



governmentattic.org

"Rummaging in the government's attic"

Description of document: List of all Department of the Treasury Office of Inspector General (OIG) investigative cases closed in CY 2017

Requested date: 2017

Release date: 17-November-2017

Posted date: 03-January-2020

Source of document: FOIA Request
FOIA and Transparency
Department of the Treasury
Office of the Inspector General
Washington, DC 20220
Fax: 202-622-3895
[Online FOIA Request Form](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: Delmar, Richard K.<DelmarR@oig.treas.gov>
Sent: Fri, Nov 17, 2017 2:41 pm
Subject: FOIA-Treasury OIG-closed cases

Responding to your FOIA request 2017-11-083 for a list of all investigative cases closed in CY 2017 at Treasury OIG. The list is attached, with names and other particular identifying information of subjects and witnesses redacted per FOIA Exemption 7C, 5 U.S.C. § 552(b)(7)(C)

The redactions constitute a partial denial of your request, and therefore an adverse action under the FOIA. Accordingly, you have the right to appeal this determination within 90 days from the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. Your appeal must be in writing, be signed by you or your representative, and contain the rationale for your appeal. Please address your appeal to:

FOIA Appeal
FOIA and Transparency
Privacy, Transparency, and Records
Department of the Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

If you would like to discuss this response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact the Treasury DO FOIA Public Liaison at (202) 622-8098 or email FOIAPL@treasury.gov.

If you are unable to resolve your FOIA dispute through our FOIA Public Liaison, the Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and federal agencies as a non-exclusive alternative to litigation. If you wish to contact OGIS, you may write directly to:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001
ogis@nara.gov
ogis.archives.gov

Please call me if you have questions.

Rich Delmar
Counsel to the Inspector General
Department of the Treasury

BANK-10-2246-I	LA JOLLA BANK BANK-10-2246-I	Referral for Investigation Memorandum from TOIG-OA. Material Loss Review conducted by OA of LaJolla Bank, FSB revealed ongoing investigations of the bank's lending practices involving the CEO and CCO with regard to potential fraudulent transactions and insider abuse.	17
BANK-11-0677-I	FIRST NATIONAL BANK OF BARNESVILLE BANK-11-0677-I	Correspondence received via OIG Intake regarding allegations of fraudulent activity by the CEO and loan officer of First National Bank of Barnesville as well as an appraiser doing business with First National Bank. There is said to be no open investigation by the OCC or the FDIC at this time.	3
FMS-12-0315-I	██████████ FMS-12-0315-I	In response to the BFS's efforts to collect on a debt, subject submitted a letter, purporting to be from the BFS's collection company, acknowledging that he had paid his debt in full; however, there is no record of any such payment and the letter appears to be fraudulent.	15
MSB-12-2214-I	WESTERN UNION	The US Department of Justice (DOJ) is looking into whether Western Union was aware that a California franchisee, US Shen Zhou, transmitted approximately \$60 million in sub-\$2,000 increments to the Peoples' Republic of China (China) in a single year - making it the largest remitter of funds to China in the Western Union network. DOJ is "looking to augment [its] investigative abilities to determine whether charges are appropriate."	1
BFS-13-0160-I	██████████ BFS-13-0160-I	Complaint received 10/23/2012, via email Complainant alleges fraud concerning US Savings Bonds	20
CFIF-13-0445-I	██████████ . CFIF-13-0445-I	Complaint received 12/27/2012, via email Complainant alleges - On 12-05-12, an subjects cashed a fraudulent US treasury Check for \$2978.00. Approximately ten minutes later at register 14, the same subjects cashed a fraudulent US Treasury Check for \$2946.72. The subjects then leave in a Silver Dodge Ram Truck.	0
BANK-13-0756-I	FLAGSHIP BANK FAILURE BANK-13-0756-I	The Federal Deposit Insurance Corporation OIG-OI requested TOIG assistance with an investigation of Flagship Bank in Florida regarding a straw borrower scheme used to circumvent banking regulations. Case stems from bank failure in 2009 and MLR completed by TOIG OA. On 7/13/10, TOIG-OA forwarded to TOIG-OI, a referral for investigative review arising from information identified during a Material Loss Review of the Subject bank. Allegations concern potential fraudulent loan modification practices promoted and committed by Flagship National Bank to enable lender to circumvent federal lending limits. OCC advised their office is not pursuing enforcement action, however TOIG-OA has learned the FBI and the FDIC-OIG are conducting an investigation into the subject loan transaction.	0
DO-13-0473-I	STANDARD CHARTER DO-13-0473-I	Correspondence received via OIG Intake from OC regarding the following: This qui tam complaint alleges that Standard Charter made misrepresentations in the course of negotiating a settlement for its violations of IEEPA sanction regulations. Keywords: Qui Tam	0
DO-14-0510-I	DEWIND CO. DO-14-0510-I	On 1/13/2014, TOIG was contacted by the USAO for the Central District of California regarding a Qui Tam case. The defendant is DeWind Company et al.	1

