

He also told interviewing agents that he does not file tax returns, he goes by the title of "Commander" and the name of the operation is "Silver Eagle". [redacted] showed agents a business card which described his position as a "Special Agent".

[redacted] could not describe how the codes are passed to him or the last time he received codes from the government. He said he worked with the IRS in 1985 in Nevada in a secret investigation. He said he served in the Navy from 1960 to 1963 and was discharged as "undesirable". He did not have a Form DD-214. [redacted] said he is ill and dying and would like to complete his operation for the U.S. government.

[redacted] denied any mental diagnoses or issues. He said he is being treated for throat cancer and had three quarters of his stomach removed. He works in his home studio producing ceramics. Though he said he has not paid income taxes, [redacted] asserted the IRS will not touch him. He said he met with the Secret Service in Washington, DC last summer. He used the code name "Silver Eagle" to get access into the Secret Service. He did not have any credentials or identification other than his business card and the report which he had delivered to the USAO in Miami.

[redacted] was also questioned and confirmed that [redacted] works for the State Department in an undercover capacity. She said she has assisted [redacted] in conducting investigations for the government over the past 20 years.

On August 1, 2011, the TOIG interviewed telephonically [redacted] landlord. [redacted] told the TOIG that [redacted] has lived at his property for three years and has told him "bizarre" things over the years but did not note any mental issues or behavior by [redacted] He said he works in the house doing artwork.

[redacted] had told him that he had written financial policy for the Federal government. He told [redacted] that he was an admiral in the Navy. (Exhibit 3).

On August 4, 2011, the TOIG interviewed [redacted] was [redacted] internist who had treated him for a stomach infection in 2008. [redacted] told TOIG that he had treated [redacted] for a period of four years and had come to know [redacted] and his wife. [redacted] said [redacted] had contracted a severe lung infection that almost killed him. He provided prescription medicines for some time but had to stop because [redacted] lacked medical insurance. As far as [redacted] could tell, [redacted] was clear and coherent and did not suffer from any medical imbalances. (Exhibit 4)

On August 15, 2011, TOIG spoke with [redacted] brother. [redacted] told TOIG that he believed his brother did work at one time for the Federal government in some kind of capacity, though he was uncertain specifically in what area of the government. [redacted] did not offer any information as to whether his brother suffered any mental illness. He said that he is not close with [redacted] and has not spoken with him in two years. He said the fact that that his brother has cancer and may be on painkillers may have caused him to act in the way that he did in going to the USAO. (Exhibit 5)

Referrals

On August 1, 2011, the TOIG and TIGTA contacted the USAO Miami, FL, regarding their interview of [redacted]. After describing the findings of the interview, First Assistant U.S. Attorney [redacted] asked if [redacted] appeared to pose a threat to the USAO. The agents advised [redacted] that they did not think he presented a threat. [redacted] then advised SA [redacted] that his office will likely decline prosecution of [redacted] for impersonating a Treasury agent. (Exhibit 6)

On January 5, 2012, the TOIG, contacted the USAO Miami, FL, regarding criminal prosecution of [redacted]. After describing the findings of the investigation of [redacted] and interviews of him

and other witnesses to [redacted] successor, [redacted], Chief of Major Crimes Division, [redacted] declined criminal prosecution of [redacted] (Exhibit 7)

Judicial Action

N/A

Findings

Investigation by the TOIG and TIGTA determined that [redacted] did attempt to gain access to the USAO in Miami, FL by representing himself as a Treasury agent. However, the USAO declined criminal prosecution of [redacted] due to the fact that he did not appear to pose a threat to the U.S. Attorney or his office.

Based on the findings of this investigation, it appears that the following statues were violated and could be applied to the case.

- 18 U.S.C. 912 Impersonation of a Federal Officer

Distribution

N/A

Signatures

Case A[redacted]

2/13/12
Date

Supervisor:

[redacted]

2-13-12
Date

Exhibits

1. Lead Information from TIGTA, dated July 29, 2011.
2. Memorandum of Activity, Interview of [redacted] dated August 4, 2011.
3. Memorandum of Activity, Interview of [redacted] dated August 4, 2011.
4. Memorandum of Activity, Interview of [redacted] dated August 4, 2011.
5. Memorandum of Activity, Interview of [redacted] dated August 16, 2011.
6. Memorandum of Activity, Criminal Referral -Declination, dated August 1, 2011.
7. Memorandum of Activity, Criminal Referral -Declination, dated January 8, 2012.

REPORT OF INVESTIGATION
DO-12-0937-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Departmental Offices

Case #: DO-12-0937-I

Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: February 27, 2012

Investigation Completed:

Conducted by: [redacted]
Special Agent

Origin: Peter A. [redacted] Attorney Advisor, Departmental Offices

Approved by: [redacted]
Special Agent-In-Charge

Summary

On February 22, 2012, the U.S. Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG) received a complaint from [redacted] Attorney Advisor, Office of Counsel (OC), Departmental Offices (DO), alleging that [redacted], DO, misused and/or abused his official government position. It was alleged that [redacted] used his official Treasury position to obtain favors for [redacted] of which he is a Senior Partner.

The investigation determined the allegation is unsubstantiated. However, there were instances where an appearance existed that [redacted] was attempting to use his official government position for personal gain. The investigation was presented to the Public Corruption Section, U.S. Attorney's Office, Washington, DC, for prosecution, but was declined due to the lack of prosecutive merit. [redacted] resigned from his position, which was effective July 16, 2012.

Basis and Scope of the Investigation

TOIG received an allegation from [redacted] that [redacted] misused and/or abused his official government position. Specifically, it was alleged that [redacted] used his official Treasury position to obtain favors for [redacted] for which he is a Senior Partner.

[redacted] is the former [redacted] within Treasury's Office of Small Business, Housing and Community Development Policy. This office coordinates policy on the following areas: small business finance and development; housing policy; community and economic development; capital access; and issues related to underserved communities. The office also oversees the Small Business Lending Fund, the State Small Business Credit Initiative, and provides policy support for Treasury's Community Development Financial Institutions Fund.

[redacted] is a venture capital firm that invests in and lends money to highly qualified entrepreneurs, many of which are minority or women-owned businesses. [redacted] is a firm interested in finance and relationship opportunities with firms that are involved in government contracting and diversity suppliers to the Fortune 500.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted], Treasury, Departmental Offices.
- [redacted],Treasury, Departmental Offices.
- [redacted] for Treasury's Office of Small Business, Housing and Community Development Policy, Departmental Offices.
- [redacted], Treasury, Deparmental Offices.
- [redacted] Sub-contractor for [redacted]
- [redacted] of the DC Chamber of Commerce.
- [redacted] of the DC Chamber of Commerce.
- [redacted], Departmental Offices.
- [redacted] with Treasury's Departmental Offices.

In addition, TOIG reviewed pertinent documents, including:

- [redacted] letter of resignation, dated July 2, 2012.

Investigative Activity

In an interview with TOIG, [redacted] reported [redacted] started his employment with Treasury as a [redacted] for Small Business in February 2011. [redacted] reports directly to [redacted]

[redacted] Deputy Assistant Secretary, Small Business, Community Development. Prior to joining Treasury, [redacted] was informed by [redacted] about his outside business with [redacted] was also notified of [redacted] and his business partners' previous involvement in a lawsuit with the Small Business Administration (SBA). [redacted] hired [redacted] based on his experience in the subject areas needed.

[redacted] reported that [redacted] attended New Employee Orientation, on February 28, 2011, at which time he received a copy of Treasury's Ethics handbook as well as an in-person briefing of the ethics restrictions he needed to comply with as a Federal employee. [redacted] continued that in June 2011, [redacted] approached [redacted] DO, with questions about restrictions on outside activities. [redacted] sent [redacted] an email outlining the general restrictions on outside activities as well as those specifically raised by his involvement with [redacted]

[redacted] added that several times thereafter, [redacted] came to his office to ask various technical questions associated with his outside activity. [redacted] explained that the activity had previously been approved by [redacted] and that he had discussed the issue generally with [redacted] [redacted] stated that he had several undocumented conversations with [redacted] regarding applicable ethics restrictions, but added that he did not feel that any additional action was necessary based on the information provided by [redacted]

[redacted] stated that [redacted] came to his office in September 2011, seeking a waiver from the criminal conflict of interest restrictions in Title 18 USC 208 – Conflict of Interest. [redacted] stated that in all other cases in which an employee has come to him to request a waiver, he or she has provided the basic facts and the Ethics Office has written the waiver request for submission to the Office of Government Ethics (OGE). In this case, [redacted] presented [redacted] with a document he (or someone at his direction) generated, that outlined what he understood to be both the factual and the legal case for a waiver. [redacted] reviewed the document and subsequently discussed the document with his supervisor, [redacted], DO, who also reviewed [redacted] request.

As a result, a meeting was scheduled between [redacted] and [redacted] to address [redacted] request. [redacted] explained how the document and his conversation with [redacted] went. [redacted] sought a waiver and outlined a potential conflict of interest solely because [redacted] may in the future seek funds from individual state entities (based on as yet undetermined criteria) and that those states may receive funding from the U.S. Government. [redacted] stated that he and [redacted] both agreed that the relationship between [redacted] current role at Treasury and the potential application for future state money was too tenuous for a waiver to be required or approved. As such, [redacted] was informed of their ([redacted] and [redacted] determination to decline the waiver during the meeting.

In February 2012, [redacted] received an unsolicited telephone call from a former Treasury Official, who requested anonymity, regarding [redacted] outside employment. This individual informed

[redacted] that [redacted] was distributing his Treasury business cards for personal business purposes; possibly using Treasury time to conduct [redacted] business; and was attempting to allay concerns about these actions by showing others his completed Outside Employment or Business Activity Request for Departmental Offices Employees (DO Form 611.1). [redacted] stated that he immediately informed [redacted] of the allegation, which subsequently led to another meeting being scheduled between [redacted] and [redacted] (Exhibit 1)

In an interview with TOIG, [redacted] stated that during a meeting with [redacted] he admitted to keeping his Treasury business cards in one pocket and his [redacted] business cards in a separate pocket; in response to her advising he is not to use his Treasury title or business card in any business dealing on the behalf of [redacted] Additionally, [redacted] informed [redacted] that the Treasury Outside Activity Form was an internal document and should not be used in any manner as proof of Treasury's approval of his business dealings on behalf of [redacted] [redacted] stated that [redacted] acknowledged that he understood and denied violating any ethics rules or regulations.

[redacted] continued that [redacted] came to her office to discuss a telephone conversation regarding [redacted] work with [redacted] (a private citizen affiliated with [redacted] contacted [redacted] to raise concerns that [redacted] was co-mingling his work with [redacted] and Treasury. [redacted] informed her that [redacted] was engaging in contract discussions for [redacted] with entities that had received and were to receive funding from a program operated by [redacted] office; the office in which [redacted] was involved in the decision making process for the allocation of funding. [redacted] stated that she requested supporting documentation, and immediately notified [redacted] of the allegation. (Exhibit 2)

In an interview with TOIG, [redacted] was also able to confirm that [redacted] called him regarding [redacted] and his outside activities. [redacted] advised [redacted] that [redacted] was soliciting potential investors for [redacted] while representing himself as a [redacted] and Treasury official. [redacted] also advised that he was given information that [redacted] was presenting both his Treasury and [redacted] business cards to potential investors for [redacted] and potential vendors for Treasury.

In March 2012, [redacted] called [redacted] for a second time to report that individuals outside of Treasury have been approached by [redacted] about potential business ventures with his outside firm.

[redacted] stated that a meeting was scheduled with [redacted] [redacted] and OC to discuss his outside activities with [redacted] [redacted] stated during the meeting, [redacted] advised that he has taken several steps to ensure that he was not engaging in any inappropriate activities. [redacted] agreed not to have any involvement in the fundraising efforts of [redacted] [redacted] stated that he would refer inquiries about [redacted] from any outside entity to his partners and corporate attorneys. (Exhibit 3)

In an interview with TOIG, [redacted] informed TOIG during the time in question, she handled approximately 20 ethical inquiries requests per week. As a result, she could not recall any specifics relating to [redacted] (Exhibit 4)

In an interview with TOIG, [redacted] acknowledged witnessing [redacted] handing out Treasury and [redacted] business cards (together), to potential [redacted] investors. [redacted] also confirmed that [redacted] provided these same investors with a copy of the official Treasury Outside Activities form. [redacted] provided three different occasions, where he witnessed [redacted] representing himself as a Treasury official and [redacted] official:

- In February 2011, [redacted] hosted meetings attended by small businesses to discuss a number of ideas that would be submitted to Treasury. [redacted] stated that [redacted] was a representative of [redacted] [redacted] stated that [redacted] gave members of the group/meeting business cards for Treasury and [redacted]

- In March 2011, [redacted] hosted another meeting, that [redacted] attended, and again supplied attendees with business cards from Treasury and [redacted] [redacted] stated that after the meeting he asked [redacted] if he had approval from Treasury to distribute both sets of business cards, in the manner he was presenting them. [redacted] stated that [redacted] advised him that he had prior approval by Treasury's ethics office.

- In April 2011, [redacted] stated that he was contacted by the Washington, DC Chamber of Commerce Foundation, relating to a lending program that was being funded by Treasury, called the State Small Business Credit Initiative (SSBCI) program to the DC Government. [redacted] contacted the foundation and wanted to enter into a memorandum of understanding to help them put a program together using a portion of the SSBCI funds to invest in small businesses in Washington, DC, while still employed as a Senior Advisor for Small business within Treasury.

[redacted] then informed TOIG that he entered into a small personal service contract with [redacted] – [redacted] [redacted] stated that he entered into this personal service contract based on the information [redacted] provided regarding his Treasury approval. [redacted] stated that the contract was to supply [redacted] with business contracts and/or potential investors for [redacted]

[redacted] explained that in email correspondence between himself and [redacted] gave [redacted] permission to supply potential [redacted] investors with a copy of his resume and official Treasury Outside Activities from. [redacted] email stated "Feel free to send this resume'. The outside activity form should accompany it also. > Thanks > [redacted] Attached to this email was a copy of [redacted] resume and outside activity form. (Exhibit 5)

In an interview with TOIG, [redacted] and [redacted] stated that [redacted] met [redacted] several years ago while he was working at Industrial Bank in Washington, DC. [redacted] stated that it was not until

[redacted] approached her at a business/social function when she and/or the DC Chamber of Commerce considered entering into a business junction with [redacted] and/or [redacted] stated that [redacted] was attempting to sell her on the idea of [redacted] being able to help small business owners with obtaining funding.

During her conversation with [redacted] stated that [redacted] mentioned that he is Senior Partner at [redacted] and is currently employed with Treasury. [redacted] stated that it was her impression that [redacted] was simply highlighting his qualifications to demonstrate his credibility. As a result of this conversation, [redacted] stated that they decided to enter into preliminary discussions with [redacted] regarding [redacted] and what they can contribute to the Washington, DC Chamber of Commerce.

When discussions between the Washington, DC Chamber of Commerce and [redacted] began, they agreed that [redacted] would be the primary point of contact for the DC Chamber of Commerce. However, when their discussion started to develop into business negotiations, [redacted] and [redacted] requested reassurance from [redacted] that there was not a conflict of interest between his roles at Treasury and [redacted] As a result, [redacted] emailed [redacted] a copy of his approved outside activity form to [redacted] and [redacted] Both advised that it was their impression that [redacted] was given blanket permission from Treasury to conduct any and all business as a [redacted] official. They decided to continue with their business relationship with [redacted] after receiving [redacted] approved outside activity form.

[redacted] and [redacted] stated that [redacted] never represented himself as a Treasury official during any discussions. In addition, both advised that [redacted] never provided them with one of Treasury business cards. They also stated that there was never any discussion with [redacted] about the $13 million Access to Capital award to the DC Government from Treasury. [redacted] and [redacted] stated [redacted] was not in any of the meetings or conference calls that they (DC Chamber of Commerce) engaged in with Treasury, regarding these funds. (Exhibit 6)

In an interview with TOIG, [redacted] stated that he met [redacted] through his work as a Commercial Loan Officer at Industrial Bank, at which time he ([redacted] was President of City First Bank of Washington, DC.

[redacted] stated that sometime in June 2011, [redacted] mentioned that [redacted] was seeking to raise funds for [redacted] continued that [redacted] told him that [redacted] was talking to officials from the DC Chamber of Commerce and Washington, DC government about investing in [redacted] perhaps including the DC's SSBCI funds. [redacted] stated that [redacted] expressed concern that [redacted] was using two business cards, one each from Treasury and [redacted] stated that [redacted] thought this could create confusion about when [redacted] represented Treasury and when [redacted] represented [redacted] stated that he has seen both of [redacted] business cards on his desk; however, he did not witness [redacted] using two business cards. (Exhibit 7)

In an interview with TOIG, [redacted] stated that he had discussions with his supervisor [redacted] and Treasury ethics officials, which included, but is not limited to: [redacted] [redacted] and [redacted] regarding his employment history and his involvement in an outside firm, [redacted] [redacted] wanted to maintain his interests in [redacted] after accepting employment with Treasury. [redacted] confirmed that he told Treasury officials that his role with [redacted] would not, in any capacity, overlap and/or interfere with his responsibilities at Treasury. Ethics officials provided him with guidance and restrictions regarding his outside involvement with [redacted]

For example, [redacted] informed Treasury officials that [redacted] did not have clients and/or investors. As a result, there was not a conflict between his roles at Treasury and [redacted] Treasury officials made recommendations based on this information. They also informed [redacted] that it was his responsibility to inform them of any changes in the company and his role in it.

[redacted] stated that he did not intentionally give any person (inside or outside Treasury) the impression that it would benefit them to assist, employ, or contribute to [redacted] and in return receive favorable treatment by Treasury. [redacted] denied that there was any quid pro quo. [redacted] confirmed that he has given his Treasury and [redacted] business cards to many individuals during his tenure with Treasury. However, he stated that he did not remember giving both business cards out at the same time.

[redacted] acknowledged that he supplied individuals outside of Treasury with a copy of his approved outside activities form. [redacted] stated that he was not aware at the time that the outside activities form was an internal document that could not be shared with outside entities. [redacted] shared his approved outside activities form to show that he had approval to conduct work with/for [redacted] [redacted] was asked if he used the outside activities form as a blanket approval, from Treasury, or did he share the restrictions and/or limitations issued to him by Treasury with these outside entities. [redacted] stated that he did not share any restrictions and/or limitations with the outside entities because he did not fully understand the restrictions. [redacted] stated that the direction given by Treasury ethics officials and his supervisor ([redacted] were not clear to him. [redacted] confirmed that there were several discussions and/or meetings regarding this topic, but claims that he was given conflicting information. (Exhibit 8)

On July 12, 2012, TOIG obtained a copy of a letter of resignation that was signed by [redacted] [redacted] resignation effective date was July 16, 2012. (Exhibit 9)

Referrals

On July 3, 2012, TOIG presented the facts of this investigation to [redacted], Assistant U.S. Attorney, Public Corruption Section, U.S. Attorney's Office (USAO), Washington, DC, for

the potential criminal and/or civil prosecution of [redacted] declined criminal and civil prosecution of [redacted] due to the lack of prosecutive merit. (Exhibit 10)

Judicial Action

N/A

Findings

The investigation determined the allegation is unsubstantiated. However, there were instances where an appearance existed that [redacted] was attempting to use his official government position for personal gain. The investigation was presented to the Public Corruption Section, U.S. Attorney's Office, Washington, DC, for prosecution, but was declined due to the lack of prosecutive merit. [redacted] resigned from his position, which was effective July 16, 2012.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policy(ies) were violated or could be applied to the case:

- 31 CFR Part 0 § 0.213 – General conduct prejudicial to the Government.

Distribution

[redacted], Senior Advisor, Department of the Treasury

Signatures

Case Agent: [redacted] 10/16/12
Date

Supervisor: [redacted] 10/16/12
Date

Exhibits

1. Memorandum of Activity, Interview of [redacted] Attorney Advisor, Treasury, Departmental Offices, dated March 19, 2012.

2. Memorandum of Activity, Interview of [redacted] Deputy Assistant General Counsel Ethics,Treasury, Departmental Offices, dated March 19, 2012.

3. Memorandum of Activity, Interview of [redacted] Deputy Assistant Secretary for Treasury's Office of Small Business, Housing and Community Development Policy, Departmental Offices, dated April 10, 2012.

4. Memorandum of Activity, Interview of [redacted] Ethics Program Manager, Treasury, Deparmental Offices, dated April 23, 2012.

5. Memorandum of Activity, Interview of [redacted] Sub-contractor for [redacted] LLC, dated May 4, 2012.

6. Memorandum of Activity, Interview of [redacted] President & Chief Executive Officer (CEO) of the DC Chamber of Commerce, and [redacted] Vice President & Executive Director of the DC Chamber of Commerce, dated May 18, 2012.

7. Memorandum of Activity, Interview of [redacted] Director of the State Small Business Credit Initiative (SSBCI), Departmental Offices, dated June 8, 2012.

8. Memorandum of Activity, Interview of [redacted] a former Senior Policy Analyst for Small Business with Treasury's Departmental Offices, dated July 2, 2012.

9. Memorandum of Activity, Record Review – Letter of Resignation fro [redacted] dated July 12, 2012.

10. Memorandum of Activity, Criminal / Civil Presentation, dated July 3, 2012.

REPORT OF INVESTIGATION
DO-12-2183-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Office of Foreign Assets Control
Departmental Offices

Case #: DO-12-2183-I

Case Type: Criminal ___
Administrative X
Civil ___

Conducted by: [redacted]
Special Agent

Investigation Initiated: July 24, 2012

Investigation Completed: OCT 1 2012

Approved by: [redacted]
Special Agent in Charge

Origin: [redacted] About.com

Summary

On July 12, 2012, the United States Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), received information from [redacted] Journalist, About.com, alleging a Treasury employee used their government-issued computer to post inappropriate comments on About.com. (Exhibit 1)

The investigation substantiated that [redacted] employee and Treasury contractor, [redacted] posted two comments on About.com on July 3 and July 11, 2012. [redacted] works on a government contract with the Office of Foreign Assets Control (OFAC), Departmental Offices (DO).