BFS-14-0533-I	[REDACTED] AND [REDACTED] [REDACTED] BFS-14-0533-I	An Internal Revenue Service (IRS) Auditor discovered discrepancies in business transactions at Vision Enterprises, during a routine audit. Transactions showed an employee of the Financial Management Service (FMS), used thier government charge card to make purchases coded as "office supplies". The business owner admitted no actual purchases occurred and they then wire a percentage of the purchase to a Treasury Department Federal Credit Union account personally owned by the subject employee. Treasury records show the employee previously worked for FMS but is not currently an employee.	0
BEP-14-0583-I	[REDACTED], ET AL. BEP-14-0583-I	Correspondence received via OIG Intake from BEP regarding allegations of possible money laundering scheme by 3 sisters who submittted mutilated currency claims to BEP. They claimed to have buried their life savings totaling \$283,000.00.	0
BFS-14-1429-I	[REDACTED], ET AL. BFS-14-1429-I	On May 4, 2014, the Department of the Treasury, Office of Inspector General (DOT-OIG), Office of Investigations (TOIG), received an OIG Hotline call fregarding stolen U.S. Treasury checks. The complainant claimed her sister deposited five U.S. Treasury checks belonging to the complainant into a Bank of America account in Charleston, SC. The complainant stayed and cared for her mother in Charleston, SC for approximately six months. The complainant requested an address change through the Department of Education (DOE) to receive her U.S. Treasury checks during that period. The sister admitted to the complainant that she deposited five U.S. Treasury checks belonging to the complainant. The sister believed teh complainant owed her money and used the U.S. Treasury checks addressed to her as payments.	20
SCAM-14-2100-I	[REDACTED] SCAM-14-2100-I	Complaint receive 7/3/2014, via email *** COMPLAINANT REQUESTS CONFIDENTIALITY *** Complainant received a fraudulent phone call from Jeff Daniels purporting to be from the US Treasury, offering a Grant of \$7000.00. The complainant was asked for a processing and the complainant gave him \$600.00 to receive the \$7000. Grant. The complainant is unable to contact Mr. Daniels since sending him the money.	2
CFIF-15-0757-I	[REDACTED], ET AL.	On 12/1/2014, USPS OIG, Providence, RI, contacted TOIG regarding a missing TSP check worth \$9,950. SAC responded with information from TCIS, and SA had subsequent regular contact with USPS OIG. USPS OIG has had other checks of interest that they believe were stolen by a USPS employee at the Providence Processing and Distribution facility. Loss of three checks at this time totals approximately \$20,000.	0
BFS-15-0818-I	[REDACTED] BFS-15-0818-I	On December 16, 2014, TOIG received an email from a Detective, Dekalb County Police Department, regarding suspected counterfeit U.S. Treasury checks. Detective requested TOIG assistance in determining the victims and how to identify the checks as counterfeit. On July 11, 2014, the subject entered the Beverage Club, Stone Mountain, GA, and presented U.S. Treasury check in the amount of \$495.00, dated June 10, 2014, for negotiation. On June 14, 2014, the subject entered the Beverage Club and presented U.S. Treasury check in the amount of \$490.00, dated June 12, 2014, for negotiation.	0

FinCEN-15-0828-I	CELL TOUCH JAX, INC. FinCEN-15-0828-I	On November 20, 2014, the Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TOIG), participated in meetings at the U.S. Attorney's Office in Jacksonville, FL (MDFL), regarding proactive identification of criminal violations of Title 31 and Title 18. Between July and October of 2014, Cell Touch Jax, Inc., made 723 cash deposits totaling \$3,650,829. Sixty-four of those deposits were between \$8,000 and \$10,000. In addition, in September, Cell Touch Jax, Inc. attempted to make two deposits into two separate accounts. The first deposit was for \$6,040 and the second deposit was for \$4,275. When the bank requested information so that it could file a CTR, Cell Touch Jax, Inc. canceled the transaction. AUSA requested that TOIG investigate this matter and determine if prosecutorial action is warranted.	0
BEP-15-1763-I	██████████	On June 3, 2015, the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), received a referral from the Bureau of Engraving and Printing (BEP), regarding an U.S. Treasury check issued for a processed mutilated currency claim, in the amount of \$10,000, that was mailed to Ariton, Alabama. The check was cashed, but the complainant/victim reported that she never received the check.	2
FinCEN-15-1440-I	RED WIRE FinCEN-15-1440-I	Subsequent to TOIG's participation with the FBI in Operation Top Gear, the FBI's Miami field office has now requested TOIG's participation with a new investigation. The FBI and IRS are currently investigating several individuals operating a taxi medallion finance group in the New York and Miami areas. Preliminary investigations have revealed suspected money laundering, structuring, bank fraud, wire fraud and specific BSA violations.	30
USM-15-1070-I	██████████, ET AL USM-15-1070-I	On 2/18/15, USM CIO ██████████ met with TOIG to advise that 2 Senior USM IT officials were gaining access to all Treasury emails and that they were not authorized to view these files. Buscher provided a list with approximately 14 names of individuals believed to have access to Treasury wide email accounts.	0
USM-15-1471-I	██████████ USM-15-1471-I	Correspondence received via OIG Intake from the USM regarding allegations of unauthorized government computer use by preparing and billing for tax preparations for HR Block on government time.	0
SCAM-16-0119-I	██████████ SCAM-16-0119-I	Complaint received 10/15/2015, via mail Complainant alleges made several payments to US Dept. of the Treasury Michael Cena in order to receive \$10.2 Million. The complainant received several emails directing her to send money via Western Union Money Transfer.	15
BFS-15-2112-I	██████████ BFS-15-2112-I	Subject is using a Treasury Direct account as a holding fund for monies that he has fraudulently obtained from at least one private citizen, and that he has attempted to obtain from multiple banks. keyword: vulnerable population BFS	1
BFS-15-1987-I	██████████ TOKES AND ██████████ ██████████ BFS-15-1987-I	Bank President reports to the Bureau of the Fiscal Service that a subject has created a TreasuryDirect account that is being used to accumulated monies being fraudulently drawn from the bank account of elderly/retired citizen more than \$810,000.	2

CYBER-15-2043-I	██████████	CYBER-15-2043-I	On July 1, 2015, FBI, Baltimore ECTF, contacted TOIG requesting to co-case a possible network intrusion at Laureate Education, Inc, Baltimore, MD. Forty student OCC regulated bank accounts were re-routed to one single Greendot account for a loss of \$73,996.00. Initial investigation reveals that a possible subject is an employee of Laureate Education, Inc. Subject accessed student's bank account information, routing numbers and possibly emails as well as passwords.	0
BFS-15-2198-I	██████████	, ET AL. BFS-15-2198-I	On July 2, 2015, USSS Jacksonville requested TOIG assistance with a stolen Treasury check case that had been referred to them by BFS. Subject and his co-conspirators obtained three stolen Treasury checks and deposited them into Navy Federal Credit Union accounts via mobile banking. The check payee name was altered from the true payee to Arcadio Blair. After reviewing the documents, two additional stolen US Treasury checks were identified. The US Attorney's Office in Jacksonville is considering pursuing federal charges against the subjects. If they decline, the chief of the special prosecution section of the State Attorney's Office has agreed to file charges, at this time.	0
BFS-15-2206-I	██████████	BFS-15-2206-I	On August 14, 2015, Jacksonville Sheriff's Office (JSO) asked TOIG to assist with investigating a subject who opened a fraudulent account and deposited twenty-three (23) U.S. Treasury checks, payable to multiple payees, and other suspicious checks.	1
BFS-15-2284-I	██████████	BFS-15-2284-I	Large dollar U.S. Treasury check labeled as counterfeit received from BFS.	0
USM-15-2285-I	██████████	USM-15-2285-I	Correspondence received via OIG Intake from the USM regarding allegations of a subject employee trying to convince fellow co workers to call off of work to get back at management.	0
BEP-16-0240-I	██████████	AND ██████████ ██████████ BEP-16-0240-I	Correspondence received via OIG Intake from the BEP regarding allegations of subjects submitting two different mutilated currency claims in the amount of \$9,900 each. One claim submitted by on February 27, 2015 in the amount of \$9,900 and the other on March 30, 2015 in the amount of 9,900. MCD/OFM notified the Product and Investigation Branch of the suspicious claims as it appears the individuals are structuring their redemption transactions to evade the reporting requirements.	1