Basis and Scope of the Investigation

This case was initiated on July 24, 2012, based upon a complaint from [redacted] informing TOIG of alleged comments posted to About.com by a Treasury employee from a government-issued computer.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] IT Specialist, OCIO, DO
- [redacted] Contractor, [redacted], DO

In addition, TOIG reviewed pertinent documents, including:

- Comments posted to About.com, dated July 3 and July 11, 2012
- OI Form-26 (Advice of Rights – Kalkines) for [redacted] dated August 16, 2012

Investigative Activity

On July 31, 2012, TOIG interviewed [redacted] Information Technology (IT) Specialist, Office of the Chief Information Officer (OCIO), DO. [redacted] said AT&T retains Internet-Protocol (IP) logs for Treasury computers for approximately two to three years. TOIG provided [redacted] with host name, beginnersinvest.wpadmin.about.com and IP address [redacted]. This host name and IP address were provided by [redacted] and are used for all About.com blogs. (Exhibit 2)

On July 31, 2012, TOIG reviewed a Treasury database query for comments posted to About.com on July 11, 2012. The results listed the originating IP address as [redacted]. It was determined that Treasury IP address [redacted] was assigned to [redacted] computer at the time when the comments were posted on About.com. (Exhibit 3)

On August 16, 2012, TOIG interviewed [redacted] regarding the comments [redacted] allegedly posted to About.com. [redacted] said he recognized the two comments posted to About.com from his government-issued laptop. [redacted] said he posted the comments during work hours. [redacted] said the two email addresses used to post the comments, "boobs@gmail.com," and [redacted]gmail.com," were both false addresses. [redacted] said the intent of the email addresses was comical, and not derogatory towards homosexuals or women. [redacted] said he does not know [redacted] nor does he know [redacted] sexual orientation. [redacted] said he has no hatred towards homosexuals. (Exhibit 4)

Referrals

On August 15, 2012, TOIG contacted [redacted], Assistant United States Attorney for the District of Columbia, to present the facts of the investigation involving comments posted to About.com by [redacted] [redacted] declined criminal prosecution of [redacted] due to lack of prosecutive merit, and approved the use of the Kalkines warning when interviewing [redacted] (Exhibit 5)

Judicial Action

N/A

Findings

The investigation substantiated that [redacted] posted two comments on About.com on July 3 and July 11, 2012.

Based on the findings of our investigation, it appears that the following pertinent regulation(s) were violated and can be applied to the case:

- 5 CFR 2635.704; Use of Government Property
- 5 CFR 2635.705; Use of Official Time
- 31 CFR 0.213; Conduct Prejudicial to the Government
- Treasury Directive 87-04; Personal Use of Government Information Technology Resources

Distribution

[redacted], Senior Advisor, DO

Signatures

Case Agent:

[redacted]

10/1/2012
Date

Supervisor:

[redacted]

10/1/12
Date

Exhibits

Number	Description
1.	Original Allegation, Correspondence, dated July 12, 2012.
2.	Memorandum of Activity, Interview of [redacted] dated July 31, 2012.
3.	Memorandum of Activity, Record Review for Treasury IP address [redacted] dated July 31, 2012.
4.	Memorandum of Activity, Interview of [redacted] dated August 16, 2012.
5.	Memorandum of Activity, Case Presentation to [redacted], Assistant United States Attorney for the District of Columbia, dated August 15, 2012.

REPORT OF INVESTIGATION
DO-12-2372-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
AKA [redacted]
SSN: [redacted]

Case #: DO-12-2372-I
Case Type: Criminal ___
Administrative X
Civil ___

Conducted by: [redacted]
Special Agent

Investigation Initiated: September 10, 2012

Investigation Completed:

Approved by: [redacted]
Special Agent in Charge

Origin: Treasury Inspector General for Tax Administration

Summary

On August 8, 2012, the U.S. Department of Treasury (Treasury), Office of Inspector General (TOIG) received a complaint from the Treasury Inspector General for Tax Administration (TIGTA), regarding an ongoing Federal Bureau of Investigation (FBI) investigation of Treasury employee, [redacted] An FBI investigation has been opened into [redacted] due to his communication with several individuals being investigated for counter-terrorism. TOIG assistance was requested because [redacted] was reportedly employed by Treasury. (Exhibit 1)

The investigation determined that the allegation is substantiated. However, the FBI investigation believes [redacted] associations with FBI person's of interest appear to be third-party relationships. [redacted] is employed as a contract employee for Treasury Contractor [redacted] and works in McLean, VA. [redacted] currently has no access to any Treasury information due to his ongoing security clearance adjudication. There appears to be no risk to Treasury.

Basis and Scope of the Investigation

This investigation was initiated on September 10, 2011, based upon a referral from TIGTA requesting assistance for the FBI. An FBI investigation was opened into [redacted] due to his communication with several individuals being investigated for counter-terrorism. TOIG assistance was requested because [redacted] was reportedly employed by Treasury.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Director, Telecommunications
- [redacted] Manager, [redacted]

In addition, TOIG reviewed pertinent documents, including:

- [redacted] Computer Use Security Banner
- [redacted] Internet logs

Investigative Activity

In an interview with TOIG, [redacted] stated [redacted] is assigned to the [redacted]. [redacted] did not have a Top Secret Clearance and did not receive his HSPD-12 card. Further inquiries by [redacted] determined [redacted] started working in October 2011, and his paperwork for his identification card was with the Prime Contractor for adjudication. [redacted] stated this was a very serious matter because of the sensitivities associated with the [redacted]. The primary function of the [redacted] is to monitor all incoming Internet traffic associated with Treasury. The individuals who are employed at the [redacted] have very special Information Technology (IT) skills. Many of them are developers and may have to write computer script at a moment's notice to address a particular problem the [redacted] encounters i.e. malware, attempted intrusions. They are considered Treasury's first line of defense. (Exhibit 2-3)

In an interview with TOIG and the FBI, [redacted] stated [redacted] is employed by [redacted], located in Herndon, VA. [redacted] has a contract with [redacted] and they provide IT security support to their Treasury contract. In the summer of 2011, [redacted] was hired to work on the Treasury contract as a web developer. [redacted] is still in the process of obtaining a Top Secret clearance. The clearance has not been approved because his application was "kicked back due to clerical problems." [redacted] stated [redacted] did not know his father's name because he had been abandoned. [redacted] has also moved around a lot, so he could not remember all of his addresses. [redacted] does not have any Treasury access due to his lack of

the required clearance level. [redacted] performs internal research and development projects for [redacted] [redacted] has limited access to non-sensitive data. (Exhibit 4)

[**AGENTS NOTE:** On November 20, 2012, SA [redacted] advised TOIG that subject will be interviewed upon his return from overseas. There does not appear to be any evidence that [redacted] poses a risk to Treasury and his relationships with other persons of interest to the FBI are third party related.

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegation is substantiated. However, the FBI investigation believes [redacted] associations with FBI person's of interest appear to be third-party relationships. [redacted] is employed as a contract employee for Treasury Contractor [redacted] and works in McLean, VA. [redacted] currently has no access to any Treasury information due to his ongoing security clearance adjudication. There appears to be no risk to Treasury.

Distribution

N/A

Signatures

Case Agent:

[redacted]

[redacted] 12/14/2012
Date

Supervisor:

[redacted] 12-14-12
Date

Exhibits

1. Initial Complaint document, dated August 8, 2012.
2. Memorandum of Activity, Interview of [redacted], dated August 31, 2012.
3. Memorandum of Activity, Document Review, dated September 14, 2012.
4. Memorandum of Activity, Interview of [redacted], dated September 7, 2012.
5. Evidence Receipt, dated September 18, 2012.

REPORT OF INVESTIGATION
DO-11-0397-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Office of Financial Innovation and Transformation
U.S. Department of Treasury

Case #: DO-11-0397-I

Case Type: Criminal X
Administrative ___
Civil ___

Conducted by: [redacted]
Special Agent

Investigation Initiated: December 8, 2010

Approved by: [redacted]
Special Agent in Charge

Investigation Completed: MAY 08 2012

Origin: Department of Transportation OIG

Summary

On December 8, 2010, the U.S. Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG), initiated an investigation based on information received from the the U.S. Department of Transportation, OIG (DOT OIG). It was alleged that [redacted], Office of Financial Innovation and Transformation, Treasury, during her previous employment as Director of Finance, Office of the Secretary of Transportation (OST), DOT, attempted to steer business to her husband, [redacted] Director of Government Systems and Services at [redacted] in violation of ethical guidelines. The work was a task order on a blanket purchase agreement held by the [redacted] would be the subcontractor. The investigation was conducted jointly with DOT OIG.

The investigation determined that the allegation is unsubstantiated. Employees of the DOT claimed that [redacted] assisted in setting up business for [redacted] without providing pertinent information that her husband worked for the selected subcontractor, [redacted] employees claimed that they could have used various subcontractors and database tools, but were told by [redacted] that DOT wanted [redacted] employees stated that [redacted] was recused of all matters involving the task order. [redacted] denied any wrongdoing. [redacted] full knowledge of the [redacted] contract prior to it being awarded could not be determined. The case was presented and declined for prosecution by the U.S. Department of Justice, Public Integrity Section.

Basis and Scope of the Investigation

It was alleged that [redacted], Office of Financial Innovation and Transformation, Treasury, during her previous employment as Director of Finance, Office of the Secretary of Transportation, DOT, attempted to steer business to her husband, [redacted] Director of Government Systems and Services at [redacted] in violation of ethical guidelines. The work was a task order on a blanket purchase agreement held by the [redacted] would be the subcontractor. The task order was for $991,000, and it was for a tool called "One View Fusion" ([redacted] being promoted by [redacted] It was awarded in August 2010, and terminated by the government in October 2010. It was terminated because DOT management decided other companies and computer applications could be used, and because of the allegations raised by DOT staff of ethical issues involving this contract and [redacted] was responsible for overseeing a staff that managed the contracting for DOT, and [redacted] was the deciding official on these contracts.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] DOT
- [redacted]
- Numerous interviews of DOT employees, [redacted] employees and [redacted] employees

During the course of the investigation, TOIG reviewed pertinent documents, including:

- E-mails between [redacted] and DOT, [redacted] and [redacted] employees.

Investigative Activity

In an interview with TOIG, [redacted] reported that she was responsible for accounting operations, coordinating audits, financial systems and essentially overseeing all financial operations in her last position as the Director of Finance, DOT. [redacted] added that her husband, [redacted] was the Deputy Chief Financial Officer, DOT, and he later became a rehired annuitant for the Federal Highway Administration. After retiring, [redacted] worked for [redacted] for approximately 15 months before he became employed with [redacted] was employed at [redacted] when they were married in 2009.

[redacted] stated that [redacted] and [redacted] had been contractors for DOT for years. She stated that she did not steer business to either companies, and did not know [redacted] was a subcontractor to [redacted] on a DOT contract until the contract had been awarded. She stated that her DOT Business Intelligence Team introduced her to [redacted] in August of 2010, and this group was responsible for selecting [redacted] as a subcontractor. [redacted] said that she was aware that [redacted] contacted her staff regarding the [redacted] Product, offered by [redacted] She said that she was upset with him for doing that and spoke to him about that matter. [redacted] became employed with Treasury in October 2010. (Exhibit 1)

In an interview with TOIG, [redacted] stated that [redacted] told him that her office, had a blanket purchase agreement with [redacted] that she wanted to use. However, she was unable to talk to the [redacted] representative for three weeks. [redacted] said that he asked a manager at [redacted] to speak with management at [redacted], and to "push the [redacted] tool by [redacted] He said that he did not have anything to

gain by selling the [redacted] as [redacted] did not provide stock benefits or commission for his sale. (Exhibit 2)

In interviews with TOIG, numerous DOT employees stated that they were concerned about this conflict of interest issue because [redacted] assisted in setting up business for [redacted] without providing pertinent information that [redacted] worked for the potential subcontractor, [redacted] provided her staff with her recusal letter, but continued to encourage potential business for her husband. The staff was further disturbed by [redacted] persistent contact with the OST staff to promote [redacted] business intelligence tool that he claimed would assist DOT with data management and data cleanup activities. The staff believed that DOT did not need the tool, and this project was an added expense to the budget, but were required to purchase it because [redacted] wanted it. The contract with [redacted] and [redacted] was terminated in October 2010, shortly after [redacted] left DOT for employment with Treasury. (Exhibit 3)

In an interview with TOIG, [redacted] Business Development Executive, [redacted] stated that in approximately May 2009, she met with [redacted] and [redacted] a subordinate of [redacted] at DOT. [redacted] stated that there was a blanket purchase agreement (BPA) between OST and [redacted] and [redacted] wanted to utilize this contract by obtaining work from OST. Shortly thereafter, [redacted] had another meeting with [redacted] where [redacted] stated that OST wanted to upgrade their Oracle system. She could not recall if [redacted] brought up [redacted] reporting tool at this time, but did recall [redacted] requesting that [redacted] use [redacted] and Leadership Management International (LMI). [redacted] had another conversation with [redacted] in the Spring of 2010, and [redacted] reiterated that OST wanted to start a reconciliation project and that [redacted] should use [redacted] and LMI for this reconciliation project. [redacted] stated that it is unusual for a customer to request a subcontractor, but it does occur. [redacted] normally is required to find the necessary subcontractors to complete the work. In this case, [redacted] had no issues with hiring [redacted] because [redacted] had a good reputation, and since [redacted] was told what subcontractor to use by the client, the selection task was easy for [redacted] In August 2010, [redacted] was notified that the task order for the work was awarded to [redacted] In October 2010, [redacted] learned that the task order was on hold. Within a couple of weeks, she learned that the task order had been cancelled. At the same time, [redacted] left DOT. (Exhibit 4)

In an interview with TOIG, [redacted] Senior Principal, [redacted] stated that she was not certain how [redacted] learned of a contract with [redacted] and DOT, but believed it occurred in the Spring of 2010. [redacted] stated that [redacted] management had heard that DOT expected the [redacted] to be part of the [redacted] contract, and [redacted] was interested in assisting [redacted] with technical solutions and staffing of the [redacted] a Business Development Manager, was developing the [redacted] in Federal markets and [redacted] was a "subject matter expert." Shortly after [redacted] began partnering" with [redacted] on this matter, [redacted] told [redacted] that [redacted] could not be involved with discussions on this contract because he was married to a DOT employee. She then recalled that [redacted] management decided to "firewall" [redacted] from any discussions or work on the [redacted] DOT contract. In the Fall of 2010, [redacted] left DOT and [redacted] was allowed to be involved in the contract because [redacted] management felt there was no longer any conflict of interest. Shortly thereafter, [redacted] learned that DOT was no longer interested in [redacted]

[redacted] stated that [redacted] would not have been evaluated on his work with this contract because he was "firewalled" soon after [redacted] began partnering with [redacted] so he did very little on this contract. If the DOT contract had continued and [redacted] were allowed to work on it because [redacted] had resigned from DOT, he may have been rated on his work on the contract for FY 2012. (Exhibit 5)

Referrals

On March 25, 2011, TOIG and DOT OIG presented the facts of this matter to the U.S. Department of Justice, Public Integrity Section and the case was accepted. (Exhibit 6)

On April 13, 2012, the TOIG received a declination of prosecution from the U.S. Department of Justice, Public Integrity Section. The declination was based on conflicting testimony heard through the Grand Jury. (Exhibit 7)

Judicial Action

N/A

Findings

The investigation determined that the allegation is unsubstantiated. Employees of the DOT claimed that [redacted] assisted in setting up business for [redacted] without providing pertinent information that her husband worked for the selected subcontractor, [redacted] employees claimed that they could have used various subcontractors and database tools, but were told by [redacted] that DOT wanted [redacted] employees stated that [redacted] was recused of all matters involving the task order. [redacted] denied any wrongdoing. [redacted] full knowledge of the [redacted] contract prior to it being awarded could not be determined. The case was presented and declined for prosecution by the U.S. Department of Justice, Public Integrity Section.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policies were violated or could be applied to the case:

- N/A

Distribution

[redacted] Senior Advisor, Treasury

[redacted], Associate CHCO, Treasury

Signatures

Case Agent:

[redacted] 5/4/12
Date

Supervisor:

[redacted] 5-4-12
Date

Exhibits

1. Memorandum of Activity, Interview of [redacted] dated March 18, 2011.
2. Memorandum of Activity, Interview of [redacted] dated March 18, 2011.
3. Memorandum of Activity, Interview of [redacted] dated December 2, 2011.
4. Memorandum of Activity, Interview of [redacted] dated July 8, 2011.
5. Memorandum of Activity, Interview of Denise [redacted] dated October 6, 2011.
6. Memorandum of Activity, Case acceptance, dated March 30, 2011.
7. Memorandum of Activity, Case declination, dated April 13, 2012.

REPORT OF INVESTIGATION
DO-11-1588-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Office of the Chief Information Officer, Departmental Offices

Investigation Initiated: September 16, 2011

Investigation Completed: DEC 23 2011

Origin: [redacted] Senior Advisor, Office of the Chief Information Officer, Departmental Offices

Case #: DO-11-1588-I
Case Type: Criminal ___
Administrative X
Civil ___

Conducted by: [redacted]
Special Agent

[redacted]
Special Agent

Approved by: [redacted]
Special Agent in Charge

Summary

On September 15, 2011, the U.S. Department of Treasury (Treasury), Office of Inspector General (TOIG), was notified by [redacted] Senior Advisor, Office of the Chief Information Officer, Departmental Offices (DO) of a potential conflict of interest between a Treasury employee and a contractor for [redacted] The allegation was focused on [redacted] a Limited Liability Company (LLC) that [redacted] and [redacted] DO, formed in August 2011, and a small business bank account that was created with Bank of America to support this venture. (Exhibit 1)

The investigation determined the allegations are substantiated. [redacted] and [redacted] established [redacted], LLC and opened a joint small business bank account with Bank of America. Neither [redacted] nor [redacted] reported the establishment of this LLC or the potential for a conflict of interest with DO and [redacted] respectively. This investigation was presented to the U.S. Attorney's Office for the District of Columbia for criminal prosecution, but was declined.

Basis and Scope of the Investigation

[redacted] is a DO employee working in [redacted] Office of the Chief Information Officer. The CPIC Program ensures that all IT investments align with the mission and support business needs while minimizing risks and maximizing returns throughout the investment's lifecycle. During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Contracting Officer's Technical Representative (COTR), DO
- [redacted] Associate Chief Information Officer [redacted], DO
- [redacted] Senior Advisor, DO
- [redacted] Director [redacted], DO
- [redacted] Manager, [redacted] Consulting
- [redacted] Supervisory Information Technology Specialist, DO
- [redacted] Associate General Counsel, [redacted]

Investigative Activity

In an interview with TOIG, [redacted] reported that task order TIRNO-06-00026-[redacted], TIPS-3 contract, issued to [redacted] was scheduled to end October 26, 2011. [redacted] stated that [redacted] works within CPIC and acknowledged that there is a possibility that [redacted] is assigned to the task order, but she was not certain. In regards to the allegation, [redacted] stated that even the appearance of a conflict between a Treasury employee and [redacted] contractor is detrimental to the overall mission. [redacted] also stated that DO employees receive ethics training on an annual basis and the appearance of a conflict of interest is covered in the training. (Exhibit 2)

In an interview with TOIG, [redacted] stated [redacted] reports directly to her and had been working there for approximately one year. [redacted] stated that she is also well acquainted with [redacted] continued that [redacted] and [redacted] worked on the CPIC organization. [redacted] said [redacted] and [redacted] had a close working relationship. [redacted] verified that there was no opportunity for [redacted] to have additional work under the [redacted] task order due to in sourcing. (Exhibit 3)

In an interview with TOIG, [redacted] stated that discussions took place in August or September 2010, pertaining to the [redacted] task order. [redacted] advised TOIG that he and [redacted] determined that it was more cost effective for DO to create FTEs to handle the work currently being done by [redacted] continued that he made recommendations regarding the re-competition of [redacted] however he and [redacted] agreed that it was in the best interest of Treasury to allow the task order to expire, without being recompeted. This decision was made prior to [redacted] joining their office. (Exhibit 4)

In an interview with TOIG, [redacted] confirmed that he reported the information regarding the conflict of interest. [redacted] was made aware of the allegation by [redacted] in September 2011. [redacted] learned of [redacted] separation in a [redacted] memo given to him. [redacted] was unaware of the circumstances surrounding [redacted] departure. The [redacted] memo stated [redacted] received the tip from their ethics department and forwarded the information to the Treasury's Ethics office. [redacted] did not know any information on the type of LLC alleged, nor could he confirm the alleged joint bank account between [redacted] and [redacted] (Exhibit 5)

In an interview with TOIG, [redacted] stated he has been employeed with Treasury's Office of the Chief Information Officer, as the Director of [redacted] since October 2010. [redacted] stated that he met [redacted] while working on the Capital Planning program. [redacted] continued that he developed a personal friendship with [redacted] outside of work based on common ideas on decision support and decision making processes. The outcome of these discussions was that they decided to create a blog (on line web-log) to discuss decision making concepts and approaches in a general way that could be applied to life, professional and government choices. Subsuequently, [redacted] was formed to provide some protection for ideas and concepts that would be in the public realm. They considered this more of a hobby than a business and anticipated that it would be a non profit organization with little or no expectation of receiving any income from this endeavor. Expenditures to date had been less than $500 and include the registration fee to incorporate, the cost to reserve a domain name and a hosting fee for a future web-site. [redacted] and [redacted] split the costs evenly. No web site has been created, no public activities have commenced and there are no employees or clients.