OCC-16-1031-I	[REDACTED] 1031-I	OCC-16-	<p>NC-TFCTF TFO was contacted by AUSA with the United States Attorney's Office out of the Middle District of North Carolina and instructed to contact Mr. [REDACTED] (G [REDACTED]), VP of Corporate Security for SunTrust Bank, in regards to a identity theft case. TFO met with [REDACTED] to discuss the details of this case. [REDACTED] stated that SunTrust Bank had previously had a branch manager, for their SunTrust Bank branch located at 2405 S. Church Street, Burlington, North Carolina, commit identity theft against one of it's elderly clients. [REDACTED] presented loan documents, credit card statements, deposit account statements and offsets, video surveillance and investigative notes to TFO. All of these items indicated that the subject had obtained a credit card (Mastercard) on March 5, 2015, in the victim's name without consent or authorization, and used that card for personal benefit totaling \$2706.54. Further, subject obtained a \$5000 unsecured loan in the name of the victim without consent, authorization or knowledge on March 24, 2015. These funds were deposited into the victim's SunTrust Bank account on March 24, 2015 and withdrawn by the subject on March 25, 2015. Finally, the subject used the victim's Visa credit card from April 13, 2015 through September 9, 2015 making unauthorized charges for personal benefit totaling \$4140.68. This case has been discussed and reviewed by AUSA from the United States Attorney's Office for the Middle District of North Carolina. AUSA requested a case report be forwarded to his office at the completion of the investigation for the purpose of prosecution.</p>	1
BFS-16-0431-I	TAX REFUND FRAUD - ACH PP VISA	<p>On 11/23/15, met with Haymarket PD OFC regarding providing assistance for tax refund fraud. On 2/12/15, victim filed his taxes with H&R rep. On 2/18/15, victim hadn't received any info his return was successfully filed. After contact with H&R, he was told his return was rejected because a return was already filed in his name. On 2/19/15, TCIS showed a processed ACH payment for \$9,982.00. to Sun Rise Banks (settlement bank). On 8/28/15, a paper check for \$8,531.59 was issued to and cashed.</p>	2	
OCC-16-0696-I	[REDACTED] 0696-I	OCC-16-	<p>NC-TFCTF TFO was contacted by a resident of Guilford County in regards to a local locksmith, taking an \$860 check from her as payment for him to order and install a floor safe in her home in July 2015. Locksmith has never produced or installed the safe. Further,subject has stopped returning the local victim's calls about the safe or return of the funds. During TFO's subsequent research on locksmith and all of his affiliated businesses, information was located in a FinCen database concerning one of the businesses, American Locksmith Enterprises, from 2014. In that case, subject and/or his wife, used a Chase Bank, an OCC regulated institution, credit card not belonging to them to purchase goods from Keyless Ride out of Texas. It was further learned after speaking with the victim of that case that subject attempted to use the Chase Bank credit card numerous other times without the cardholder's consent or authorization. This case was reviewed with AUSA from the U.S. Attorney's Office out of the Middle District of North Carolina. He requested a case report to be forwarded to his office at the completion of the investigation for the purpose of federal prosecution.</p>	1
BEP-16-1206-I	[REDACTED]	BEP-16-1206-I	<p>Correspondence received via OIG Intake from BEP with allegations of subject filing a suspicious mutilated currency claim on behalf of his father.</p>	1