[redacted] stated that it was decided, before he gained employment with DO, that Treasury was not going to re-compete the [redacted] task order that [redacted] was currently working on. DO determined it would be more cost effective for DO to create full-time equivalents (FTE) to handle the tasking currently being worked by [redacted] There was no opportunity for [redacted] to have additional work under this task order. [redacted] did not believe that there is a conflict of interest of any type, between the [redacted] activities and his position at Treasury. While he may have applied some of the ideas and concepts that he and [redacted] discussed in his present position, they were in no way trying to sell products to the Treasury. In addition, there has never been a coercive element to his relationship with [redacted] in either direction. [redacted] believed that since [redacted] contract support with Treasury had already been planned to end prior to beginning their personal relationship, there was no opportunity for [redacted] to make any sourcing decisions based on that relationship. Lastly, while [redacted] is legally an entity, [redacted] believes that his level of involvement had not warranted notifying DO of his activity at this time. Should the [redacted] venture have continued, he would have submitted that information in a revised financial disclosure form as required. (Exhibit 6)

In an interview with TOIG, [redacted] was involved in the handling of the issue regarding [redacted] joint venture with [redacted] [redacted] stated the complaint originated with an anonymous phone call to the [redacted] hotline. [redacted] continued that there were two issues that [redacted] wanted to address; the potential conflict of interest; and [redacted] potentially violating [redacted] outside and/or secondary employment policy. [redacted] employees must request prior approval in entering into outside employment from their Human Resources Department (HR). [redacted] reported that on September 2, 2011, a [redacted] HR representative spoke with the anonymous caller and was told of the outside employment and appearance of a conflict of interest between the two individuals. On September 5, 2011, [redacted] was questioned by [redacted] HR regarding the allegation. [redacted] denied the allegation. [redacted] denied establishing [redacted] with [redacted] However, [redacted] later determined that [redacted] lied to [redacted] officials regarding [redacted]. As a result, [redacted] decided to terminate [redacted] based on violations of ethical policies.

Based on [redacted] decision to terminate [redacted] a meeting was scheduled on September 9, 2011, between [redacted] officials and [redacted] to notify [redacted] of their decision. During the meeting, [redacted] was

advised that he was going to be terminated, at which time [redacted] officials attempted to serve [redacted] with a letter of termination. [redacted] immediately supplied [redacted] officials with a signed letter of resignation, which [redacted] accepted. (Exhibit 7)

Referrals

This investigation was presented to the U.S. Attorney's Office for the District of Columbia for the potential criminal prosecution of [redacted] and [redacted] the case was declined. (Exhibit 8)

Judicial Action

None

Findings

The investigation determined the allegations are substantiated. [redacted] and [redacted] established [redacted], LLC and opened a joint small business bank account with Bank of America. Neither [redacted] nor [redacted] reported the establishment of this LLC or the potential for a conflict of interest with DO and [redacted] respectively.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policy(ies) were violated or could be applied to the case:

- Standards of Ethical Conduct for Employees of the Executive Branch 5 C.F.R. 2635.803 – Prior Approval for Outside Employment and Activities.

Distribution

[redacted], Chief Information Officer, DO

Signatures

Case Agent:

[redacted]

12/20/11
Date

Superyisor:

[redacted]

12-20-11
Date

Exhibits

Number	Description
1.	Original allegation, Correspondence, dated September 15, 2011.
2.	Memoradum of Activity, Interview of [redacted] dated September 23, 2011.
3.	Memoradum of Activity, Interview of [redacted] dated September 26, 2011.
4.	Memoradum of Activity, Interview of [redacted] dated October 31, 2011.
5.	Memoradum of Activity, Interview of [redacted], dated September 28, 2011.
6.	Memoradum of Activity, Interview of [redacted] dated September 28, 2011.
7.	Memoradum of Activity, Interview of [redacted] dated November 9, 2011.
8.	Memoradum of Activity, Case Presentation, dated October 13, 2011.

REPORT OF INVESTIGATION
DO-12-0183-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case #: DO-12-0183-I

Investigation Initiated: November 17, 2011

Case Type: Criminal ____ Administrative _X_ Civil ____

Investigation Completed: JAN 17 2012

Conducted by: [redacted] Senior Special Agent

[redacted] Special Agent

Origin: Treasury, Departmental Offices, Office of Intelligence and Analysis

Approved by: [redacted] Special Agent in Charge

Summary

On November 1, 2011, [redacted] Supervisory Operations Officer with the Treasury Office of Intelligence and Analysis (OIA), Departmental Offices (DO), contacted the Treasury, Office of Inspector General, Office of Investigations (TOIG) to notify of a possible PII (Personally Identifiable Information) disclosure in the OIA. [redacted] said that a document that had been stored on a restricted folder on the Microsoft Windows office server had been accidentally or intentionally accessed. The office server involved is the unclassified information server. The folder stored a spreadsheet file containing the Human Resources (HR) performance ratings for the most recently completed evaluation cycle. The file contained the rating scores and rankings of employees in the Office of Security and the OIA by name and General Scale (GS) grade. [redacted] advised that an Intelligence Research Specialist (IRS), [redacted] was the alleged source of the leak. OIA Counsel has placed [redacted] on administrative leave as of November 1, 2011, pending the outcome of the investigation.

The investigation determined [redacted] did access the subject file. However, at the time [redacted] was not blocked from doing so nor did he take any actions to access the file that would be considered "hacking."

Basis and Scope of the Investigation

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Supervisory Operations Officer and Intelligence Research Specialist, OIA, DO
- [redacted] Senior Advisor to Deputy Assistant Secretary (DAS) for Intelligence Community Integrity, OIA, DO
- [redacted] Intelligence Research Specialist, OIA, DO
- [redacted] Intelligence Research Specialist, OIA, DO
- [redacted] Intelligence Research Specialist, OIA, DO
- [redacted] Intelligence Research Specialist, OIA, DO
- [redacted] Systems Engineer, DO

In addition, TOIG reviewed pertinent documents, including:

- [redacted] FY2011 Privacy Awareness Course completion records provided by Bureau of Public Debt (BPD), Human Resources Division
- Copies of the e-mails and the file attachment containing an Excel spreadsheet file with the performance ratings for employees of OIA and Office of Security within DO
- The Excel file in question, FY2011 Performance Ratings – revised draft (2).xlsx, located on a Storage Area Network (SAN) drive that was locally mapped to the F:\ drive on a Windows Server 2008 file server [redacted]
- Letter from OIA to [redacted] detailing administrative leave, dated November 1, 2011.

Background

OIA was established by the Intelligence Authorization Act for Fiscal Year 2004. The Act specifies that OIA shall be responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of the Department of the Treasury. OIA's mission is to support the formulation of policy and execution of Treasury authorities by providing expert analysis and intelligence production on financial and other support networks for terrorist groups, proliferators, and other key national security threats; as well as, timely, accurate, and focused intelligence support on the full range of economic, political, and security issues.

Investigative Activity

On November 1, 2011, [redacted] contacted TOIG to advise of a possible PII disclosure in OIA. [redacted] said that a document that had been stored on a restricted folder on the Microsoft Windows office server had been accidentally or intentionally accessed. The office server involved is the unclassified information server. The folder stored an Excel spreadsheet file containing the HR performance ratings for the most recently completed evaluation cycle. The file contained the rating scores and rankings of employees in the Office of Security and the OIA by name and GS grade.

[redacted] said that the Excel file was accessed and e-mailed by an OIA employee to another employee in the office. [redacted] said that there had been a rumor circulating among a few employees that a sensitive file was floating around the office. She said the rumor first surfaced a few weeks ago. On October 31, 2011, a senior advisor to the DAS for OIA Intelligence Community Integrity, (Michael Madden), [redacted] approached [redacted] and spoke to her about the rumor. [redacted] said [redacted] had been contacted by two employees who had been sent the HR file by the employee. The employee who sent the file to the other employees was identified as [redacted] said she did not know for certain whether the file had access restrictions placed on it –i.e., that it was a restricted folder and only users with access rights could open the file. She said that a user would have had to enter or type specific keystrokes to get around the file folder's access restrictions. She added that DO's Information Technology (IT) help desk was checking the Microsoft Outlook e-mail accounts of the individuals involved to determine whether the folder was accessed by [redacted] and whether it was subsequently sent via e-mail to other Outlook email accounts in the OIA. [redacted] said [redacted] is a GS-13 who is detailed once per week to another government agency. [redacted] has access to highly classified information in his position and [redacted] management was concerned that [redacted] could have access to other classified information and could be accessing that information without authorization. [redacted] said [redacted] had been recently passed over for promotion to GS-14. [redacted] advised that her office had placed [redacted] on administrative leave pending the outcome of the IT review and the investigation by the TOIG. Her managers cited concerns over [redacted] treatment of sensitive information and that he could be engaged in similar conduct in his workplace, which is a Sensitive Compartmented Information Facility (SCIF), and at the other government agency as well. (Exhibit 1)

On November 1, 2011, [redacted] e-mailed TOIG copies of the e-mails and the file attachment containing an Excel spreadsheet file with the performance ratings for employees of the OIA and Office of Security. [redacted] had notified TOIG earlier that date that the file had been accessed and e-mailed by an OIA employee to another employee in the office. (Exhibit 2).

On November 3, 2011, TOIG interviewed [redacted] stated that he had contacted OIA management at various points in the past several days regarding a possible PII disclosure. [redacted] advised that on October 31, 2011, another OIA employee approached him about a rumor that was going around that a file with the performance appraisal information for the office was on a shared office drive (office computer server). [redacted] said he notified [redacted] a supervisor for Personnel and Operations in the OIA. The employee who approached [redacted] was [redacted] told [redacted] he had seen the document in question and closed it immediately. [redacted] did not tell [redacted] how he got access to the file. [redacted] e-mailed [redacted] and asked her to investigate the matter. [redacted] told [redacted] that it was her understanding that the appraisal file was protected and was buried in an office file structure within the file server. [redacted] told [redacted] a lot of talk was going on around the office about the incident and that senior officials had met to discuss the matter. The Office of the Chief Information Officer was also contacted to conduct a trace of the e-mail chain. [redacted] also advised [redacted] that [redacted] had been placed on administrative leave. [redacted] said he himself tried to access the file and did not see it on the office server. [redacted] said that at lunch on November 1, 2011, another OIA employee told him that she had accessed a file belonging to [redacted] on the classified information server. [redacted] expressed surprise and the person he was having lunch with, [redacted] an OIA IRS, asked a

lot of "probing" questions. [redacted] told [redacted] that she knew of the same incident (the accessing of the document that contained Excel spreadsheet file containing the HR performance ratings for the most recently completed evaluation cycle.) [redacted] asked [redacted] if she could reach out to the other employee and he ([redacted] would try to get to the bottom of the incident and also advised her not to share the file with anyone. On November 2, 2011, [redacted] and [redacted] another OIA IRS, came to [redacted] office and were noticeably nervous. They had heard that management had been keeping silent about the matter. [redacted] counseled them to both be honest. [redacted] said she had sent the appraisal file to another employee, identified as [redacted] said [redacted] sent the file to [redacted] from her office Outlook e-mail account on or about October 27, 2011. She then approached [redacted] after she realized what she had done was wrong. [redacted] said that both [redacted] and [redacted] came to an agreement that if they could find someone whom they should report their conduct to they would, and so [redacted] was contacted by [redacted] added that the appraisal file may have been e-mailed or viewed on someone's desk. [redacted] the employee who is suspected of having downloaded or opened the file, had told [redacted] that the appraisal file was on the Treasury Department's web site. (Exhibit 3)

On November 4, 2011, TOIG interviewed [redacted] stated that she received an e-mail from another OIA employee. The e-mail and file attachment contained an Excel spreadsheet file containing performance ratings for employees of the OIA and DO Office of Security. [redacted] said she received the e-mail from IRS [redacted] told her the appraisal file was on the Treasury website and asked [redacted] if she wanted to see it. She responded that she did and [redacted] e-mailed the file to her. She opened the attachment not knowing that the appraisal information contained in the file attachment contained PII. [redacted] said she forwarded the file to one other person, [redacted] OIA IRS. [redacted] said both she and [redacted] could not believe the appraisal file was posted on the Internet. [redacted] said at first she did not delete the file or the e-mail. But she has since then deleted it. [redacted] said she socializes with [redacted] in the office. She did not tell anyone else about the file being on the Internet because she thought it may have been common knowledge that it was posted there. She described her receiving and opening the appraisal file as a "lapse in judgment". [redacted] added that she spoke with another IRS, [redacted] tried to find the file on the Internet and could not. They both decided to approach a friend who works in the front office at OIA, [redacted] to see if [redacted] had heard about the file. (Exhibit 4)

On November 8, 2011, TOIG interviewed [redacted] stated that approximately two to three weeks ago, she received an e-mail from another OIA employee. The e-mail and file attachment contained an Excel spreadsheet file containing performance ratings for employees of the OIA and DO Office of Security. [redacted] said she was told by the person who sent the file to her that it was posted on the DO. Local Area Network (LAN). A few days after she received the e-mail and file, the other employee, [redacted] told [redacted] to delete the e-mail. [redacted] said she learned that the appraisal information constituted an unauthorized disclosure of information. [redacted] said [redacted] had initially told her that the appraisal information was available and asked if she wanted to see her evaluation score. When she told [redacted] she would like to see her score and received the file from [redacted] she opened it, saw her evaluation rating, and then closed the file. [redacted] said she left the e-mail and attachment in her in-box. She said she did not send the file to anyone else. Later [redacted] told [redacted] that the appraisal information was not actually taken from the DO LAN. [redacted] said

[redacted] told her she received the appraisal spreadsheet from [redacted] said [redacted] is detailed to another government intelligence agency. (Exhibit 5)

On November 9, 2011, TOIG interviewed [redacted] A. [redacted] stated that a friend of his had mentioned to him that a file was going around the office and was located on one of the shared drives in the Office of Intelligence and Analysis. The file contained an Excel spreadsheet with the performance ratings for employees of the OIA and DO Office of Security. The friend, [redacted] gave [redacted] the location of the file on the office file server. [redacted] said she had received the file from another OIA employee, [redacted] That day, [redacted] said he looked for the file. He said it was listed under the folder name "OA (name)/resources." This is where office files are placed and available to other employees. He said he double-clicked on the file and it opened up to an Excel spreadsheet, containing OIA personnel appraisal information. [redacted] said he looked at the data for approximately one minute. [redacted] advised he did not print out or e-mail the file to anyone else. [redacted] said this occurred approximately on October 27 or 28, 2011. He said he then told [redacted] on the following Monday what had happened. [redacted] said [redacted] had been e-mailed the appraisal file by [redacted] sent it to another person, to whom [redacted] did not know. According to what [redacted] told him, [redacted] told her that the appraisal file was posted on the Treasury Internet web site. [redacted] was certain that the file was accessible without having to utilize a password or that no warning banner appeared telling a restricted file was being accessed. [redacted] said he thought [redacted] may have accessed another file on the classified server in the office. (Exhibit 6).

On November 29, 2011, TOIG interviewed [redacted] stated that he was looking for an electronic copy of his performance evaluation standards when he looked in a common folder and located a file on one of the shared drives in the OIA. The file contained an Excel spreadsheet with the performance ratings for employees of the OIA and Treasury DO Office of Security. [redacted] stated he was looking for an electronic copy because he had no paper copy of the performance evaluation standards. [redacted] was looking for FY2011 standards and working on completing his self-assessment that his office Director, [redacted], requested he complete.

The common folder [redacted] entered was a general shared OIA folder labeled "Performance" or "Evaluation", according to [redacted] stated that within the shared OIA folder he opened was the "HR" folder that contained the spreadsheet titled "2011 Standards", or "2011 Perf", according to [redacted] reported he had no problems accessing this file and that it contained no warnings or password protection. [redacted] stated he knows certain files labeled within the OIA network are not to be opened or accessed only if the need exists, for example, "U.S. Persons" (USP) files. However, [redacted] stated this was not a folder like USP and was in a shared folder.

The file had several spreadsheets [redacted] opened and closed once he determined the criteria for performance evaluation standards he was looking for was not in the spreadsheets. [redacted] stated the spreadsheets contained breakdown of employees within the OIA office and their individual evaluation ratings. [redacted] saved a copy to his personal folder on his H:\ drive under the username "[redacted] stated he did not manipulate any data within the file. [redacted] said performance

evaluations within OIA were going on during this time and not yet completed. [redacted] stated this incident occurred in or around mid-October. [redacted] stated as a part of his duties, he meets weekly with [redacted] every Tuesday afternoon.

[redacted] provided [redacted] with a hardcopy of the performance evaluation standards that he was searching for when he opened the file with performance ratings of employees within OIA. [redacted] stated that as a part of his duties, he also meets with [redacted] and during a meeting with her [redacted] mentioned the existence of the file with performance ratings. [redacted] requested that [redacted] e-mail her the file. [redacted] reported this meeting with [redacted] was a few weeks after the first time he accessed the file and evaluations were completed. [redacted] stated [redacted] seemed surprised that the file existed on the shared drive and requested [redacted] to send it to her to see if the ratings matched what they had received since evaluations had been completed. [redacted] stated his ratings on the spreadsheet in the file matched what he had received at the completion of his evaluation. [redacted] sent the file to [redacted] via e-mail through the VPN because [redacted] was detailed to another agency on the day he sent it to [redacted] [redacted] stated he did not send the file to anyone else and did not discuss the file with [redacted] after he sent it to her.

[redacted] stated he was unaware if [redacted] sent the file to anyone else or if anyone else received it or accessed it. [redacted] stated he only accessed the file twice, initially in mid-October and again to send it to [redacted] [redacted] stated he had taken PII online training in September or October of 2011. [redacted] stated he has not had any trouble or problems while working at Treasury and has received outstanding and excellent evaluations. [redacted] stated he gets along well with his supervisor, [redacted]

On November 1, 2011, [redacted] stated he was having his regularly scheduled meeting with [redacted] and after was told to meet with [redacted] and [redacted] the Deputy Assistant Secretary for Intelligence and Analysis. [redacted] stated that at the meeting, he was provided with a letter that he read over. [redacted] and [redacted] did not tell [redacted] what the letter pertained to and had [redacted] turn in all his access and employee identification cards. [redacted] stated he believed the incident described in the letter involved Bank Secrecy Act data that as a part of his duties, he regularly accesses. [redacted] said he was shocked to receive the letter and was escorted to his desk to get his belongings and placed on administrative leave. (Exhibit 7 and 8)

[redacted] provided a written statement to TOIG. (Exhibit 9)

On December 21, 2011, the Treasury Department Bureau of Public Debt (BPD), HR e-mailed TOIG a screen print out of [redacted] FY 2011 Privacy Awareness Course completion record. The training was completed by [redacted] on June 14, 2011. (Exhibit 10)

On December 23, 2011, TOIG collaborated with and interviewed [redacted] Systems Engineer, Treasury Office of the Chief Information Officer, to determine how Treasury employee [redacted] could have accessed a spreadsheet containing personnel evaluations. The file in question, FY2011 Performance Ratings – revised draft (2).xlsx, was located on a Storage Area Network (SAN) drive that was locally mapped to the F:\ drive on a Windows Server 2008 file server [redacted] The file

server then shared the F:\Department directory as the S:\ drive for users to connect to. Users who were able to map to the S:\ drive would be able to view the files and directories contained on it.

According to the login script (see below) which executed each time [redacted] logged on to the network, [redacted] H:\ drive was the file server's S:\ drive. [redacted] permissions were such that he could view and access most of the files and directories on the S:\ drive. Although [redacted] logon script permissions allow him to view the S:\ drive, the permissions enumerated above do not list his user account as a user or group that has access to the directory where the file was stored. [redacted] made multiple attempts to access the file using [redacted] account, to include using Windows Explorer, the command line interface, using a direct path to the file, attempting to open the file by using the full path in Excel, and attempting to access the file by logging in through terminal services. All attempts to access the file were unsuccessful. TOIG and [redacted] concluded that the most probable hypotheses to explain how [redacted] accessed the file were:

1) [redacted] utilized a third-party tool to elevate his privileges to an administrator account so that he could access the file.
2) [redacted] cracked the password of someone with access to file and logged in as that person to access the file.
3) (Most Probable) The permissions had been changed in the interim between when [redacted] claimed to have accessed the file and when TOIG and [redacted] began their inquiry. (Exhibit 11)

On December 30, 2011, TOIG re-interviewed [redacted] to determine if the file access permissions on the directory and personnel evaluations spreadsheet accessed by Treasury employee [redacted] in October 2011, were changed prior to TOIG's inquiry on December 23, 2011. [redacted] advised that when she became aware of rumors in late October 2011 that someone in OIA had accessed the spreadsheet containing the OIA FY 2011 personnel evaluations she requested that the Treasury DO IT Help Desk rename and restrict the directory the file was contained in. TOIG confirmed [redacted] statement with the DO IT Help Desk which reported that on October 26, 2011, [redacted] requested that the directory OIA Resources be renamed to OIA OPO and that access to that directory and all its sub-directories be restricted to [redacted] and [redacted] (an OIA subordinate of [redacted]. That request was handled by Help Desk Technician [redacted] and assigned ticket number [redacted]. (Exhibit 12)

Referrals

N/A

Judicial Action

N/A

Findings

During the course of this investigation, TOIG did not find any criminal or administrative misconduct. However, it is substantiated that [redacted] accessed the Excel spreadsheet file containing the OIA HR performance ratings for the most recently completed evaluation cycle. It has been determined that [redacted] had access to the folder containing the subject file during the time period in which he accessed it. [redacted] permissions were restricted blocking him from that folder after the incident.

Distribution

[redacted], Senior Advisor, Treasury Departmental Offices

Signatures

Case Agent:

[redacted] _____ 1-11-12
Date

Supervisor:

[redacted] _____ 1-11-12
Date

Exhibits

1. Memorandum of Activity, Interview of [redacted] Supervisory Operations Office and Intelligence Research Specialist, OIA, DO, dated November 1, 2011.

2. Memorandum of Activity, Records/Information Obtained of e-mails and the file attachment containing an Excel spreadsheet file with the performance ratings for employees of the OIA and Office of Security, dated November 1, 2011.

3. Memorandum of Activity, Interview of [redacted] Senior Advisor to DAS for Intelligence Community Integrity, OIA, DO dated November 3, 2011.