TTB-16-1795-I	TTB TTB-16-1795-I	Correspondence received via OIG Intake from OC regarding an incoming complaint from complainant with allegations of named TTB employees leaked tax information about him to the Oregonian newspaper, he states that he is being targeted because of his political views and that one TTB employee admitted to him that his information was mishandled.	0
DO-16-1802-I	██████████ DO-16-1802-I	On May 15, 2016, TOIG received a complaint via the duty phone in regards to a subject contract employee with the Office of Technical Assistance was traveling from San Juan, Puerto Rico to Dominica on her official passport to conduct training when a Customs and Border Protection Officer located approximately 40 grams (1.4 ounces) of marijuana concealed within her baggage. TOIG was contacted by HSI San Juan and informed of the discovery.	0
BFS-16-1450-I	██████████ BFS-16-1450-I	Representative payee for payee, who passed away on 11/15/2011, benefits continued to be issued for many years in the form of paper checks. Treasury checks were suspended in August of 2015. Subject concealed payee's death and continued to cash the Social Security Checks totaling an overpayment of \$39,518 dollars.	1
BFS-16-2033-I	FEDERAL RESERVE PERSONNEL SECURITY INCIDENTS	Correspondence received via OIG Intake from BFS regarding subject not being a US citizen and has supported ITS. The individual has been employed with FRB-NY since August 2009. Added: Incident involving a Non-US citizen performing work on behalf of Treasury at the Federal Reserve Bank of Dallas. The individual has been employed by FRB Dallas since March 2015, but provided Treasury support to Moderate Risk system May - July 2016.	
CYBER-17-0115-I	LOCKY RANSOMWARE ATTACK CYBER-17-0115-I	Locky ransomware attack that affected 2 DO computers and 1 OCC computer	2
CYBER-16-2902-I	HFS FINANCIAL CYBER-16-2902-I	FBI Baltimore requested Cyber assistance for HFS Financial network intrusion. HFS Financial helps individuals acquire loans for personal or home improvements. On August 30, 2016, HFS Financial's website was used to acquire 60 client's loan agreements, and email addresses. The subject, soccastar001@yahoo.com , IP 8.44.100.11, sent defamatory blogs to these clients causing a loss in sales for HFS Financial. HFS Financial estimates the loss at \$800,000.00.	1

OCC-16-2931-I	██████████	OCC-16-2931-I	On August 23, 2016, the Department of the Treasury Office of Inspector General (TOIG) Office of Investigations received a complaint from the Bank of Oak Ridge Vice President of Corporate Security in regards to theft of government funds. VP stated that their financial institution had an elderly client, who maintained a representative payee account with them, which was opened on August 29, 2014. VP stated that the representative payee for this account was the daughter, of the account holder. VP stated that both payee and representative payee/subject were given debit cards for this account, but after reviewing transactions made by the card in subject's possession, the funds appear to not being properly used by subject for the benefit of payee, which is the sole purpose of a representative payee account. VP stated that on several occasions payee has come into their branches inquiring about his balance and wondering if all of his money has already been spent. When subject's debit card access was removed, she used the starter checks for the account, made them payable to herself, and cashed them at her bank. As of November 2014, payee's account received \$119,753.63 in deposits and subject has withdrawn \$104,560.50. In August 2016, payee's account received \$4715.90 in deposits. Subject withdrew \$4700.00 in cash leaving a balance of \$18.84 in the account.	
OCC-16-2584-I	██████████	OCC-16-2584-I	Correspondence received via OIG Intake from OCC regarding allegations of the above named subject being arrested for a DUI.	1
BFS-16-2718-I	██████████		Correspondence received via OIG Intake with allegations of Social Security deceased payee benefit fraud by the above named subject.	
USM-16-2755-I	████████████████████	USM-16-2755-I	Correspondence received via OIG Intake from the USM regarding allegations of the above named subject having a warrant for his arrest.	2
OCC-16-2444-I	WELLS FARGO VENEZUELAN ACCOUNT TAKE-OVER		On 5/25/2016, TOIG and JSO met with Wells Fargo Bank regarding a string of related account-takeovers of high-value accounts belonging to Venezuelan Nationals between October 2015 - July 2016, resulting in the rapid withdrawal of funds via wire, cash withdrawals and transfers to new accounts opened in the names of the victims, but controlled by the suspects. Attempted loss is over \$945,000, but reversal of wires and transfers has limited the loss to \$405,358.19 thus far.	2
BFS-17-0819-I	██████████	BFS-17-0399-P	Correspondence received via OIG Intake from the BFS regarding allegations of the following: NIRT Case # 80811 Contractor performed unauthorized activity by moving Treasury information to an HP laptop. The individual reported the laptop stolen and when the individual was going to be interviewed by HP, they resigned.	1
-17-0846-I	██████████		SSA-OIG and the USAO-Southern District of Florida requested assistance in the interview of subject who continued to receive her mother's SSA annuity after her mother passed away. ██████████ subsequently confessed and the USAO asked TOIG to assist in serving ██████████ with a Target Letter prior to ██████████ being charged with 18 USC 641 (Theft of Government Funds).	
BFS-16-1042-I	██████████		Correspondence received via OIG Intake from the BFS regarding allegations of the above named calling into a BFS Call Center asking for the address to shoot up the government facility.	0
DO-16-2607-I	████████████████████		Correspondence received via OIG Intake from OC, with allegations of the above named subject being arrested for a DUI.	0

BFS-14-2853-I	██████████, ET AL.	The USSS reported the following and requested assistance with this investigation from TOIG and IRS-CI: The Bibb County, GA Sheriffs Office (BCSO) is investigating a subject, who is the central figure in a large scale Identity Theft operation / criminal organization. It is believed that the subject is additionally involved in the filing of false income tax returns. The BCSO has determined that the subject is additionally using stolen identities / fraudulently obtained credit cards to apply funds to assist local jail inmates in making bond.	1
CYBER-17-0856-I	██████████	The IG, FLRA, contacted TOIG requesting computer forensics on her assistant's work computer. IG stated that her IG share file was deleted on 7/27/2017 and that the last person in the files was her assistant. IG advised the assistant that the assistant would be RIF'd prior to the files being deleted. FLRA, IT, advised that this occurred on 7/27/2017 at approximately 6:30PM EST.	0
BEP-16-1869-I	████████████████████	Correspondence received via OIG Intake from the BEP regarding allegations of a verbal threat by the above named subject.	2
BFS-15-1696-I	██████████	Correspondence received via OIG Intake from BFS regarding allegations of the following: On May 8, 2015 the Compliance and Risk Management Staff (CRMS) was contacted by Comerica Bank who said they had identified several savings bonds they felt may have been altered and were being cashed by subject at several of their banks branches. He said it looked like the owners name and social security numbers were scratched out and then a new social security number and owners name were typed onto the bonds.	
DO-16-2111-I	██████████	The Broward County Florida Sheriff's Office requested assistance from TOIG to investigate a case where a group of Sovereign Citizens filed documents in the Broward Clerk's Office. The documents were filed in a foreclosure case against Bank of America. In the documents one of the subjects forged U.S. Treasury Secretary Jacob J. Lew's, signature on IRS Form 56 (Notice Concerning Fiduciary Relationship). The documents are being filed in support of a bankruptcy scheme to allow the subjects to "squat" in residence they rented in 2008 and have made very few payments on.	1
OCC-16-2272-I	████████████████████, ET AL.	On 5/12/2016, subject was identified as the manufacturer of counterfeit identifications for co-conspirators to obtain fraudulent lines of credit at financial institutions, including Synchrony Bank. Between February 15, 2016 and June 20, 2016, subject provided counterfeit identification documents to co-conspirators, who opened accounts in stolen identities. On Jun 2, 2016, an arrest warrant for the and a search warrant for the subject's residence was executed.	2
OCC-17-0836-I	██████████	Subject is a serial bigamist, who poses as a pastor and lures vulnerable women to his compound for sex trafficking or involuntary servitude. Subject has converted or taken over various social security benefits for children and adult victims and has schemed to defraud TD Bank.	0

OCC-14-0393-I	██████████ & ██████████	Office of the Comptroller of the Currency (OCC) reports that TCF National Bank has filed a Report with the Financial Crimes Enforcement Network regarding both a current OCC employee and a former OCC employee ██████████, both of whom have been the subjects of OI investigations in the past. The report was filed with respect to " . . . \$81,631.00 in Official Bank Check (OBC), Internal transfer, and cash activity, which reflects potential structuring to avoid federal Currency Transaction Report (CTR) requirements, potential money laundering, and concealment of funds."	
DO-13-1651-I	██████████	Correspondence received via OIG Intake from OC in reference to uncovered evidence regarding the above named subject.	2
BFS-16-0184-I	██████████ (SAVINGS BONDS) BFS-16-0184-I	Correspondence received via OIG Intake from OC regarding a request for agents in Indiana from an Attorney, Office of the Chief Counsel, Bureau of the Fiscal Service.	2
DO-16-1721-I	██████████ DO-16-1721-I	Correspondence received via OIG Intake from OIG Counsel regarding allegations of the following: Subject was responsible for housing finance while at Goldman prior to joining the USGov. While at Treasury, subject has worked on housing finance. subject is now meeting with former Treasury and other Administration officials regarding housing finance for his job at Goldman. The White House visitor log shows subject's attendance at several housing finance meetings after he left his Gov position.	14
BFS-16-2816-I	██████████ (SSA PAYMENT FRAUD) BFS-16-2816-I	Subject was allegedly smuggled into the United States and obtained passports and documentation under a fraudulent identity. Subject further obtained passport and immigration documents for his spouse and children based on his fraudulent immigration document and status. In 2002 subject applied for disability benefits from the Social Security Administration (SSA) office. Subject has been receiving Social Security Benefits through Treasury check payments since September 2005. To date he has received \$263,828 in benefits based on a disability claim he filed in 2002. According to the statements obtained by the State Department, subject was smuggled into the country and has lived under an alias and a false identity. According to information obtained from SSA-OIG, subject would not have been entitled to the benefits received based on his fraudulent identity.	2
BEP-15-1127-I	██████████	On March 6, 2015, TIGTA contacted TOIG regarding an ongoing investigation with USPS-OIG and DOL in connection to medical fraud totaling approximately \$8,000,000 committed by a doctor in Dallas, TX. The doctor allegedly submitted fraudulent claims in order for USPS and BEP employees in the Dallas area to receive worker's compensation. According to TIGTA and the USPS-OIG, a BEP employee was involved in the scheme to defraud the government.	30