4. Memorandum of Activity, Interview of [redacted] Intelligence Research Specialist, OIA, DO, dated November 4, 2011.

5. Memorandum of Activity, Interview of [redacted] Intelligence Research Specialist, OIA, DO, dated November 9, 2011.

6. Memorandum of Activity, Interview of [redacted] Intelligence Research Specialist, OIA, DO, dated November 9, 2011.

7. Copy of the letter detailing administrative leave from OIA to [redacted] dated November 1, 2011

8. Memorandum of Activity, Interview of [redacted] Intelligence Research Specialist, OIA, DO, dated November 29, 2011.

9. Sworn statement of [redacted] dated November 29, 2011.

10. Memorandum of Activity, Records/Information Obtained of [redacted] FY 2011 Privacy Awareness Course completion record, dated December 21, 2011.

11. Memorandum of Activity, Interview of [redacted] Systems Engineer, DO, dated December 23, 2011.

12. Memorandum of Activity, Interview of [redacted] Supervisory Operations Office and Intelligence Research Specialist, OIA, DO, dated December 30, 2011.

REPORT OF INVESTIGATION
FMS-11-0723-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case Type: Criminal X
Administrative
Civil

Investigation Initiated: 03/04/2011

Investigation Completed: JAN 05 2012

Conducted by: [redacted]
Special Agent

Origin: Bureau Referral

Approved by: [redacted]
Special Agent in Charge

Case #: FMS-11-0723-I

Summary

On March 3, 2011, the Department of the Treasury Office of Inspector General (TOIG) was notified by the Financial Management Service (FMS) that a security camera had been moved and the computer controlling an industrial scanner may have been intentionally damaged at the Birmingham Debt Management Operation Center (BDMOC). (Exhibit 1)

TOIG's investigation determined that FMS Digital Scanning Technician [redacted] moved the camera and intentionally damaged the computer controlling the industrial scanner. The investigation was declined for prosecution by the United States Attorney's Office (USAO) for the Northern District of Alabama.

Basis and Scope of the Investigation

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] FMS Information Technology (IT) Specialist
- [redacted], FMS IT Specialist
- [redacted], FMS Program Manager
- [redacted], IBML Director of Information Technology
- [redacted] FMS Digital Scanning Technician

In addition, TOIG reviewed pertinent documents, including:

- Access Logs for BDMOC [redacted]
- Internet Usage for [redacted] and the shared account [redacted]
- Incident Report by FMS Threat Engineering and Operations Branch
- IBML Trouble Ticket and Incident Report

Investigative Activity

General Overview

The BDMOC supports the FMS delinquent debt owed to the government collection program. The BDMOC facility contains an IBML industrial scanner (Image Trac III, [redacted]) used to scan and digitize correspondence regarding debts. The IBML industrial scanner is located in the [redacted], sometimes referred to as the "vault." (Exhibit 2) The IBML industrial scanner and the [redacted] are monitored by an FMS Security Branch camera and access is controlled via electronic key cards/access badges: (Exhibit 1)

[redacted] the technical lead of BDMOC digital imaging operations described the work flow as follows: When mail arrives at the BDMOC it is scanned using the IBML industrial scanner which is controlled by a computer workstation (Computer Name: [redacted]) which can be accessed directly or over the network via a Remote Desktop Protocol (RDP) connection. The scanned images are stored on an external storage array located in the BDMOC Data Processing Branch, which is mapped as a shared drive on the IBML scanner workstation. Another computer workstation, the Returned Mail Processing Program PC (RMPPC) (Computer Name: [redacted]) is then used to transfer the images stored on the external storage array to the IBML Export Server (Computer Name: [redacted]) using an RDP session. [redacted] then initiates a secure FTP transfer of the images to the FMS Integrated Document Management System.

[redacted] is the Digital Scanning Technician who performs the duties described in the workflow above.

Until recently, the user account [redacted] was used to logon to all the computers involved in the scanning process. The password for this account was known to at least 5 people, including [redacted] (Exhibit 2)

{AGENT'S NOTE: An RDP session is a method of allowing a user on one computer to log on to a remote computer and run programs on the remote computer while viewing the results on their computer.}

Chronology

February 10, 2011 FMS Digital Scanning Technician [redacted] informs [redacted] that the IBML industrial scanner computer is not working between 1:30 and 2:00 CST. [redacted] confirms this. (Exhibit 2)

February 11, 2011 An IBML technician removed the IBML industrial scanner computer's hard drive and transports it to IBML corporate headquarters for repair. (Exhibit 3)

February 14, 2011 An IBML technician reinstalled the repaired hard drive into the IBML industrial scanner computer and full functionality was restored. (Exhibit 3)

February 17, 2011 During a review of security camera footage, FMS Security Officer [redacted] noticed that the security camera in the [redacted] had been moved and its field of vision faced the wall instead of the IBML industrial scanner. [redacted] reset the security camera to cover its original field of vision. (Exhibit 1)

February 25, 2011 During a review of security camera footage, FMS Security Officer [redacted] noticed that the security camera in the [redacted] had been moved and its field of vision faced the wall instead of the IBML industrial scanner. [redacted] reset the security camera to cover its original field of vision. (Exhibit 1)

IBML Drive Repair, Analysis and Damage Assessment

On February 11, 2011, [redacted], the IBML Director of Information Technology began the repair of the IBML industrial scanner computer by verifying that its partition table had been altered and that the entry for the Linux partition had been removed, but that the Windows partition (and the Windows operating system) still existed. The removal of the Linux partition eliminated the configuration files for the boot loader program (grub) which rendered the computer unbootable, i.e. when the power is turned on, the computer cannot load (boot) the operating system.

[redacted] attempted to recreate the Linux partition and reinstall the Linux operating system, but was unsuccessful. [redacted] then copied the Windows partition to another hard drive, and re-imaged the IBML industrial scanner computer hard drive using another similar scanner computer hard drive. [redacted] then reinstalled the Windows operating system files from the original scanner computer to new Windows partition. The recovery operation was successful and the original hard drive was installed it back into the IBML industrial scanner at the BDMOC on February 14, 2011.

In his email dated March 7, 2011, [redacted], the IBML Director of Support Services, stated that: "In our service history, this error has only happened one time before, and that was a situation where an ibml employee deleted the partition because it had been created incorrectly."

"It would be difficult to find the root cause of this issue to any degree of certainty. IBML has hundreds of servers around the world that said, we have a good history of the "normal" things that happen. This is not one of those. Ruling out any corruption to the partition leaves only that it was removed by someone. This of course is an educated guess."

The BDMOC is covered by a maintenance agreement with IBML so there was not an additional cost incurred for the repair of the scanner computer's hard drive. However, [redacted] stated that cost to repair the scanner computer's hard drive would be $3000 (10 hours at a billing rate of $300/hour) absent such an agreement. (Exhibit 3)

FMS Incident Inquiry

[redacted], an IT Specialist in the FMS Threat Engineering and Operations Branch provided a summary of his findings regarding the incident involving the IBML industrial scanner located at the BDMOC which identified the following significant occurrences:

1) On February 10, 2011 at 12:49:53 PM, an RDP session from the user account [redacted] on the FMS computer workstation [redacted] (the computer that controls the IBML industrial scanner) was initiated to the FMS server [redacted].

2) On February 10, 2011 at 1:09:25 PM, the user account [redacted] created a PDF of the document http://www.ehow.com/how_6026_format-hard-drive.html.

3) On February 10, 2011 at 1:23:36 PM, the user account [redacted] logged off the server [redacted], terminating the RDP session.

[redacted] confirmed the time zone setting for the [redacted] computer as GMT-6 or Central Standard Time. (Exhibit 4)

Gunther Room Access Logs

The access logs for the [redacted] for February 10, 2011 show the following individuals entering and exiting the [redacted] and [redacted] are contract security officers, [redacted], [redacted] are FMS employees with work related reasons to briefly enter the [redacted]. [redacted] and [redacted] are FMS IT Specialists who were working on updating computers in the [redacted].

Name	Time In	Time Out	Duration (M:S)
[redacted]	04:54:24	04:55:45	1:31
[redacted]	07:55:06	07:55:28	:22
[redacted]	08:51:29	08:52:01	:32

[redacted]	08:58:03	08:58:17	:14
	09:04:16	09:19:00	14:48
	09:47:33	09:52:13	4:40
	09:47:35	09:49:27	1:52
	10:01:08	10:03:27	2:19
	10:04:10	10:38:22	34:12
	10:25:13	10:29:18	4:05
	11:16:57	11:41:25	24:28
	11:56:24	12:07:33	11:09
	12:23:18	12:40:36	17:18
	12:41:24	13:40:38	59:14
	12:43:26	13:24:57	41:31
	13:42:10	13:42:54	:44
	13:43:50	13:55:12	11:22
	13:43:52	13:49:58	6:06
	13:53:01	13:55:09	2:08
	14:23:34	14:55:08	31:34
	15:07:41	15:33:33	25:52
	15:25:56	15:29:42	3:46
	15:33:58	15:41:43	7:45
	17:20:30	17:21:23	:53
	23:10:45	23:12:13	1:28

(Exhibit 5)

[redacted] Interview

As one of the two individuals who spent the most time in the [redacted], FMS IT Specialist [redacted] was interviewed by TOIG.

On February 10, 2011, [redacted] was working the [redacted] to install and configure computers for issue to FMS employees. FMS Digital Scanning Technician [redacted] was also in the [redacted] working at the IBML industrial scanner. TOIG asked [redacted] specifically if he damaged the IBML scanner and he replied "no."

[redacted] first became aware that the computer controlling the IBML scanner was damaged when FMS Branch Manager [redacted] asked him not to talk about the incident and that it was under investigation. [redacted] stated he initially surmised that the damage may have been caused by a virus. He then said that he didn't think that anyone would damage the IBML scanner computer intentionally, especially since their actions could easily be tracked. [redacted] also commented that he did not think anyone was "tech savvy" enough to damage the IBML scanner computer.

[redacted] was asked by FMS Security Officer [redacted] to review the server [redacted], since that computer could be accessed from the IBML scanner computer and during the course of his review,

noticed [redacted] Facebook page in the Address Bar of the Internet Explorer web browser installed on the computer.

{AGENT'S NOTE: Internet Explorer by default saves websites that users visit and displays them in the Address Bar's pull down menu.}

TOIG asked if he moved the FMS Security Branch camera in the Gunther Room and [redacted] replied "no." (Exhibit 6)

[redacted] Interview

After initially denying it, [redacted] admitted to moving the FMS security camera installed in his work space as documented in FMS Security Branch Initial Inquiry Forms dated February 22, 2011 and February 28, 2011. (Exhibit 1) When asked by the TOIG why he moved the cameras, [redacted] replied that he didn't like being spied on and expanded that he occasionally took breaks when he was supposed to be working. When the TOIG asked if he took naps, [redacted] replied that he rarely did, but became tired during his duty hours because he was doing the work of two employees. After the incident documented in the FMS Security Branch Initial Inquiry Forms, [redacted] stated he was told by his branch manager [redacted] that he was not allowed to move FMS security cameras.

[redacted] also stated that he did not feel comfortable interacting with his direct supervisor [redacted]. [redacted] stated that [redacted] accused him of making a "smart" remark concerning a co-worker and then refused to provide the same training that was offered to other employees [redacted] supervised. When [redacted] asked [redacted] if he could have the training, [redacted] answered that he'd like to have a million dollars – implying that [redacted] would not be receiving the training.

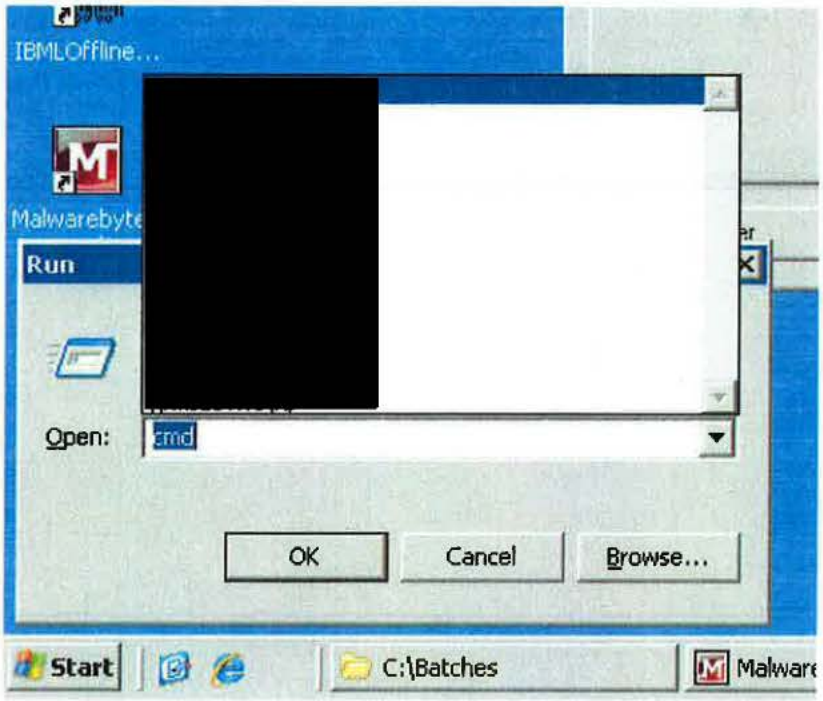
After a second series of denials and obfuscation, [redacted] also admitted that on February 10, 2011 he ran commands on the computer that controlled the IBML industrial scanner which rendered it unbootable. [redacted] explained his actions by stating that he was merely trying to learn more about how computers worked. [redacted] could not provide an explanation for his failure to inform FMS Technical Lead [redacted] that his actions rendered the IBML scanner computer unbootable when he reported the issue to [redacted] on February 10, 2011.

[redacted] also admitted to searching the Internet for instructions on how to format a hard drive and admitted to running a series of commands relating to formatting a hard drive on the [redacted] server.

[redacted] provided a written, three-page, signed, sworn statement. (Exhibit 7)

Format Commands on the [redacted] Server

During [redacted] interview he referenced observing commands typed into the Windows Run window of the [redacted] server and supplied a screenshot on March 15, 2011 at 2:38 PM. showing the Windows Run command window with a series of previously entered commands by individuals logging into the [redacted] account.



{AGENT'S NOTE: The Run window is an optional component of the Windows Start Menu, that provides a place for a user to enter and execute a command line program without having to launch the Windows command shell. By default, the Windows operating system saves previously entered commands as an enhancement to the user experience so that a user could easily execute previously typed commands.}

The previous commands listed in the Run window box can be defined as follows:

cmd	Opens a Windows command shell or DOS prompt
Format c	The command to format (create a news file system) the primary partition on a hard drive, not valid without a colon after the c
format hard drive	The command to format a hard drive, the words "hard drive" are incorrect parameters to the format command
format c:/s	The command to format the c: partition, the /s is a command switch that instructs the format command to copy system files to the newly formatted c: drive. The lack of a space between the c: and the /s prevents the command from executing.
ms dos	Not a valid command
[redacted]	The command to access a windows shared drive on a computer
[redacted]	The command to access a windows shared drive on a computer

notepad	The command to open the windows text editor
regedit	The command to open the Windows registry editor
[redacted]	The command to display windows system information
[redacted]	The command to access the default shared drive on a computer
[redacted]	The command to access a windows shared drive on a computer

(Exhibit 8)

[redacted] Internet Usage

Web browsing logs for the account associated with [redacted] from February 7 – 11, 2011 were collected from the Internet content filter and proxy server Websense by [redacted] of the FMS Threat Engineering & Operations Branch. No indications of suspicious activity were identified.

The web browsing logs from the computer [redacted] spanned approximately 18 minutes on February 10, 2011. According to [redacted], this represented the only web browsing on the computer between February 9 – 11, 2011.

The time zone setting for the Websense proxy server is Eastern Standard Time (GMT-5) and is reflected on the attached Websense logs. The times below have been converted to Central Standard Time for ease of comparison.

Relevant Web Browsing Activity

13:07:07 http://www.ehow.com/how_6026_format hard-drive.html

In Step 1 of Preparation section readers are cautioned that: "When you format a computer hard drive you will lose everything that is on the drive. Therefore, it is very important to back up anything you might want later."

13:12:49 http://www.mahalo.com/ how-to-format-a-hard-drive

In the third paragraph readers are cautioned to: "Back up any important information prior to starting the formatting process because the information on your drive will not be accessible after you have finalized the formatting process."

This caveat is followed by a section titled: Step 1: Back Up All of The Data On Your Hard Drive.

13:16:41 http://www.webopedia.com/DidYouKnow/hardware_software/2005/hard drive.format. Asp

[redacted] was clearly aware that his actions were not approved and potentially illegal as evidenced by his use of a shared login account rather than his personal login account in an attempt to conceal his Internet research, his decision not to inform FMS management that his actions caused the damage and his initial denials and obfuscations to TOIG.

Distribution

[redacted], Assistant Commissioner for Management, FMS

Signatures

Case Agent:

[redacted]

[redacted]

12/30/2011
Date

Supervisor:

[redacted]

[redacted]

1-5-12
Date

Exhibits

1. FMS Security Branch Initial Inquiry Forms and Video dated March 3, 2011
2. Memorandum of Activity, Interview of [redacted] dated March 15, 2011
3. Memorandum of Activity, Interview of [redacted], dated April 14, 2011
4. Memorandum of Activity, Interview of [redacted], dated March 29, 2011
5. Memorandum of Activity, [redacted] Access Logs, dated April 5, 2011
6. Memorandum of Activity, Interview of [redacted], dated April 12, 2011
7. Memorandum of Activity, Interview of [redacted] dated April 12, 2011
8. Memorandum of Activity, Information supplied by [redacted] dated March 29, 2011
9. Memorandum of Activity, Web Browsing Logs, dated March 29, 2011
10. Memorandum of Activity, Microsoft Knowledge Base Article, dated April 29, 2011
11. Memorandum of Activity, Interview of [redacted], dated April 12, 2011
12. Memorandum of Activity, Position Description and Performance Plan, dated April 19, 2011
13. Memorandum of Activity, Case Presentation, dated May 3, 2011
14. Memorandum of Activity, Case Declination, Dated November 17, 2011

REPORT OF INVESTIGATION
FMS-11-1579-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case #: FMS-11-1579-I

Investigation Initiated: September 20, 2011

Case Type: Criminal X
Administrative
Civil

Investigation Completed: MAR 23 2012

Conducted by: [redacted]
Special Agent

Origin: [redacted], Financial Management Service

Approved by: [redacted],
Special Agent in Charge

Summary

On September 20, 2011, a preliminary investigation was initiated by the Treasury Office of Inspector General (TOIG), Office of Investigation (OI), after receiving notification from the Financial Management Service (FMS) that on September 6, 2011, two individuals, identified as [redacted] and [redacted] traveled over 400 miles to the FMS, Birmingham, AL facility (FMS-Birmingham) to attempt to negotiate a fraudulent bond valued at $100 Billion. The individuals never entered the facility grounds, but were stopped and questioned by FMS security. The individuals submitted identification and documentation of their alleged bond. Federal Protective Service was called and arrived on the scene and questioned the individuals. The subjects claimed that they received the information on how to negotiate the bond on a Sovereign Citizen website. During questioning and search, one of the subjects possessed a handgun along with an Alabama concealed carry permit. The subjects were informed that FMS could not assist them with their request and they were directed to leave the premises.

On November 21, 2011, TOIG contacted Assistant United States Attorney (AUSA) [redacted] United States Attorney's Office (USAO), Northern District of Alabama (USAALN) for prosecutorial determination.

On January 18, 2012, AUSA [redacted], USAO, USAALN declined prosecution of this case.

This investigation substantiated that [redacted] and [redacted] appeared at the FMS, Birmingham, AL facility to ask about how to redeem a fraudulent U.S. Treasury bond.

Basis and Scope of the Investigation

During the course of the investigation, relevant interviews were conducted with:

- [redacted], Special Agent, Treasury Inspector General for Tax Administration (TIGTA)
- [redacted], Special Agent, TIGTA
- [redacted] Special Agent, Federal Protective Service (FPS)
- [redacted], Special Agent, FPS
- [redacted] Inspector, FPS
- [redacted] Detective, [redacted] (AL) Police Department
- [redacted] Subject

In addition, TOIG reviewed pertinent documents, including:

- Incident report from FPS, dated September 6, 2011.
- National Crime Information Center checks for [redacted] and [redacted]

Investigative Activity

On September 20, 2011, a preliminary investigation was initiated by TOIG, after receiving notification from the FMS that on September 6, 2011, two individuals, identified as [redacted] and [redacted] traveled over 400 miles to the FMS, Birmingham, AL facility (FMS-Birmingham) to attempt to negotiate a fraudulent bond valued at $100 Billion. (Exhibit 1)

On September 21, 2011, TOIG conducted criminal history checks on [redacted] and [redacted] A criminal history check on [redacted] revealed convictions to include: threat to kill, terroristic threats and aggravated assault. A criminal history check on [redacted] revealed a conviction for possession of stolen property, possession of controlled substance, and burglary. (Exhibit 2)

On November 7, 2011, TOIG spoke to [redacted] Special Agent, FPS. [redacted] is the FPS Agent that had contact with subjects [redacted] and [redacted] at the FMS Facility in Birmingham, AL.

[redacted] said that they did not open a case on the subjects. [redacted] said that they did not make any threats and were trying to access their Treasury account that they learned about on a Sovereign Citizen website called **www.theredemptionservice.com**. (Exhibit 3)

On November 18, 2011, TOIG spoke to [redacted] Special Agent, TIGTA. Franklin is TIGTA's representative to the Domestic Terrorism Operations Unit at the Federal Bureau of Investigations (FBI) Headquarters. [redacted] checked FBI terrorism databases for both subjects and reported no record of either individual. (Exhibit 4)

On January 25, 2012, TOIG re-interviewed [redacted] Special Agent, FPS.

[redacted] said that he and FPS Inspector [redacted] arrived at FMS-Birmingham after they were called by FMS security that two individuals arrived at the employee gate trying to get information on cashing an $100,000,000,000 (100 Billion) bond. [redacted] said that the subjects were compliant and were not acting suspiciously. [redacted] felt that the subjects were there to see what would happen when they presented the bond. He felt that they actually thought they could possibly cash it.

[redacted] was asked about the comment that was included in the FMS security report that the subjects were trying "to see what would happen. It is unclear if this means they intended to actually enter the premises only or to test the security procedures and response." [redacted] said, "that shouldn't have been put in there. They were not threatening." [redacted] said that was not their report and they wouldn't have put that in there because he felt they were just trying to cash the bond. [redacted] said that FPS did not open a case on the incident.

[redacted] said that the subjects mentioned that they learned about cashing the bond on the internet and [redacted] believes all the forms that were presented were from that website. [redacted] recognized it immediately as a "sovereign type" thing.

[redacted] said that when the subjects were asked if they had any weapons, the passenger (he couldn't recall which [redacted] it was) said they did and voluntarily allowed the FPS Agents to store the weapon during the interview. [redacted] said that they had a valid permit to carry the weapon and were forthcoming about having it.

[redacted] said that he contacted the Alabama Fusion Center, North Florida Fusion Center and local police regarding the [redacted] None were aware of the subjects or have record of past incidences.

[redacted] said that given the time since the incident and that there are no other contacts, he doesn't think there's an issue. (Exhibit 5)

On January 25, 2012, TOIG interviewed [redacted] Inspector, FPS, Birmingham, AL. [redacted] was the responding FPS Inspector that had contact with Subjects [redacted] and [redacted] at FMS-Birmingham.

[redacted] said that he and SA [redacted] arrived at FMS-Birmingham after they were called by FMS security that two individuals arrived at the employee gate trying to get information on cashing a $100,000,000,000 (100 Billion) bond. [redacted] said that the subjects were "very compliant". [redacted] felt that the subjects "actually thought they could speak to somebody about cashing the bond". He never felt that they were acting suspiciously and figured that the subjects "would never know what you can get (cashing the bond) unless you ask." [redacted] said that after they were told that they could not cash it, they seemed "OK with it" and got back in their truck and left. They never got upset.

[redacted] was asked about the comment that was included in the FMS security report that he reported "that the individuals drove the four hours to see what happened when they showed up". [redacted] said

that they did drive four hours, but the rest of the comment about trying to see what would happen is out of context. [redacted] said that after the interview, he was speaking to some of the security guards in conversation and they were kicking around all sorts of ideas as to why they would have come. [redacted] said that was one of about 10-15 reasons they were kicking around, but he did not believe that to be the case. He believes they were just trying to see if they could cash the bond.

[redacted] was asked about the weapon that the passenger had. [redacted] said that before the interview started they asked the subjects if they had any weapons and that they said that they did. They voluntarily surrendered the weapon to the FPS Agents for the duration of the interview. When the weapon was retrieved, [redacted] said that it was unloaded and in a gun case "and way back in the backseat" of the double cab of the truck. It was not easily accessible. [redacted] said [redacted] had a valid Alabama concealed weapon permit. [redacted] said that when asked why they had the weapon, the subject responded that everybody has one in Alabama. (Exhibit 6)

On February 6, 2012, TOIG spoke telephonically to [redacted] said that he has been doing research about revoking his "strawman account" with the government and how to receive his allowance. [redacted] said that he found out about how to do it through the website "redemptionservice.com", which he believes is based out of Illinois. He said that he went to the FMS-Birmingham facility because it was the closest Treasury facility to his house and thought that he may have to show up at a Treasury facility to get a "starter check" for his account. [redacted] said that his brother [redacted] was with him to drive him to Birmingham. Attempts to locate [redacted] met with negative results. [redacted] said that when he was told that he couldn't do it there, he understood and came back home. When mentioned to him about showing up at a Treasury facility, [redacted] said, "Oh no, I won't be doing that anymore." [redacted] said that he was very appreciative to the FPS Agent who told him that he couldn't just start writing checks off this account because that's how people get in trouble. [redacted] said that he was very glad that he was told this because he was going to start writing checks and didn't want to do anything illegal.

[redacted] said that he found out that he has to spend more money in order to purchase a CD with more information about the proper paperwork to file with the Internal Revenue Service in order to receive his money. (Exhibit 7)

On February 13, 2012, TOIG interviewed [redacted] at his residence. [redacted] said that he drove to the FMS-Birmingham because he thought that was the place to go to get starter checks off his "strawman account". [redacted] said that he went to FMS-Birmingham because it was the closest Treasury facility and he didn't want to travel to Washington, DC. He and his brother thought the FMS-Birmingham facility was going to be similar to a bank and he would be able to go through a "drive-through". [redacted] said that when he saw that it wasn't like that, they went to the gate and pushed the button. He said that the security at the facility asked for the bond and his documentation, but he didn't want to give his originals so they left and made a copy and came back. [redacted] says he remembers the "Homeland Security" Agent telling him that there may be a way to get his money, but it was not going to happen "today" and "this is not how it is done". [redacted] said that the agent told him that he cannot write checks off this account and [redacted] was very appreciative that he was told this, because he doesn't want to get in trouble for doing it the wrong way.

During the course of the interview, TOIG noticed what appeared to be a "Sovereign Citizen" identification card on [redacted] counter. [redacted] said that he purchased the card for $80 on the internet. During the course of the interview, [redacted] became upset by the perceived questioning of his beliefs and his tax filing status and said, "I invited you into my house, you can't talk to me that way" and ordered TOIG to leave his residence. While leaving his residence, TOIG reminded [redacted] that he could not show up at Treasury facilities and [redacted] replied that he had no plans to. (Exhibit 8)

On February 13, 2012, TOIG met with Detective [redacted] Police Department. [redacted] was informed that TOIG had just interviewed [redacted] in regards to his showing up at the FMS-Birmingham facility to try to cash a bond for $100 Billion. [redacted] said that he did not know of [redacted] but they have seen an increase in Sovereign Citizen activity in the recent past.

[redacted] provided a current driver's license photo and vehicle information. [redacted] ran a database check for local criminal history and reported that [redacted] did not have a record in their database. (Exhibit 9)

Referrals

On November 21, 2011, TOIG presented this case to AUSA [redacted], USAALN to determine the prosecutorial merit. [redacted] said that he was going to pass the information to AUSA [redacted] Terrorism section. (Exhibit 10)

Judicial Action

On January 18, 2012, AUSA [redacted], USAALN declined prosecution of this case based on the fact that the case does not rise to the level that he thinks could result in a successful prosecution. (Exhibit 11)

Findings

The investigation determined that [redacted] and [redacted] did appear at FMS-Birmingham facility to obtain information on how to redeem a fictitious Treasury Bond that they created based on information from the Sovereign Citizen website theredemptionservice.com.

Based on the findings of the investigation, the following pertinent statutes were violated and can be applied to the case:

- 18 USC 514: Fictitious obligations

Distribution

[redacted], Chief Security Officer, FMS

Signatures

Case Agent: [redacted]

[redacted] 3/23/2012
Signature Date

Supervisor [redacted]

3-23-12
[redacted]
Signature Date

Exhibits

1. Initiation documents, dated September 7, 2011.
2. Memorandum of Activity, NCIC records checks, dated January 24, 2012.
3. Memorandum of Activity, Interview of [redacted] FPS dated November 21, 2011.
4. Memorandum of Activity, Interview of [redacted], TIGTA dated November 21, 2011.
5. Memorandum of Activity, Interview of [redacted] FPS dated January 25, 2012.
6. Memorandum of Activity, Interview of [redacted] FPS dated January 25, 2012.
7. Memorandum of Activity, Interview of [redacted] dated February 6, 2012.
8. Memorandum of Activity, Interview of [redacted] dated February 13, 2012.
9. Memorandum of Activity, Interview of Detective [redacted] Elberta PD, dated February 13, 2012.
10. Memorandum of Activity, case presentment to AUSA, dated December 21, 2011.
11. Memorandum of Activity, case declination from AUSA, dated January 18, 2012.

REPORT OF INVESTIGATION
FMS-12-1644-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Financial Management Services (Legacy)

Case #: FMS-12-1644

Case Type: Criminal ___ Administrative X Civil ___

Investigation Initiated: May 2, 2012

Investigation Completed:

Origin: Anonymous

Conducted by: [redacted]
Special Agent

Approved by: [redacted]
Special Agent in Charge

Summary

On April 30, 2012, the Department of Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG) received information via email from a legacy Financial Management Services (FMS) employee who alleged disregard for policies, processes and procedures with the FMS/DMS Apple Ipad implementation program in Birmingham, AL. (Exhibit 1)

The investigation determined the allegations are unfounded. No facts were uncovered to support the allegations.

Basis and Scope of the Investigation

On April 30, 2012, TOIG received information via email from a legacy FMS employee who alleged disregard for policies, processes and procedures with the FMS/DMS Apple IPad implementation program in Birmingham, AL.

During the course of the investigation, TOIG conducted relevant interviews with:

- FMS/DMS Employee One
- FMS/DMS Employee Two
- [redacted] Former Assistant Commissioner, FMS/DMS
- [redacted] Assistant Commissioner, FMS/DMS

In addition, TOIG reviewed pertinent documents, including:

- DMS iPad Ground Rules

Investigative Activity

In an interview with TOIG, FMS employee one stated FMS has a pilot program involving Apple IPads' and MacBook. The program was implemented by Former Assistant Commissioner [redacted] There is no accountability for this equipment. The equipment, which has been purchased over a two year period, has never been inventoried and as a result not bar coded. Information technology (IT) personnel only knows about the Apple equipment if the employee has configuration issues and asks for IT support. It is impossible to determine who at FMS is issued the Apple products. In addition, IT has never been asked to draft any guidance, policy, or rules and regulations their use. FMS has also purchased MiFi's for the Mac's and this allows them to bypass FMS security protocols. IT personnel learned about the MiFi's in the same manner as they learned about the IPads and MacBooks. Nothing is encrypted and any PII that FMS possesses is at great risk. The employee also stated they heard that [redacted] reportedly instructed FMS Managers and Directors that when they can retire they will be able to keep their IPads. (Exhibit 2)

In an interview with TOIG, FMS employee two stated there were irregularities regarding the FMS purchase of Apple Mac Book Computers and IPads by FMS personnel. There was no accountability and IT had been unable to locate any requisition documents from the employees who obtained them. There were no barcodes and it is believed there may be approximately 20 in circulation. The IT section at FMS–Birmingham finds out about the computers when they are brought in by employees and the employees request configuration. The employee stated that within the last couple of weeks FMS Management has been taking action to correct the accountability issue and recently sent an email to IT employees to stop looking into the issue.

Employee two also stated they had no firsthand knowledge but heard a rumor that employees who had IPads could keep them as gifts when they retired. (Exhibit 3)

In an interview with TOIG, [redacted] stated he is currently a Senior Advisor for FMS and is the point of contact for FMS regarding the merger between them and the Bureau of Public Debt. [redacted] was the Assistant Commissioner for FMS, Debt Management Services in Birmingham, AL and Austin, TX for approximately two years from January 2009 to January 2011. [redacted] stated he was based out of Washington, D.C. while Assistant Commissioner, but traveled extensively back and forth. [redacted] stated he did not have any knowledge of the allegations and this was the first he had heard of them.

[redacted] stated the allegation regarding employees retiring from FMS could retain their FMS issued MacBooks was false. [redacted] stated he would have never said anything like that. [redacted] stated in the spring of 2009 he started the MacBook program and Apple products acquisition when he was Assistant Commissioner. The concept behind the program was to enhance communications and communications only. The program was not implemented for anyone to use the MacBooks for PII or Sensitive But Unclassified (SBU) and that was clearly explained to staff when he had oversight of Debt Management.

When [redacted] was Assistant Commissioner, he originally authorized Senior Level employees (approximately 6-10), then Branch Managers (GS-14's and above) to have MacBooks. [redacted] believed there were approximately 20 MacBooks purchased when he was Assistant Commissioner. All the MacBooks would have been purchased through FMS' acquisitions process using credit cards. The MacBooks were bar coded; however, IPads and IPhones, which were added on at a later point, were not because they were below the $1000 threshold for accountable property. All the MacBooks had security features such as WPA and WPA2 and GOOD for Enterprise for email. FMS's IT staff was not involved in the decision to purchase but they had full knowledge of the purchases. [redacted] reiterated the Apple products were never intended as a portable portal for PII information and was to be used only for communications and to assist in productivity. [redacted] stated no formalized policy was issued but there was an internal policy. [redacted] also had Apple Technical personnel provide training to those employees who were issued MacBooks. (Exhibit 4)

In an interview with TOIG, [redacted] stated that employees using the MacBook follow FMS' laptop guidelines and all MacBook's are inventoried, managed and supported by FMS. All employees who are in possession of these devices are aware of the rules. When employees in Birmingham, AL obtain a MacBook, iPad or a Media Tablet they receive briefings about the approved uses. (Exhibit 5)

In a TOIG document review of the IPad Pilot Ground rules the following was noted: All employees would comply with FMS policies regarding sensitive data. Citrix connections could not be supported from IPads, funding for acquisition, monthly access charges and accessories

would be funded by FMS. In addition, lost or stolen IPads would be reported immediately to FMS, remotely wiped and a new one acquired by the designated IPad pilot coordinator. The distribution of the IPads would be limited to FMS senior management and other unidentified FMS employees. (Exhibit 6)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined the allegations are unfounded. No facts were uncovered to support the allegations.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policy(ies) were violated or could be applied to the case:

- N/A

Distribution

N/A

Signatures

Case Agent:

[redacted]

12/21/2012
Date

Supervisor:

[redacted]

12-21-12
Date

Exhibits

1. Initial Complaint document, dated April 30, 2012.
2. Memorandum of Activity, Interview of Confidential Complainant, dated May 9, 2012.
3. Memorandum of Activity, Interview of Confidential Complainant, dated May 11, 2012.
4. Memorandum of Activity, Interview of [redacted] dated July 3, 2012.
5. Memorandum of Activity, Interview of [redacted] dated August 27, 2012.
6. Memorandum of Activity, Review of iPad Pilot Ground Rules, dated December 12, 2012.

REPORT OF INVESTIGATION
FMS-12-0747-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: Fraudulent Use of Treasury Routing and Transit Number Multiple Subjects

Case #: FMS-12-0747-I

Case Type: Criminal X
Administrative ____
Civil ____

Investigation Initiated: February 22, 2012

Investigation Completed: SEP 12 2012

Conducted by: [redacted]
Special Agent

Origin: [redacted]
Security Specialist
Financial Management Services

Approved by: [redacted],
Special Agent in Charge

Summary

On February 22, 2012, the U.S. Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG), initiated an investigation based on allegations received from the Financial Management Services (FMS) concerning the fraudulent Automated Enrollment (ENR) entries coming into FMS under the Routing and Transit Number (RTN) [redacted].

The investigation determined that the allegation was substantiated. However, after exhausting all investigative leads and not being able to locate many of the subjects identified by FMS, and being declined for criminal prosecution, it was determined this matter lacks further investigative merit. There was no monetary loss to the United States Government.

Basis and Scope of the Investigation

This investigation was initiated on February 22, 2012, based on information forwarded by Eastmond Buckner, Security Specialist, FMS, concerning allegations fraudulent ENR entries coming into FMS under RTN [redacted]. An initial inquiry by FMS revealed multiple individuals who used the Treasury RTN to conduct 88 fraudulent transactions totaling $195,523.31. **(Exhibit 1) (Exhibit 3)**

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Kansas City Financial Center, FMS, Kansas City, MO
- [redacted] Supervisory Manager Program Analyst, FMS, Kansas City, MO
- [redacted] Kansas City, MO

TOIG reviewed pertinent documents, including:

- Excel Spreadsheet generated by FMS containing ENR debits and the names and social security numbers of the alleged individuals that completed the transactions
- Excel Spreadsheet generated by FMS with payee's bank information

Investigative Activity

In an interview with TOIG, [redacted] stated the ENR used for the transactions are for enrollment entries with zero dollars attached. The primary users of these particular ENRs are recipients of government benefits dispersed by FMS, such as social security. If the benefit recipient is interested in their benefits being directly deposited into their bank account then they would contact their banking institution. The bank takes the benefit recipient's information (i.e. social security, date of birth, etc.) and attaches it to an ENR record, which is sent to the National Automated Clearing House (ACH) for processing.

ACH, which is operated by the Federal Reserve Board (FRB), looks at the RTN and forwards the transaction to the appropriate financial institution. In this case, the RTN used belonged to Treasury; therefore FRB temporarily seized payment from Treasury. Treasury identified the transaction to be fraudulent and rejected the transaction. The money was eventually refunded to Treasury by FRB

Although [redacted] is not certain how the individuals got the RTN, he stated the number is legitimately published by FRB through the Federal Reserve Routing Payment Directory located at www.federaldirectory.frb. [redacted] stated the individuals used the Treasury RTN and their social security numbers as account numbers to make web bill payments.

[redacted] stated FMS contacted some of the individuals that initiated these transactions. They informed FMS they were entitled to the funds. [redacted] provided TOIG with an Excel spreadsheet that contained the dates, social security numbers, and names used to conduct the transactions. As well as the monetary amount the individuals attempted to steal from the Treasury. **(Exhibit 2)**

A document review conducted by TOIG revealed from January 2012 to February 2012, approximately 26 individuals used Treasury RTN [redacted] to conduct 88 fraudulent transactions totaling $195,523.31. In some instances, the same social security number was used for multiple individuals. FMS identified five individuals who attempted to steal the highest dollar amount, which included [redacted] **(Exhibit 3)**

In an interview with TOIG, [redacted] stated FMS was able to determine that [redacted] attempted to pay Chevron and Walmart, while [redacted] submitted payments to Chase credit card, Dish Network, AT&T, and Sprint. According to HSBC bank, [redacted] went online and set up the payment on January 17, 2012. FMS telephonically spoke to [redacted], who was certain that he was entitled to the funds. [redacted] stated FMS also telephonically spoke to [redacted], who admitted to using the Treasury RTN. FMS asked [redacted] how she acquired the RTN. [redacted] stated that you have to search the internet for the right thing. **(Exhibits 4)**

In an interview with TOIG, [redacted] stated his father, [redacted] came home one day and said his co-worker knew how to retrieve money from the United States Treasury that belonged to American citizens. [redacted] could not recall the co-worker's name. [redacted] along with [redacted] mother, consented to having the co-worker use their social security numbers to pay their bills. [redacted] was aware that a United States Treasury RTN was being used for the transaction. [redacted] allowed his father's co-worker to pay a Kansas City Power and Light utility bill on his behalf. [redacted] repeatedly denied paying the bill himself. [redacted] stated that the transaction was not successful and he eventually paid the bill.

[redacted] stated his father formerly worked at Oppenheimer & Co, however, retired five to six months ago. According to [redacted] both his parents left for Ecuador shortly after his father retired. [redacted] provided TOIG with an email address [redacted] for his father and stated that his parents cannot be reached via telephone. **(Exhibit 5)**

[**Agent's Note:** TOIG contacted SECTOR to determine if [redacted] were in the United States. SECTOR informed TOIG that both [redacted] left the United States on March 6, 2012 and returned May 1, 2012 from Guayaquail-Simon Bolivar airport. Their point of entry was Miami, FL. TOIG visited several employment and home addresses of

the aforementioned subjects provided by FMS and performed various investigative queries. However, were unable to locate them.]

Referrals

The investigation was declined for criminal prosecution by [redacted], Assistant United States Attorney (AUSA), United States Attorney's Office, Western District of Missouri, involving a potential violation of 18 USC 1343 (Wire Fraud).

Judicial Action

N/A

Findings

The investigation determined that the allegation was substantiated. However, after exhausting all investigative leads and not being able to locate any of the subjects identified by FMS it was determined this matter lacks further investigative merit. Furthermore, there was no monetary loss to United States Government.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policy(ies) were violated or could be applied to the case:

18 U.S.C. § 641 -Public money, property or records
18 USC 1343 -Wire Fraud

Distribution

[redacted] Chief Security Officer, Financial Management Services

Signatures

Case Agent:

[redacted]

9/11/12
Date

Supervisor:

[redacted]

9-11-12
Date

Exhibits

1. Lead Initiation Document, dated February 7, 2012.
2. Memorandum of Activity, Interview of [redacted] dated March 22, 2012.
3. Memorandum of Activity, Document Review, dated April 11, 2012.
4. Memorandum of Activity, Interview of [redacted] dated June 5, 2012.
5. Memorandum of Activity, Interview of [redacted] dated June 5, 2012.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 15, 2012

MEMORANDUM TO FILE

FROM: [redacted] 10/15/12

SUBJECT: MSB Initiative Project Case Closure

OIG Project Number: MSB-12-0090-I

In October 2010, TOIG embarked on an initiative surrounding fraud related to unlicensed/unregistered Money Service Businesses (MSB). The current rules amended in 1999 by the Financial Crimes Enforcement Network (FinCEN) revised the regulatory definitions of certain non-bank financial institutions for purposes of the Bank Secrecy Act (BSA) and grouped the definitions into a separate category of financial institution called MSBs. A business that meets one or more of the definitions of a type of MSB is an MSB and must comply with BSA requirements applicable to it as an MSB, as a financial institution and as a specific type of MSB.

As such, OI develops and receives information from various Federal and state regulatory and law enforcement agencies related to unlicensed/unregistered MSBs or licensed/registered MSBs conducting unlawful activities.

In October 2011, TOIG opened an investigative case number for Fiscal Year (FY) 2012 to allow agents to utilize for case development and to document agent activities in relation to the initiative. TOIG has received approximately 600 leads concerning the above mentioned MSB types. Leads conducted to date have yielded no criminal results, but several potential inquiries are being reviewed.

Therefore, with the ending of FY 2012, it is recommended that with the approval of this memorandum, this project be administratively closed.

REPORT OF INVESTIGATION
OCC-11-1048-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted] Office of the Comptroller of the Currency, Washington, D.C.

Case Type: Criminal ___ Administrative _X_ Civil ___

Conducted by: [redacted] Special Agent

Investigation Initiated: May 26, 2011

AUG 31 2011

Investigation Completed:

[redacted] Special Agent

Origin: [redacted] Office of the Comptroller of the Currency

Approved by: [redacted] Special Agent in Charge

Case #: OCC-11-1048-I

Summary

The Department of Treasury, Office of the Inspector General, Office of Investigations (TOIG), received a complaint from the Office of the Comptroller of the Currency (OCC) that [redacted] OCC National Bank Examiner, submitted two non-sufficient fund (NSF) payments related to his Government Citibank travel card. Specifically, OCC's travel program office reported that [redacted] Government Citibank travel card account ([redacted]) was closed by Citibank because [redacted] submitted two NSF payments within a 12-month period that were rejected by Citibank. (Exhibit 1)

The investigation determined that the allegation is substantiated. It was discovered that [redacted] telephonically submitted two NSF payments to Citibank in December 2010 and April 2011 in an attempt to pay his Government Citibank travel card account. Due to the two NSF payments [redacted] Government Citibank travel card account was closed by Citibank on May 11, 2011.

Basis and Scope of the Investigation

The Government Travel Charge Card Program (GTCC) provides travelers with a safe, effective, convenient, and commercially available method to pay for expenses associated with official travel. The GTCC includes Individually Billed Accounts (IBAs) and Centrally Billed Accounts (CBAs). Use of the travel card is mandated by the Travel and Transportation Reform Act of 1998.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Contractor with Travel Operations, OCC-Financial Management
- [redacted] Bank Examiner, OCC

In addition, TOIG reviewed pertinent documents, including:

- [redacted] Citibank Credit Card Statements 7/2010-6/2011
- [redacted] Citibank Balance as of 6/2011
- Correspondence (emails) between [redacted] and OCC's travel office regarding the reinstatement of [redacted] travel card
- Correspondence (emails) between OCC's travel office and [redacted] supervisor
- Citibank Card Holder Account Agreement

Investigative Activity

A TOIG document review of [redacted] Government Citibank travel card statements dated December 4, 2010 to January 3, 2011, revealed that [redacted] attempted to pay the $1,677.05 due on his Government Citibank travel card; however, the payment was returned due to NSF. [redacted] Government Citibank travel card statement dated April 4, 2011 to May 3, 2011, revealed that [redacted] attempted to pay the $1,261.40 due on his Government Citibank travel card; however, that payment was also returned due to NSF. (Exhibits 2 & 3)

In an interview with TOIG, [redacted] Contractor with Travel Operations, OCC Financial Management (FM) stated that FM conducts a monthly monitoring review of OCC's Citibank Travel Charge Card Program. [redacted] said the monthly review specifically provides information related to employee's payment history and payments that were returned due to NSF. [redacted] stated that [redacted] and his supervisor, [redacted], were notified that [redacted] December 2010 payment was returned due to NSF and if it happened again, [redacted] Government Citibank travel card account would be closed.

[redacted] further stated that [redacted] Government Citibank travel card statement dated April 4, 2011 to May 3, 2011, revealed that [redacted] attempted to pay the $1,261.40 due on his Government Citibank travel card; however, that payment was returned due to NSF and [redacted] Government Citibank travel card was cancelled on May 11, 2011. (Exhibit 4)

In an interview with TOIG, [redacted] stated that his Government Citibank travel card balance was due on the 28th of every month and if not paid the account becomes delinquent. [redacted] stated that he failed to pay the balances due from the December 2010 to January 2011 statement and the April 2011 to May

2011 statement because he was late processing his expense vouchers. [redacted] said that he submitted the expense vouchers on/or about the 28th of December 2010 and April 2011; however, it took approximately four to six-days for his supervisor to approve the vouchers, then the funds had to be forwarded to Citibank for payment.

[redacted] further said that he knew that there were possibilities that the OCC voucher payments would not make the 28th deadline date; therefore, he telephonically submitted payments to avoid the late payments in which the payments were returned due to NSF in his personal checking account. The OCC voucher payments were posted to [redacted] Citibank travel card account on January 3, 2011 and May 3, 2011. Although OCC's voucher payments were posted within the 6 day grace period, [redacted] still submitted the NSF payments, which caused his account to be closed. (Exhibit 5)

Referrals

TOIG presented this investigation to [redacted], Assistant United States Attorney (AUSA) for the Southern District of Ohio for criminal prosecution. AUSA [redacted] declined the investigation for criminal prosecution. (Exhibit 6)

Judicial Action

NA

Findings

The investigation determined that the allegation is substantiated. It was discovered that [redacted] telephonically submitted two NSF payments to Citibank in December 2010 and April 2011 in an attempt to pay his Government Citibank travel card account. Due to the two NSF payments [redacted] Government Citibank travel card account was closed by Citibank on May 11, 2011.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policies were violated or could be applied to the case:

- 5 C.F.R., 2635.101(b) (12)– Basic Obligation of Public Service-Employees shall satisfy in good faith their obligations as citizens, including all just financial obligations, especially those—such as Federal, State, or local taxes—that are imposed by law.

- Government Services Travel Card Program Cardholder Account Agreement-(10)(b)(iv) Suspension and Cancellation-Account has been paid with checks returned by the financial institution for insufficient funds ("NSF") two or more times in a 12-month period. In this event, the Account is subject to immediate cancellation.

Distribution

[redacted], Senior Advisor, OCC

Signatures

[redacted]

8/31/2011
Date

Supervisor: [redacted]

8-31-11
Date

Exhibits

1. Letter from [redacted], Senior Advisor, OCC, to TOIG, dated May 20, 2011.
2. Memorandum of Activity, Document Review of [redacted] Citibank Travel Card Statements, dated May 31, 2011.
3. Memorandum of Activity, Document Review of [redacted] Citibank balance, dated June 16, 2011.
4. Memorandum of Activity, Interview of [redacted] dated July 27, 2011.
5. Memorandum of Activity, Interview of [redacted] dated June 29, 2011.
6. Memorandum of Activity, Criminal Declination, dated July 25, 2011.

REPORT OF INVESTIGATION
OCC-12-0325-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted] – Alleged Credit Card Misuse

Case #: OCC-12-0325-I

Case Type: Criminal ___
Administrative _X__
Civil ____

Investigation Initiated: November 17, 2011

Investigation Completed: FEB 23 2012

Conducted by: [redacted]
Special Agent

Approved by: [redacted]
Special Agent in Charge

Origin: Office of the Comptroller of the Currency

Summary

On November, 17, 2011, the US Department of Treasury (Treasury), Office of Inspector General (TOIG), received a complaint from the Office of the Comptroller of the Currency (OCC) regarding [redacted] National Bank Examiner, OCC, misusing her government travel card by taking cash advances while not in travel status, taking excessive cash advances, and taking cash advances and charging expenses during the same travel period.

The investigation determined that the allegation is substantiated. [redacted] admitted to consistently withdrawing more than $400 per week in cash advances while not in travel status. She could not fully explain why she needed the case advances, but stated that she did not pay personal bills with the funds. [redacted] resigned from her position at OCC effective January 25, 2012. She has paid off her government credit card balance and returned the card to OCC.

Basis and Scope of the Investigation

TOIG received a complaint from OCC that [redacted] National Bank Examiner, is misusing her government travel card by taking cash advances while not in travel status, taking excessive cash advances, and taking cash advances and charging expenses during the same travel period. The OCC is a Treasury agency that supervises and regulates national banks. (Exhibit 1)

The OCC Federal Travel Regulations Supplement dated April 2011, states: "You are authorized to utilize the ATM feature of your government travel charge card within two business days of travel to obtain cash advances for expected business expenses that cannot be charged during official travel. The amount of your cash advance should closely approximate the amount of travel reimbursement you estimate you will be entitled to claim. Generally, the amount should not exceed the total estimate estimated for M&IE (e.g. tips, telephone, local transportation, etc.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] National Bank Examiner, OCC
- [redacted], Human Resources Consultant, OCC
- [redacted] Assistant Deputy Comptroller, OCC
- [redacted] National Bank Examiner Team Leader, OCC
- [redacted], National Bank Examiner Team Leader, OCC

During the course of the investigation, TOIG reviewed pertinent documents, including:

- [redacted] government credit card record

Investigative Activity

In an interview with TOIG, [redacted], Human Resources Consultant, OCC, stated that her office conducts audits on employee credit cards that are delinquent over 60 days, has multiple ATM transactions, or are alerted about suspicious activity on the card. [redacted] conducted an audit on [redacted] credit card because it was more than 60 days delinquent. She found during the audit, that [redacted] had several Automatic Teller Machine (ATM) transactions in the amount of $440, had a balance of $3,000 over the past year (2011), took cash advances while not on a travel status, and made unauthorized purchases. [redacted] recalled a $60 purchase to a popcorn company. [redacted] notified [redacted] supervisors, [redacted] National Bank Examiner Team Leader, OCC, and [redacted] Assistant Deputy Comptroller, OCC, who spoke with [redacted] informed [redacted] and [redacted] that she believed she could obtain cash advances in the amount of $440 and that she would pay the balance of the credit card immediately. (Exhibit 2)

TOIG conducted a document review of [redacted] credit card transactions, to include ATM withdrawals. The record contained a list of ATM transactions from April 2009 through August 2011. During this time period, [redacted] had 175 ATM withdrawals. The amounts varied from $23 to $443. As of September 2011, [redacted] held a $3,302.36 balance and was $1,993.97 past due on this account.

The record contained cardholder statements from [redacted] government issued credit card from September 2010 to October 2011. The statements reflected the aforementioned ATM withdrawals as well as many hotels, restaurants, and gas stations. The statements did not reflect any questionable purchases with the exception of a $60.72 purchase at the "Popcorn Haven" on December 9, 2010. (Exhibit 3)

In an interview with TOIG, [redacted] stated he is the second line supervisor of [redacted] He stated that he and [redacted] were notified by [redacted] of suspicious activity on [redacted] credit card on approximately November 3, 2011. Specifically, they were informed that [redacted] made multiple cash advances over the OCC limit of $400 per week, made charges while not on travel, and that her card was past due. He and [redacted] spoke with [redacted] and she stated that she believed she was allowed to take the $440 cash advances. She then claimed ignorance to the rules of the use of government credit cards. [redacted] stated that he does not believe she is unaware of the rules regarding the use of the government credit card because his predecessor, [redacted] (now retired) counseled her previously regarding the same matter. (Exhibit 4)

In an interview with TOIG, [redacted] stated he has been the direct supervisor of [redacted] since August 2011, but has supervised her on examinations from 2009 to the present. [redacted] stated that in 2008, he noticed some ATM cash withdrawals when reviewing her account after an audit. He and [redacted] Assistant Deputy Comptroller, OCC, spoke with her about using cash advances when necessary. [redacted] also spoke to her about using her credit card only for travel, and paying her credit card off in a timely manner, because other pre-commissioned bank examiners had similar issues, and some were terminated. In November 2011, [redacted] was notified by [redacted] of suspicious activity on [redacted] travel credit card. Specifically, he was informed that [redacted] made multiple cash advances over the OCC limit of $400 per week, made charges while not on travel, and that her card was past due. [redacted] reviewed several documents to include [redacted] credit card ATM withdrawals and credit card statements. The records showed numerous ATM withdrawals with some totaling more than $400 per week. The credit card statements did not reflect any suspicious purchases except for a $60 purchase at a popcorn store. The records did show that she had an approximate $3000 balance and was past due approximately $1,900.

[redacted] and [redacted] spoke to [redacted] in November 2011. [redacted] stated that she believed she was allowed to take the cash advances because she had contacted Citicard and was informed of the maximum weekly limit of $450. [redacted] stated that he contacted Citicard later and was also informed of the $450 weekly limit. However, [redacted] believed that OCC policy follows a $400 maximum weekly amount. [redacted] stated that [redacted] wrote a statement to him and [redacted] following their conversation, but [redacted] believed there were some incorrect statements in her statement. She stated that during her 2008 meeting with [redacted] and [redacted] they only discussed cash advances. However, [redacted] stated that using the travel card only while on travel and repaying the card in a timely manner were also discussed. [redacted] did not believe she has ever been disciplined in writing or suspended, but stated that her former supervisor, [redacted], NBE Team Leader, OCC, would need to know more details. (Exhibit 5)

In an interview with TOIG, [redacted], stated he was the direct supervisor of [redacted] from 2009 until August 2011. In November 2011, [redacted] was notified by [redacted] of suspicious activity on

[redacted] travel credit card. Specifically, he was informed that [redacted] made multiple cash advances over the OCC limit of $400 per week. [redacted] stated that [redacted] spoke with [redacted] regarding these matters, and believed resolved the issue. [redacted] stated that he never noticed any issues with [redacted] travel vouchers while she was under his supervision. However, he only saw some of her vouchers and never reviewed any documents such as ATM withdrawals. (Exhibit 6)

In an interview with TOIG, [redacted] stated that she has a government credit card used for travel, and that she travels almost weekly to oversee banks in the southeastern United States. She believes she received a General Services Administration regulation booklet on credit card use when she received her card in 2008. She also believes she has had yearly computer training on proper credit card usage, but that is simply a powerpoint that she "did not pay much attention to."

In approximately 2008, [redacted] spoke to her about credit card use and invoices and [redacted] was present. [redacted] stated that the conversation was only a few minutes and did not seem very serious in nature. [redacted] spoke about credit card advances and that they could only be used when on travel. He also spoke about splitting costs to the government credit card and to the traveler for items like per diem. [redacted] discontinued obtaining cash advances for approximately six months after this meeting. She could not explain why she stopped cash advances except that she did not want to be spoken to again about the cash advances.

[redacted] began using cash advances again because she wanted cash for her trips. She called Citibank to ascertain how much in cash advances she could take. She was informed that she could take $440 weekly so that is what she withdrew. [redacted] could not explain why she needed $440 weekly except that she and the other bank examiners liked to eat out and that "a girl likes to have cash in her pocket." She stated that she did not use the cash to pay personal bills and paid the credit card bill off monthly.

[redacted] stated she forgot to complete one travel voucher for $1,479 in June 2011, that put her behind on her bills. She then had a balance on the government credit card for approximately three months. During that time, she paid the minimum balance. In November 2011, [redacted] spoke to her again about her credit card usage and informed her that she did not submit the aforementioned voucher. [redacted] immediately submitted the voucher, received the funds, and paid off the credit card bill. [redacted] also stated that she misused the card by purchasing gasoline locally and purchasing popcorn at a store. She stated that she thought she could use the card to purchase gasoline if she was over 50 miles from her duty station. On the occasions, she purchased gasoline, she was at an examination 50 miles from her residence and duty station. She admitted to purchasing the popcorn, but stated that she ate it for lunch. [redacted] asked her to write a statement regarding her credit card use, and misunderstandings, which she did, and provided it to him.

[redacted] stated that OCC is causing her too much stress and travel, and she has found a position with a private accounting firm. [redacted] resigned from OCC effective January 25, 2012. (Exhibit 7)

On January 26, 2012, [redacted] confirmed that [redacted] resigned and returned her OCC laptop, badge, keys, government travel card and other miscellaneous items to OCC on January 25, 2012. He also confirmed that she has a $0 balance on her government travel credit card. (Exhibit 8)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegation is substantiated. [redacted] admitted to consistently withdrawing more than $400 per week in cash advances while not in travel status. She could not fully explain why she needed the case advances, but stated that she did not pay personal bills with the funds. [redacted] resigned from her position at the OCC effective January 25, 2012. She has paid off her government credit card balance and returned the card to the OCC.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policies were violated or could be applied to the case:

- 5 C.F.R. 2635.101 - Basic obligation of public service
- OCC Federal Travel Regulations Supplement dated April 2011

Distribution

[redacted], Senior Advisor, Office of the Comptroller of the Currency

Signatures

Case Agent:

[redacted]

2/10/12
Date

Supervisor:

[redacted]

2-16-12
Date

Exhibits

1. Letter from OCC, dated November 17, 2011.
2. Memorandum of Activity, Interview of [redacted], Human Resources Consultant, OCC, dated December 5, 2011.
3. Memorandum of Activity, Record Review dated December, 9, 2011.
4. Memorandum of Activity, Interview of [redacted] Assistant Deputy Comptroller, OCC, dated December 5, 2011.
5. Memorandum of Activity, Interview of [redacted], NBE Team Leader, OCC, dated December 14, 2011.
6. Memorandum of Activity, Interview of [redacted], NBE Team Leader, OCC, dated December 14, 2011.
7. Memorandum of Activity, Interview of [redacted], Associate NBE, OCC, dated January 26, 2012.
8. Memorandum of Activity, Interview of [redacted], NBE Team Leader, dated January 27, 2012.

REPORT OF INVESTIGATION
OCC-12-0860-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Office of the Comptroller of the Currency
Washington, DC

Case #: OCC-12-0860-I

Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: February 22, 2012

Investigation Completed: MAY 21 2012

Conducted by: [redacted]
Special Agent

Origin: Anonymous

Approved by: [redacted]
Special Agent in Charge

Summary

On February 15, 2012, the Department of the Treasury, Office of Inspector General Office of Investigations (TOIG) received an allegation from an anonymous complainant alleging that [redacted], was involved with a potential ethics violation. Specifically, [redacted] wife is an employee of Bank of America (BoA); therefore, [redacted] was prohibited from working on BoA related matters. However, [redacted] was promoted to [redacted] a position that has industry-wide policy making authority. (Exhibit 1)

The investigation determined that the allegation is unsubstantiated. TOIG determined that while [redacted] was [redacted] he did not work on any policy matters specific to BoA and observed a recusal approved by OCC's Office of Counsel, hence taking the appropriate steps necessary to avoid violating the law.

Basis and Scope of the Investigation

TOIG received information from an anonymous complainant alleging that [redacted] was involved with a potential ethics violation. [redacted] wife is an employee of BoA; therefore, [redacted] was prohibited from working on BoA related matters. However, [redacted] was promoted to the position of [redacted] a position that has industry-wide policy making authority. Furthermore, the complainant alleged that the OCC failed to follow government ethics rules and notify TOIG of the potential ethics violation.

The applicable ethics violation is 18 U.S.C 208(a)-Acts Affecting a Personal Financial Interest, which states "except as permitted by subsection (b) hereof, whoever, being an officer or employee of the executive branch of the United States Government, or of any independent agency of the United States, a Federal Reserve bank director, officer, or employee, or an officer or employee of the District of Columbia, including a special Government employee, participates personally and substantially as a Government officer or employee, through decision, approval, disapproval, recommendation, the rendering of advice, investigation.....or other particular matter in which, to his knowledge, he, his spouse, minor child, general partner, organization in which he is serving as officer, director, trustee, general partner or employee, or any person or organization with whom he is negotiating or has any arrangement concerning prospective employment, has a financial interest shall be subject to the penalties set forth in section 216 of this title."

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Ethics Counsel, OCC
- [redacted] Examiner-In-Charge, OCC
- [redacted] (Acting) Comptroller of the Currency, OCC

In addition, TOIG reviewed pertinent documents, including:

- Waiver for [redacted] issued by [redacted], former Comptroller of the Currency, OCC
- Email correspondence
- OCC's Draft Waiver Request for [redacted] addressed to [redacted]
- [redacted] OCC Confidential Financial Disclosure Report for Filing Year 2004-2010

Investigative Activity

In an interview with TOIG, [redacted] stated OCC has a Securities Prohibition that states all employees may not have stock in banks; however, OCC has the authority to grant waivers. In addition to following OCC's policy, OCC is required to consult with the Office of Government Ethics (OGE), which states employees can have up to $25,000 in bank interest and obtain an exemption. Although OCC usually implements the most restrictive policy, [redacted] stated there are instances that the most restrictive policy is not implemented. These instances may include a new employee with stock in a state chartered bank, inherited stocks, or stock of a spouse.

Prior to becoming [redacted] disclosed his wife's stock interest in BoA, which is over $200,000 via OCC Confidential Financial Disclosure Report. [redacted] stated that [redacted] had an OCC waiver and did not think he needed one from OGE. However, [redacted] spoke with her supervisor [redacted] and [redacted] Chief Counsel, OCC, regarding [redacted] recusal and waiver. [redacted] suggested that [redacted] request a waiver from OGE. In September 2011, [redacted] sent a waiver request to OGE, which was verbally denied. In October 2011, [redacted] was reassigned to Examiner-in-Charge of Citibank. (Exhibit 2)

In an interview with TOIG, [redacted] stated that since 2004 he has disclosed his wife's employment with BoA, including all financial interests that are part of her compensation package, in his OCC Confidential Financial Disclosure Report. [redacted] has always observed a company-wide recusal from BoA matters. The scope of [redacted] recusal was determined by OCC Ethics officials.

After [redacted] was promoted to [redacted] in July 2011, he spoke with [redacted] regarding the scope of his recusal in relation to his new position. It was determined that the general policy matters that [redacted] was working on, although not specific to BoA, may fall within the scope of [redacted] recusal. As a result, [redacted] recused himself from those matters. In October 2011, [redacted] approached [redacted] after a meeting and stated that their interpretation of his recusal may be incorrect. In October 2011, [redacted] stated that a collaborative decision was made by [redacted], Senior Deputy Comptroller for Large Bank Supervision, OCC; [redacted] Senior Deputy Comptroller for Midsize/Community Bank Supervision, OCC; [redacted], Senior Deputy Comptroller Bank Supervision Policy and [redacted] OCC; and [redacted] to remove [redacted] from [redacted] and reassign him to Citibank Examiner in Charge.

As [redacted] was involved with rulemaking and other activities related to the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Dodd-Frank Act created the Financial Stability Oversight Council (FSOC) comprised of numerous governmental agencies. [redacted] supported the Acting Comptroller on FSOC and was the OCC representative on FSOC Deputies subcommittee. [redacted] also represented the OCC before Congress on matters related to supervision and certain Dodd-Frank matters and served on certain interagency groups as the OCC representative. [redacted] stated that policies and communications that went under his signature were largely conceived and developed before he was the [redacted] In addition, most of the policies and communications were jointly issued by OCC, the Federal Reserve, and the Federal Deposit Insurance Corporation. Other communications that went out under [redacted] name were procedural and not policy related. Other policies were in development while [redacted] was [redacted] but were not finalized. (Exhibit 3)

In an interview with TOIG, [redacted] stated that he was aware that [redacted] wife had a senior level position and financial interest in BoA at the time [redacted] was promoted to [redacted] however, decided that [redacted] would observe the prevailing guidance of a BoA recusal he already had with OCC. [redacted] stated that if BoA matters were discussed during meetings [redacted] would recuse himself and leave. OCC decided that [redacted] could work on broad policy matters that may include BoA. To avoid violating any ethics laws, particularly 18 U.S.C 208(a), [redacted] sought a waiver from the OGE on [redacted] behalf. OGE subsequently denied the waiver. [redacted] stated that OGE had a much broader interpretation of the conflict of interest law. [redacted] stated that OCC then removed [redacted] from the position. [redacted] informed TOIG that he was not aware of any policy that [redacted] worked on during his tenure as [redacted] that may have been specific to BoA. (Exhibit 4)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegation is unsubstantiated. TOIG determined that while [redacted] was [redacted] he did not work on any policy specific to BoA and observed a recusal approved by OCC's Office of Counsel, hence taking the appropriate steps necessary to avoid violating the law

Based on the findings of our investigation, it appears that the following statues or regulations and/or policies were violated:

- N/A

Distribution

[redacted], Senior Advisor, OCC

Signatures

Case Agent:

[redacted]

5/14/12
Date

Supervisor:

[redacted]

5-15-12
Date

Exhibits

1. Complaint Referral from Anonymous Complainant, dated February 15, 2012.

2. Memorandum of Activity, Interview of [redacted] dated February 29, 2012.

3. Memorandum of Activity, Interview of [redacted] dated March 15, 2012.

4. Memorandum of Activity, Interview of [redacted] dated March 20, 2012.

REPORT OF INVESTIGATION
OCC-12-1383-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted] Misuse of Credentials
(Treasury Employee)

Case #: OCC-12-1383-I

Case Type: Criminal ___
Administrative x
Civil ___

Investigation Initiated: April 23, 2012

Investigation Completed:

Conducted by: [redacted]
Special Agent

Origin: Office of the Comptroller of the Currency (OCC)

Approved by: [redacted]
Special Agent In Charge

Summary

On April 3, 2012, the Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), was contacted via OIG Intake by [redacted] OCC, regarding the following complaint reported to her by a third party that [redacted] inappropriately displayed his OCC badge in a private family estate legal matter. (Exhibit 1)

The allegation stems from [redacted] visit to the property of [redacted] uncle, [redacted] to inventory property related to the estate of [redacted] Grandmother, [redacted] is a beneficiary of his Grandmother's estate. [redacted] is a [redacted] serving as [redacted] in the OCC's [redacted] field office.

Based on conflicting statements of the complainant and witness, and interview of the subject, TOIG could not substantiate the allegation that [redacted] misused his OCC issued badge or credentials to intimidate, harass or influence.

Our investigation determined the allegations could not be substantiated.

Basis and Scope of the Investigation

On April 3, 2012, TOIG hotline received a complaint by [redacted], Attorney representing [redacted] reporting that [redacted] inappropriately displayed his OCC badge in a private family estate legal matter. [redacted] is a [redacted] serving as [redacted] in the OCC's [redacted] field office.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Complainant
- [redacted] OCC
- [redacted] Witness

In addition, TOIG reviewed pertinent documents, including:

- Written complaint from [redacted], Attorney representing [redacted]

Investigative Activity

On June 4, 2012, TOIG interviewed [redacted] in reference to a complaint received indicating [redacted] OCC, misused his OCC badge and credentials.

[redacted] said that [redacted] is representing his ([redacted] mother's estate. [redacted] is a beneficiary of his [redacted] grandmother, [redacted] estate. [redacted] father and mother are also beneficiaries of [redacted] estate.

[redacted] said that [redacted] has been contesting the estate for seven years saying that his mother's estate has never been allowed to see what was in the barn on [redacted] property. [redacted] property is directly adjacent to [redacted] home and property. [redacted] was given access by the court to view the property owned by Leona [redacted] estate, more specifically the barn. In May 2012, [redacted] had an appointment to look inside the barn. [redacted] said that [redacted] showed up early for the appointment and when [redacted] went out to meet him, [redacted] pulled out his badge. [redacted] stated that neither he nor [redacted] said anything at that point. A couple minutes later, when [redacted] asked to see the barn, [redacted] said that he thought [redacted] was wasting his time because everything in the barn was his dad's. Again, [redacted] pulled out his badge. [redacted] said that nothing was said at that time. [redacted] advised he didn't know what [redacted] was doing at that point, but it didn't seem like he had any other reason to pull out the badge except for making a point for [redacted] to see it.

[redacted] said that [redacted] began taking pictures of the property and then left. [redacted] said that a few minutes later [redacted] came back and started taking pictures of [redacted] property. Upon seeing this, [redacted] and his mother went out to see what [redacted] was doing. They

informed him that that property was not part of the estate. [redacted] responded that he had the right to take the pictures. [redacted] advised he told [redacted] that he was going to call the State Police, to which [redacted] responded, "Ha, State, I'm Federal" and pulled out his badge and said, "call whoever you want, I'm taking pictures and recording". [redacted] said that his mother then asked [redacted] who he worked for and [redacted] said "Treasury". [redacted] said that [redacted] never said that he was on official business.

[redacted] said that if [redacted] was trying to intimidate them, it worked. [redacted] told his mother right after [redacted] left that they... "for sure were going to be audited now." (Exhibit 2)

On August 1, 2012, TOIG interviewed [redacted], OCC, [redacted] relating to an allegation that [redacted] misused his OCC issued credentials.

[redacted] said that he is a beneficiary of the estate of his Grandmother, [redacted] as is his uncle, [redacted] [redacted] said that there has been growing "anger" between the beneficiaries because a lack of movement to liquidate the estate by [redacted] [redacted] owns the property directly adjacent to his Grandmother's property. [redacted] said that as part of the estate liquidation, he was allowed, by court order in March 2012, to have access to his Grandmother's property to do an accounting of all the property regarding the estate.

After receiving permission by the court to view the property, [redacted] said he made arrangements with [redacted] to visit the property. In May 2012, [redacted] said he went to the property to account for all the estate property. [redacted] said that he arrived at the farm and parked in front of the barn. [redacted] said that [redacted] cousin, came out of his house and told [redacted] that he couldn't take pictures. [redacted] said that at that point he conference called his wife and his attorney. [redacted] advised after the call [redacted] finally agreed to let him take pictures. [redacted] said that he entered the barn to begin taking pictures but the camera he had would not take good pictures in the dark. [redacted] went back to his car to get his other camera. [redacted] said that because his camera was in his backpack, he dumped his backpack contents onto his front car seat to find the camera. While dumping everything out, [redacted] said that his OCC credentials fell onto the ground. [redacted] said that [redacted] picked his credentials off the ground and asked, "Do you still work for the Fed?" and handed his credentials back to [redacted] [redacted] responded that he did.

[redacted] went back into the barn to continue his accounting. [redacted] said that all of his Grandmother's equipment was gone. [redacted] said that he then went back to his car to leave. As [redacted] was driving away he noticed that a couple of his Grandmother's tractors were in [redacted] driveway. [redacted] said that he got out of his car, not on his uncle's property, and began taking pictures of the tractors. [redacted] said that [redacted] and his wife, [redacted] (Agent Note: [redacted] reported that [redacted] was [redacted] wife, but [redacted] is actually [redacted] mother), came out of their home and started cursing at [redacted] and telling him that he can't take pictures. [redacted] said they were verbally abusive and [redacted] said she would call the Sheriff's Department, then the

State Police. [redacted] said that he responded, "I don't care who you call". [redacted] explained that he actually would have liked them to call the authorities because he believed it would have defused their anger.

[redacted] said that he has no idea why [redacted] would have said that [redacted] credentials were shown numerous times and that he never said, "I don't care who you call, call the locals, I'm a Fed." [redacted] said that he did not intend to intimidate, harass or influence [redacted] based on his Federal Government position. [redacted] denied ever showing his credentials. [redacted] said that he has been very careful the entire time to not send an email to [redacted] Attorney, [redacted], from his work email because of the perception. [redacted] said that he just wants the estate matter, "to get to a resolution".

[redacted] provided a sworn written statement addressing the above. (Exhibit 3)

On September 12, 2012, TOIG reinterviewed [redacted] was asked if he could describe the badge that he alleges was shown to him by [redacted] said that "it was gold". When asked if he could describe it a little more, [redacted] said he could not see it very well, he only saw that it was gold and could not tell if there was any other identification attached to the badge. [redacted] said that [redacted] seemed to flip open his wallet and he saw the badge. [redacted] said that the other side of the wallet was not black but didn't see anything there. (Exhibit 4)

On September 12, 2012, TOIG interviewed [redacted] who was present when [redacted] allegedly showed his badge. [redacted] was asked to recount the timeline of what happened the day of [redacted] showing his credentials/badge. [redacted] said that her memory was not very good and she has a hard time remembering back that far. [redacted] said that [redacted] Nephew, was taking pictures of [redacted] property, which is next door to her property, to account for property that is included in the [redacted] Estate, in which [redacted] is a beneficiary. [redacted] said that she does not know what happened while [redacted] and her son, [redacted] were next door at the property. [redacted] said that after [redacted] accounted for the property next door, he stopped by her mailbox and was taking pictures of her property. [redacted] said that both she and [redacted] went outside and told [redacted] that he had no business taking pictures of her property. [redacted] said that she was going to call the police. [redacted] said that [redacted] pulled out his wallet and said "I'm federal", in which she responded you're a "federal asshole". [redacted] said that [redacted] flipped open his wallet and showed his credentials. [redacted] said she doesn't remember seeing a badge. [redacted] said that she was approximately 15 feet away from [redacted] at the time. [redacted] said that [redacted] never said he was there on official business and never threatened them. [redacted] was asked if there was any estate property on her property at the time [redacted] was taking pictures and [redacted] said that [redacted] was questioning the tractors that were in her driveway.

[redacted] said that she never called the police and [redacted] got in the car and left without further incident. She said she has only seen him in court since that incident and he does not speak to them. [redacted] supplied a sworn written statement. (Exhibit 5)

Referrals

None

Judicial Action

None

Findings

TOIG's investigation of the misuse of OCC badge and credentials in violation of 31 CFR 0.213 - General conduct prejudicial to the Government and 5 CFR 2635.704 – Use of Government Property led to differing accounts by witnesses and uncorroborated statements, therefore TOIG finds the allegations unsubstantiated.

Distribution

[redacted], Senior Advisor, Office of the Comptroller of the Currency.

Signatures

Case Agent:

[redacted]

10/1/12
Date

Supervisor:

[redacted]

10/4/12
Date

Exhibits

1. Complaint document, Letter from Attorney [redacted], dated March 30, 2012.
2. Memorandum of Activity, Interview of [redacted] dated June 4, 2012.
3. Memorandum of Activity, Interview of [redacted] dated August 1, 2012.
4. Memorandum of Activity, Interview of [redacted] dated September 12, 2012.
5. Memorandum of Activity, Interview of [redacted] dated September 12, 2012.

REPORT OF INVESTIGATION
TTB-12-1678-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted] U.S. Custom and Border Protection (Non-Employee)

Case #: TTB-12-1678-I

Case Type: Criminal _ X__
Administrative ___
Civil ____

Investigation Initiated: May 7, 2012

Conducted by: [redacted], Special Agent

Investigation Completed:

Approved by: [redacted], Special Agent in Charge

Origin: [redacted], Alcohol and Tobacco Tax and Trade Bureau

Summary

On May 7, 2012, the U.S. Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG) initiated an investigation based on an allegation received from [redacted] Director of the Intelligence Division, Alcohol and Tobacco Tax and Trade Bureau (TTB), regarding a possible improper collusion between [redacted] and importer, [redacted] During a joint inspection conducted by TTB and U.S. Custom and Border Protection (CBP), it was discovered that [redacted] did not obtain export documentation from [redacted] required by CBP.

The investigation determined that the allegation was unsubstantiated. [redacted] stated that she did not assist [redacted] with processing fraudulent documentation. In addition, [redacted] denied providing [redacted] ship stamps; visiting the warehouse; having a relationship with anyone affiliated with [redacted] or knowingly or intentionally assisting [redacted] in obtaining alcohol and tobacco products tax free.

[**Agent's Note:** In the initial allegation [redacted] was referred to as [redacted] CBP eventually provided TOIG with [redacted] correct name.]

Basis and Scope of the Investigation

On May 7, 2012, TOIG initiated an investigation based on allegations received from [redacted] regarding a possible improper collusion between [redacted] and [redacted] During a joint inspection conducted by TTB and CBP, it was discovered that [redacted] did not obtain export documentation from [redacted] required by CBP. Currently, TTB, CBP, and the Homeland Security Investigators are criminally investigating [redacted] (Exhibit 1)

In a ROI prepared by [redacted], CBP, [redacted], Intelligence Research Specialist, TTB, stated that she believed [redacted] improperly allowed [redacted] to obtain alcohol and tobacco products free of tax. [redacted] reportedly stated that she allowed [redacted] not to file documentation for each withdrawal contrary to the Code of Federal Regulation (CFR), which resulted in an estimated potential loss of $1 million in Federal Excise Taxes during calendar year 2009 through 2012. (Exhibit 3)

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Investigator, TTB

TOIG reviewed pertinent documents, including:

- Report of Investigation prepared by [redacted]
- Report of Investigation prepared by [redacted] Special Agent, ICE-OPR
- [redacted] Supervisory Custom Entry Officer, CBP, signed sworn affidavit to [redacted] Special Agent, CBP-Internal Affairs
- [redacted] signed sworn affidavit to [redacted]

Investigative Activity

In an interview with TOIG, [redacted] stated that [redacted] never collected CBP Export Form 7512 as proof of export from [redacted] In March 2012, [redacted], Special Operations Investigator, TTB, and a CBP employee who [redacted] does not recall, conducted a conference call with [redacted] During the conversation, the CBP employee asked [redacted] why was [redacted] not required to submit CBP Export Form 7512. [redacted] responded that [redacted] was the exception. [redacted] stated that the CBP employee immediately terminated the conversation after [redacted] response. According to [redacted] it is CBP's standard operating procedure for [redacted] to be assigned a CBP Export Specialist. Although [redacted] had been exporting for over 25 years, CBP never collected Export Form 7512. (Exhibit 2)

A TOIG review of the ICE-OPR ROI revealed that [redacted] was advised by a CBP Entry Specialist that [redacted] is Korean and the owners of the [redacted] are also Korean. [redacted]

acknowledged there was no logbook showing [redacted] at [redacted] warehouse at any time prior to the Fraud Investigative Strike Team (FIST) (composed of CBP, TTB, and Homeland Security Investigators) inspection. [redacted] provided no further evidence of collusion between [redacted] and [redacted] ICE OPR referred the investigation to CBP/Internal Affairs for administrative action. (Exhibit 4)

A TOIG review of [redacted] affidavit to [redacted] confirmed that [redacted] has been an [redacted] since mid-2008 and works in the [redacted] of the [redacted]. [redacted] stated multiple ship stamps, which are commonly found on TTB and CBP paperwork to signify that the ship received the bonded goods, were found at [redacted] warehouse. [redacted] recalled there was a discussion that the Warehouse Section was accepting improper documentation, such as a 7501 for clearance of merchandise rather than the more commonly utilized document of a 7512. In [redacted] case, the merchandise was said to be sent to vessels and the 7501 process was applicable. According to [redacted] [redacted] followed proper protocol and procedures by following 19 CFR 19.6-Deposits, withdrawals, blanket permits to withdraw and sealing requirements: 19 CFR 19.6(5)-Blank Permit Summary. 19 CFR 19.6 (5) states:

> "when all of the merchandise covered by an entry on which a blanket permit to withdraw was issued has been withdrawn, including withdrawals made for purposes other than duty-free delivery, vessel, or aircraft supply, or diplomatic use, the proprietor must prepare a report on a copy of CBP Form 7501, or a form on the letterhead of the proprietor, which provides as account of the disposition of the merchandise covered by the blanket permit. The form must bear the words "Blanket Permit Summary" in capital letters conspicuously printed or stamped in the top margin. On the form, the proprietor must certify that the merchandise listed thereunder was withdrawn in compliance 19.6 (d), and must account for all of the merchandise withdrawn under the blanket permit by tariff number, quantity, and value. If applicable the account must separately list and identify merchandise withdrawn for:
>
> - Duty-free store exportation
> - Vessel or aircraft supply use
> - Personal or official use

[redacted] stated that it is not a normal practice of entry personnel to determine whether documents received are fraudulent. If a determination has been made that documentation was questionable beyond a reasonable doubt, then a referral is made to the Broker Review Analysis Verification Office for a more thorough review. Per [redacted] [redacted] submitted their documents in accordance to regulations and remained the same over the past ten years. Since 2009, [redacted] stated that [redacted] only connection to [redacted] is the review of their final

documentation submitted. [redacted] added that she has supervised [redacted] for several years and has always found her work to be impeccable and her integrity above reproach. (Exhibit 5)

A TOIG review of [redacted] affidavit to [redacted] states companies normally file a 7512 for each withdrawal. However, CBP allows [redacted] to file a 7501 with the stamp "Blank Permit" for each withdrawal. [redacted] also types the words "For Export Only" on the 7501. [redacted] stated that she was trained to process [redacted] withdrawals this way. [redacted] has previously asked why [redacted] is allowed to file 7501s instead of 7512s. However, no one could explain why. [redacted] stated that [redacted] are not required to physically go to the warehouses to verify merchandise withdrawals.

[redacted] stated that she did not assist [redacted] with processing fraudulent documentation. In addition, [redacted] denied providing [redacted] ship stamps; visiting the warehouse; having a relationship with anyone affiliated with [redacted] or knowingly or intentionally assisting [redacted] in obtaining alcohol and tobacco products tax free. (Exhibit 6)

[**Agent's Note**: TOIG attempted to interview [redacted] however, per the advice of a representative from the National Treasury Employee Union, [redacted] declined because TOIG could not provide a Kalkines Warning. [redacted] agreed to incorporate TOIG's questions during the interview.]

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegation was unsubstantiated. [redacted] stated that she did not assist [redacted] with processing fraudulent documentation. In addition, [redacted] denied providing [redacted] ship stamps; visiting the warehouse; having a relationship with anyone affiliated with [redacted] or knowingly or intentionally assisting [redacted] in obtaining alcohol and tobacco products tax free.

Distribution

[redacted] TTB

Signatures

Case Agent:

[redacted]

12/14/12
Date

Supervisor:

[redacted]

12/20/12
Date

Exhibits

1. Lead Initiation Document from [redacted] dated May 2, 2012.
2. Memorandum of Activity, Interview with [redacted] [redacted] dated July 27, 2012.
3. Memorandum of Activity, Document Review of ROI prepared by [redacted] dated October 16, 2012.
4. Memorandum of Activity, Document Review of ROI prepared by [redacted] dated October 16, 2012.
5. Memorandum of Activity, Document Review of [redacted] Affidavit, dated October 16, 2012.
6. Memorandum of Activity, Document Review of [redacted] Affidavit, dated October 23, 2012.

REPORT OF INVESTIGATION
USM-11-0062-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
Philadelphia, PA

Case #: USM-11-0062-I

Case Type: Criminal X
Administrative ____
Civil ____

Investigation Initiated: October 14, 2010

Investigation Completed:

Conducted by: [redacted]
Special Agent

Origin: Internal Revenue Service
Criminal Investigations

Approved by: [redacted]
Special Agent in Charge

Summary

On October 14, 2010, the U.S. Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG), initiated an investigation based on information received from the Internal Revenue Service (IRS), Criminal Investigations (CI), concerning allegations that U.S. Mint (Mint) Police Officer [redacted] was involved in a money structuring and money laundering scheme.

The investigation determined that the allegations are substantiated. [redacted] confessed that he stole Mint error coins from the Philadelphia Mint facility over a five-year period. [redacted] sold coins to [redacted] of [redacted] Numismatic Corp. (BNC), for which he received payments totaling $2,423,907. On September 8, 2011, [redacted] pled guilty to a four count Criminal Information. On September 13, 2012, [redacted] was sentenced in the District of New Jersey to 36 months of incarceration, three years of supervised release, ordered to pay $15,208 in restitution to the Mint, forfeit $2.3 million in forfeitable assets, and pay a $400 special assessment fee. Additionally, [redacted] was ordered to resolve his tax liability of $801,651 with the IRS.

Basis and Scope of the Investigation

This investigation was initiated on October 14, 2010, based on allegations and supporting documentation provided by IRS-CI. IRS-CI forwarded copies of financial records concerning potential structuring and laundering of funds, which were associated with [redacted] accounts at the Police and Fire Federal Credit Union, Philadelphia, PA.

In September 2010 and November 2010, [redacted] was interviewed by IRS-CI. On both occasions, [redacted] denied structuring cash withdrawals. He alleged that his source of cash came from retirement income and his savings account. [redacted] reported he was a retired [redacted]. [redacted] also reported he made $100,000 to $200,000 from the sale of coins he inherited from his deceased aunt. [redacted] further explained his aunt gave him 25, 5-gallon buckets of "old" coins, which he sold to [redacted] (Exhibit 1)

According to [redacted] financial records from March 2007 to July 2010, [redacted] received at least 47 check payments from [redacted] and BNC totaling approximately $2.3M. Specifically, on a check dated May 28, 2008 for $25,000 from [redacted] the memo section of the check stated, "Mint Errors." The individual checks [redacted] provided to [redacted] as payment for mint error coins, ranged from approximately $10,000 to $114,000. Additionally, [redacted] bank records revealed structured check and cash withdrawals totaling approximately $1.43M. Furthermore, an initial review of FedEx records associated with [redacted] and [redacted] revealed that [redacted] frequently corresponded with [redacted] at his home address, [redacted] over the three-year period that [redacted] made check payments to [redacted] (Exhibit 2)

[redacted] was employed as a Mint Police Officer in Philadelphia, PA, from June 1996 until his retirement on January 31, 2011. [redacted] maintained the night-shift assignment from 12-midnight to 8 am, where his primary duties included patrolling the Mint facility, and standing post.

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted], Special Agent, IRS-CI
- [redacted], Field Chief, Mint Police, Philadelphia Mint
- [redacted], San Clemente, California
- [redacted], Mint Headquarters
- [redacted] Mint Police, Philadelphia Mint

In addition, TOIG reviewed pertinent documents, including:

- Financial Records associated with [redacted]
- Invoices and other documents relating to business transactions between [redacted] and [redacted]

Investigative Activity

When interviewed by TOIG, [redacted] revealed that he has purchased many Presidential Dollar coins with the missing edge lettering (MEL) since 2007 when they went into production. [redacted] indicated that most of his MELs came from [redacted] who claimed to have gotten them from

counting rooms. [redacted] further revealed that in 2005 or 2006, [redacted] mailed him a handwritten letter on lined notebook paper inquiring about the sale of some Martha Washington test "tokens." [redacted] stated that enclosed with the letter was a Xerox/color photo of a nickel- and quarter-size Martha Washington tokens, with the Washington Monument on the reverse side. [redacted] further stated that he called [redacted] and found out that [redacted] aunt died and he came across these coins in her attic. [redacted] indicated that he purchased eight of these Martha Washington tokens from [redacted] along with some old silver pieces, and wrote him a check for $2,000 to $3,000. [redacted] stated that he no longer had the Martha Washington tokens in his collection. [redacted] also revealed that in 2007 he purchased about 4,000 MEL Washington Dollars from [redacted] who alleged were from his deceased aunt. [redacted] indicated that he instructed [redacted] to mail the coins via Express Mail from the U.S. Postal Service.

[redacted] revealed that since 2007, he purchased a hundreds of Sacagawea Dollar planchets (in circulation from 1999 to 2000), along with hundreds to thousands more of the Presidential Dollars. [redacted] clarified that of the MEL Presidential Dollars, the errors were not just the MEL and also included blanks, off-center strikes, and double struck coins. He also claimed that some of them were regular Presidential Dollars that did not have any errors. [redacted] indicated that because he would receive such a large quantity from [redacted] he would just buy them in the bulk quantity from [redacted] and later go through them and slab the coins that he thought were worth grading.

After the Washington Dollars, [redacted] purchased about 800-900 Jefferson Dollars at $70 to $75 each from [redacted] felt he overpaid for these, but thinks he still made a good deal. Then he purchased Madison Dollars from [redacted] but could not recollect how many or how much he paid for these. However, [redacted] indicated that these were more valuable. [redacted] did not recall purchasing any Monroe Dollars from [redacted] but claimed he purchased approximately 5,000-7,000 of the Quincy Adams Dollars from [redacted] He said he paid $50 to $60 for each of these. [redacted] revealed that he became discouraged after the Quincy Adams Dollars, and that his business with [redacted] began to dwindle shortly thereafter, mainly because of the large quantities of MELs that were available.

[redacted] explained that over the first year to year and half that he corresponded with [redacted] he gave [redacted] his Express Mail account information and all [redacted] had to do was place items in a shipping box and attach the mailing labels. However, later on [redacted] changed over to FedEx, but he continued the same system of prepaid labels with [redacted] believed the coins were shipped loose in a bag, which were placed in a shipping box. [redacted] expressed that his last business transaction with [redacted] was the Fillmore Dollars in June 2010. [redacted] claimed he did not have any knowledge of [redacted] working for the Mint. He reported that his transactions with [redacted] over a four-year period likely totaled between $2M to $2.4M, and that most of it was from MELs. [redacted] sent all checks FedEx to [redacted] residence in [redacted] (Exhibit 3)

When interviewed by TOIG, [redacted] indicated that his work shift at the Mint was 11:30pm to 7:30am. In the morning, he worked at the employee entrance, and throughout most of the shift, [redacted] patrolled the entire Mint including the offices, die shops and blanking and coining areas.

[redacted] admitted that he stole coins from the Mint. [redacted] revealed that he took a couple of shaving/toiletry-type bags and proceeded to the coining area where the Presidential Dollar coins were made. [redacted] looked for the bin that had the MEL Presidential Dollar coins, proceeded to the non-edge tank, and just pulled the coins out of the open tank with his hands, and placed the coins into the bags. [redacted] then took the bags filled with the coins and placed them in his coin locker by the front entrance of the Mint. Prior to reaching the coin locker, [redacted] would walk through the metal detector towards the officer in the front entrance and he would relieve that officer. At the end of his shift, in the morning, [redacted] would return to the coin locker, place the smaller bags of coins in a larger overnight/shopping bag and carry the bags, filled with stolen coins, out of the Mint.

[redacted] stated that he stole the coins when no one else was working on the Mint production floor, usually on weekends. [redacted] stole the Presidential Dollar coins since they went into production in 2007. He also stole Martha Washington test tokens that were kept at his friend, [redacted] desk drawer, who had retired from the Mint. [redacted] indicated that one day he was sitting alone at [redacted]'s desk, opened the top drawer of the desk and noticed some coins. He took about three or four Martha Washington coins from the desk drawer. This happened in approximately 2001 or 2002, and was the first time [redacted] had stolen anything from the Mint. [redacted] stated that no one else assisted him with stealing coins from the Mint. He revealed that all the coins that he sold to [redacted] were stolen from the Mint.

[redacted] sold [redacted] Martha Washington tokens, Sacagawea coins, and Presidential Dollar coins, until about the third or fourth Presidential Dollar coin was produced. [redacted] explained that he mailed [redacted] the coins from a U.S. Post Office in NJ. However, when shipping costs became expensive, [redacted] shipped him pre-paid FedEx labels. Additionally, he stated that after [redacted] received the coins, he would FedEx the check payments to [redacted] for the coins. [redacted] explained that he stole coins after noticing that no one was on the Mint production floor during the night shift on the weekends. [redacted] stated that no one ever made him put his bags through the X-ray machine, and he always took the stolen coins out of the Mint during the shift change. (Exhibit 4)

Referrals

On November 10, 2010, this matter was presented and accepted for criminal prosecution by AUSA [redacted], USAO, District of New Jersey, Camden Office. (Exhibit 5)

Judicial Action

On September 8, 2011, [redacted] pled guilty to a Criminal Information on four counts: a) 18 U.S.C. 641 – Theft of Government Property, b) 18 U.S.C. 1341 – Mail Fraud, c) 18 U.S.C. 1957 – Money Laundering, and d) 26 U.S.C. 7201 – Evasion of Income Tax (Exhibit 6)

On October 19, 2011, in a subsequent plea hearing, U.S. District Judge [redacted], District of New Jersey, formally accepted [redacted] guilty pleas to all four counts. (Exhibit 7)

On September 13, 2012, [redacted] was sentenced to 36 months of incarceration, three years of supervised release, ordered to pay $15,208 in restitution to the Mint, forfeit $2.3 million in forfeitable assets, and pay a $400 special assessment fee. Additionally, [redacted] was ordered to resolve his tax liability of $801,651 with the IRS. (Exhibit 8)

Findings

The investigation determined that the allegations are substantiated. [redacted] confessed that he stole Mint error coins from the Philadelphia Mint facility over a five-year period. [redacted] sold coins to BNC, for which he received payments totaling $2,423,907. On September 8, 2011, [redacted] pled guilty to a four count Criminal Information. On September 13, 2012, [redacted] was sentenced in the District of New Jersey to 36 months of incarceration, three years of supervised release, ordered to pay $15,208 in restitution to the Mint, forfeit $2.3 million in forfeitable assets, and pay a $400 special assessment fee. Additionally, [redacted] was ordered to resolve his tax liability of $801,651 with the IRS.

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policy(ies) were violated or could be applied to the case:

- 18 U.S.C. 641 – Theft of Government Property
- 18 U.S.C. 1341 – Mail Fraud
- 18 U.S.C. 1957 – Money Laundering
- 26 U.S.C. 7201 – Evasion of Income Tax

Distribution

[redacted], Chief, U.S. Mint Police

Signatures

Case Agent:

[redacted] 11/19/12
Date

Supervisor:

[redacted] 11/19/12
Date

Exhibits

1. Lead Initiation Document/Memorandum of Activity, Interview of Steve Helmstetter, dated October 29, 2010.

2. Memorandum of Activity, LEO Activity: Record/Information Review ([redacted] Financial Records), dated October 29, 2010.

3. Memorandum of Activity, Interview of [redacted] dated February 1, 2011.

4. Memorandum of Interview by IRS, [redacted] dated February 9, 2011.

5. Memorandum of Activity, Judicial: Referral/Acceptance, dated November 10, 2010.

6. Memorandum of Activity, Judicial: Information, dated September 8, 2011.

7. Memorandum of Activity, Judicial: Other, dated October 19, 2011.

8. Memorandum of Activity, Judicial: Sentencing, dated September 13, 2012.

REPORT OF INVESTIGATION
USM-12-0406-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case Type: Criminal
Administrative X
Civil

Investigation Initiated: December 7, 2011

Investigation Completed: APR 19 2012

Conducted by: [redacted]
Special Agent

Origin: Bureau Referral

Approved by: [redacted]
Special Agent in Charge

Case #: USM-12-0406-I

Summary

On December 7, 2011, the Department of the Treasury Office of Inspector General (TOIG) opened an investigation based on a referral from the United States Mint (USM) alleging that USM employee [redacted] had been viewing pornography on his USM-issued laptop computer. TOIG's investigation, which included digital forensic analysis and a confession by Hebron during his interveiw substantiated the allegation.

Basis and Scope of the Investigation

During the course of the investigation, the TOIG conducted digital forensic analysis on [redacted] USM-issued laptop computer and interviewed Hebron.

Investigative Activity

On December 6, 2011, USM Police submitted a report to the TOIG hotline detailing the allegation that [redacted] had been viewing pornography on his USM-issued laptop computer. (Exhibit 1)

In conjunction with USM Information Security Analyst [redacted], TOIG decrypted [redacted] USM-issued laptop on January 30, 2012 and created a verified, bit-stream image of its internal hard drive. (Exhibit 2)

On January 30, 2012, TOIG reviewed Workforce Analytics and National Crime Information Center (NCIC) records pertaining to [redacted] with no derogatory information located. (Exhibit 3)

On April 6, 2012, TOIG completed the digital forensic analysis of [redacted] USM-issued laptop, the results of which supported the allegation that [redacted] had been using it to view pornography. (Exhibit 4)

On April 9, 2012, TOIG interviewed [redacted] who stated that he was aware that viewing pornography on USM-issued computers was against USM policy and admitted to viewing pornography on his USM-issued laptop for approximately 45 minutes to an hour a day after he completed his assigned work. [redacted] then reviewed the TOIG digital forensic report and confirmed that he had viewed all the images, movies and web pages listed in the report. [redacted] stated that had an addiction to pornography and was currently seeking help for his addiction. (Exhibit 5)

On April 10, 2012, TOIG reviewed USM Form 2240, United States Mint IT System Rules of Behavior, which [redacted] signed on November 1, 2011 acknowledging that he would use information systems in compliance with "Federal law, regulation and United States Mint Policy." TOIG then reviewed Treasury Directive 87-04, Personal Use of Government Information Technology Resources, which stated that "Government IT systems are not to be used for downloading, accessing or using illegal, inappropriate, and/or unauthorized content." (Exhibit 6)

Referrals

Not Applicable.

Judicial Action

Not Applicable.

Findings

TOIG's investigation substantiated that [redacted] viewed pornography on his USM-issued computer in violation of United States Mint IT Systems Rules of Behavior and Treasury Directive 87-04, Personal Use of Government Information Technology Resources.

Distribution

[redacted] Chief, United States Mint Police

Signatures

Case Agent:

[redacted]

4/18/2012
Date

Supervisor:

[redacted]

4-18-12
Date

Exhibits

1. USM Police Referral, dated December 6, 2011.
2. Memorandum of Activity, Digital Evidence Acquisition, dated January 30, 2012.
3. Memorandum of Activity, Initial Record Review, dated January 30, 2012.
4. Memorandum of Activity, Digital Forensic Analysis, dated April 6, 2012.
5. Memorandum of Activity, Interview of [redacted], dated April 9, 2012.
6. Memorandum of Activity, Use of Government IT, dated April 10, 2012.

REPORT OF INVESTIGATION
USM-12-0871-I

Office of Inspector General

United States Department of the Treasury

Office of the Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]

Case #: USM-12-0871-I

Investigation Initiated: January 3, 2012

Case Type: Criminal ___ Administrative x Civil ___

Investigation Completed: MAR 29 2012

Conducted by: [redacted]
Special Agent

Origin: [redacted]
Chief, United States Mint Police

Approved by: [redacted]
Special Agent in Charge

Summary

On January 3, 2012, the Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), was advised by U.S. Mint (USM) Police of an allegation of theft involving the unauthorized use of the USM's Federal Express account.

On December 12, 2011, former USM employee, [redacted] sent a personal package via Federal Express utilizing a USM Federal Express direct billing account number. [redacted] was an employee with the USM, but had transferred to another federal agency in February 2010. [redacted] currently works for the Federal Insurance Deposit Corporation (FDIC) as a Senior Administrative Specialist.

On February 13, 2012, TOIG interviewed [redacted] She stated she recalled sending the package, but did not realize she had utilized a USM Federal Express bill. [redacted] stated she would rectify the situation immediately.

On February 14, 2012, [redacted] was provided with payment information. TOIG received notification from [redacted] that she had made contact with the appropriate individuals and made the appropriate payment.

On March 23, 2012, TOIG contacted Fedex Government services and verified that invoice #[redacted] was paid in full on February 14, 2012.

Our investigation has substantiated the allegation, however there was no loss to the government and the actions of the former USM employee were deemed unintentional.

Basis and Scope of the Investigation

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Senior Administrative Specialist, FDIC

Investigative Activity

On January 3, 2012, the Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), was advised by USM Police of an allegation of unauthorized use of the USM's Federal Express account.

On December 12, 2011, former USM employee, [redacted] sent a personal package via Federal Express utilizing a USM Federal Express direct billing account number. [redacted] was an employee with the USM, but had transferred to another federal agency in February 2010. [redacted] currently works for the Federal Insurance Deposit Corporation (FDIC) as a [redacted]

On December 29, 2011, USM employee, [redacted], advised USM Detective [redacted] that he had been contacted by the Administrative Resource Center, Bureau of Public Debt (ARC) regarding a bill from Federal Express in the amount of $60.20. [redacted] was contacted because the USM had closed their account with Federal Express and had been utilizing United Parcel Services (UPS) since October 2011. (Exhibit 1)

On February 13, 2012, TOIG interviewed [redacted] She stated she recalls sending the package, but did not realize she had utilized a USM Federal Express bill. [redacted] stated she would rectify the situation immediately. She further stated she would examine all Federal Express preprinted bills to ensure she was not in possession of other USM labels. (Exhibit 2)

On February 14, 2012, [redacted] was provided with payment information. TOIG received notification from [redacted] that she had made contact with the appropriate individuals and made the appropriate payment. (Exhibit 3)

On March 23, 2012, TOIG contacted Fedex Government services and verified that invoice #[redacted] was paid in full on February 14, 2012. (Exhibit 4)

Referrals

None

Judicial Action

None

Findings

Our investigation has determined the allegation is substantiated, although it has been determined that the action taken by [redacted] was due to an oversight on her part.

Distribution

[redacted] Chief, United States Mint Police

Signatures

Case Agent: [redacted]

3/27/12
Date

Supervisor: [redacted]

3-27-12
Date

Exhibits

1. Lead Initiation documents, dated January 3, 2012.
2. Memorandum of Activity, Interview of [redacted] FDIC, dated February 13, 2012.
3. Email correspondence with [redacted] dated February 14, 2012.
4. Memorandum of Activity, Interview of [redacted], Fedex, dated March 23, 2012.

REPORT OF INVESTIGATION
USM-12-0951-I

Office of Inspector General

United States Department of the Treasury

Office of Inspector General
U.S. Department of the Treasury

Report of Investigation

Case Title: [redacted]
[redacted] Coining Division, USM

Origin: United States Mint

Case #: USM-12-0951-I
Case Type: Criminal ___
Administrative X
Civil ___

Investigation Initiated: February 27, 2012

Conducted by: [redacted]
Special Agent

Investigation Completed: MAY 08 2012

Approved by: [redacted]
Special Agent in Charge

Summary

On February 27, 2012, the Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), initiated an investigation based on information received from the United States Mint (USM) alleging that [redacted] USM Philadelphia, PA was detected entering the building with 18 penny blanks and one dime blank inside a clear plastic bag within [redacted] hand bag. (Exhibit 1)

The investigation determined that the allegation is substantiated. [redacted] attempted to return 18 penny blanks and one dime blank to the Philadelphia USM after he discovered them in his clothing at his residence. [redacted] stated he did not intentionally remove the blanks from the building and opined they likely fell into his shirt pockets while he was working on the factory floor. On March 31, 2012, [redacted] voluntarily retired from the USM.

Basis and Scope of the Investigation

This investigation was initiated on February 27, 2012, based on information submitted by [redacted], Chief, USM Police, which included USM Police Report [redacted], prepared by Officer [redacted] USM Police. Additionally provided were written statements of [redacted] and Officer [redacted].

According to the USM Police Report, on February 22, 2012, Officer [redacted] was assigned to Post #5 when at 9:53PM, [redacted] placed a personal hand bag through the x-ray machine. Officer [redacted] detected what appeared to be several coins inside the bag and he informed [redacted] of this. [redacted] sat down and began searching through his bag. When Officer [redacted] volunteered to assist [redacted] look for the coins, [redacted] retrieved a clear plastic bag from inside the hand bag and stated "blanks".

Officer [redacted] observed several copper colored blanks inside the clear plastic bag so he informed [redacted], Sergeant, USM Police. Sergeant [redacted] obtained custody of the clear plastic bag containing 18 blank pennies and one blank dime. [redacted] was subsequently taken to the USM Police Office where he provided a written statement. Officer [redacted] also provided a statement on the incident. (Exhibit 1)

During the course of the investigation, TOIG conducted relevant interviews with:

- [redacted] Press Operator, Coining Division, USM
- [redacted] Officer, USM Police, USM

In addition, TOIG reviewed pertinent documents, including:

- USM Police Report and Statements

Investigative Activity

In an interview with TOIG, Officer [redacted] confirmed when using the x-ray machine he detected coins inside [redacted] hand bag and informed [redacted] of his discovery. After [redacted] searched through his bag for several minutes without producing the coins, Officer [redacted] offered his assistance in looking for the coins. When Officer [redacted] approached [redacted] pulled a clear plastic bag out of his hand bag and said "blanks".

Officer [redacted] stated the clear plastic bag contained approximately 19-20 copper-colored objects which appeared to be penny blanks. Officer [redacted] consequently informed Sergeant [redacted] who took custody of the clear plastic bag and its contents. According to Officer [redacted] claimed he discovered the blanks in his clothing when he returned home from the prior work week and he wanted to return the blanks. (Exhibit 2)

In an interview with TOIG, [redacted] said on Friday, February 17, 2012, he returned home from his shift and when doing laundry he discovered 18 penny blanks and one dime blank in his clothing. [redacted] placed the blanks in a clear plastic bag intending to return them to the USM. [redacted] recalled February 20, 2012, was a Federal Holiday and his Alternate Work Schedule (AWS) day was on February 21, 2012, so he did not return to work until Wednesday, February 22, 2012. [redacted] confirmed he placed his hand bag through the x-ray machine and a USM Police Officer informed [redacted] of coins detected in his bag. According to [redacted] he retrieved the clear plastic bag from his hand bag, showed it to the officer, and informed the officer the contents were "blanks". [redacted] said the officer took custody of the blanks before obtaining a written statement from [redacted]

[redacted] claimed he did not intentionally remove the blanks from the USM building and does not know how he got them through security. [redacted] opined the blanks fell into his clothing while working on the factory floor. [redacted] said whenever he leaves the USM building, he checks his clothing for blank pennies and dimes. [redacted] reported on past occasions he has found blanks in his pockets which he deposits into the "amnesty box" when going through security to leave the building. [redacted] stated when he found the blank pennies and blank dime in his clothing he did not throw them in the trash because he knew they were USM property so he decided to return them to the USM. (Exhibit 3)

Referrals

N/A

Judicial Action

N/A

Findings

The investigation determined that the allegation is substantiated. [redacted] attempted to return 18 penny blanks and one dime blank to the Philadelphia USM after he discovered them in his clothing at his residence. [redacted] stated he did not intentionally remove the blanks from the building and opined they likely fell into his shirt pockets while he was working on the factory floor. On March 31, 2012, [redacted] voluntarily retired from the USM. (Exhibit 4)

Based on the findings of our investigation, it appears that the following pertinent statute(s), regulation(s) and/or policies were violated or could be applied to the case:

- 31 Code of Federal Regulations (CFR) 91, Regulations Governing Conduct In or On the Bureau of the Mint Buildings and Grounds. Specifically, 31 CFR § 91.4 - Preservation of Property which states "It shall be unlawful for any person without proper authority to willfully destroy, damage, deface, or remove property or any part thereof or any furnishings therein."

Distribution

[redacted], Chief, USM Police, USM

Signatures

Case Agent:

[redacted] 5/7/12
Date

Supervisor:

[redacted] 5-7-12
Date

Exhibits

1. Lead Initiation, dated February 24, 2012.
2. Memorandum of Activity, Interview of [redacted] dated March 20, 2012.
3. Memorandum of Activity, Interview of [redacted] dated March 20, 2012.
4. Standard Form 50, Voluntary Retirement of [redacted] dated March 31, 2012.