OCC-16-2935-I	[REDACTED]	<p>The District of Columbia Department of Motor Vehicles (DCDMV) informed DSS Special Agent that they had encountered an individual who they believe was using two identities for driver's licenses. The two identities were discovered by DCDMV'S facial recognition software. SA informed the HSI Document and Benefit Fraud Task Force (DBFTF) of the possible fraud. The HSI DBFTF sent images of subject to the HSI Victim Identification Unit for expert comparison. Based on this information, HSI SA conducted various database searches on subject and his associates. The research indicates that subject has been associated with approximately eight Virginia based corporations. Subject has been the organizer and/or registered agent for most of these corporations. The formation of these corporations was accomplished electronically with the Virginia State Corporation Commission (SCC). No physical documentation, which would help indicate the true identities or addresses of organizers, registered agents or corporate officers, is retained by the SCC. The SCC indicates that the subject's mother is the organizer of America's Janitorial Services LLC. SunTrust Bank indicates that the subject and a female were the account holders of four bank accounts related to America's Janitorial Services. Female is believed to be subject's current girlfriend. Female is illegally present in the United States of America. SunTrust indicates that over \$140,000 was deposited in these accounts between May 2015 through February 2016. Most of the deposits were in cash. SunTrust closed these accounts. In February and March 2012, two credit card merchant accounts were created for the Stafford Diner. Elsy Food Corp. appears to have been doing business as (DBA) the Stafford Diner. Elsy Food Corp. appears to have been form in February 9, 2012. Mother is listed as the Registered Agent. Between May and July 2012, approximately 47 disputed or unusual transactions occurred.</p>
TTB-14-1528-I	[REDACTED] TTB-14-1528-I	<p>Correspondence received via OIG Intake from TTB regarding allegations of fraudulent documents on TTB letterhead</p>
CFIF-12-2713-I	[REDACTED], ET AL. (DBA [REDACTED]) CFIF-12-2713-I	<p>On 06/18/2012, TOIG received email correspondence from Assistant District Attorney, Queens County, NY, regarding case assistance related to numerous stolen U.S. Treasury checks. ADA requested certification of the checks and an in person meeting to discuss an investigative partnership. On 07/02/2012, TOIG met with ADA as well as the Chief, Airport Investigations Unit and the Deputy Bureau Chief, Organized Crime & Rackets Bureau. TOIG agreed to provided investigative support and future Grand Jury testimony regarding the Treasury checks.</p>
OCC-16-2114-I	BANK LIVING WILLS MEDIA LEAK OCC-16-2114-I	<p>In May 2016, the Federal Deposit Insurance Corporation contacted TOIG regarding a possible leak of sensitive information to the Wall Street Journal involving Bank "Living Wills" that lead to an article appearing in the Wall Street Journal prior to the information's official dissemination to the public. The information was only known to a limited number of individuals at the OCC, FDIC, and FRB.</p>
BFS-15-1290-I	[REDACTED], et al.	<p>Correspondence received via OIG Intake from the BFS regarding allegations of the following: The Compliance and Risk Management Staff (CRMS) has identified 255 counterfeit savings bonds that were submitted to various banks/paying agents for redemption. The counterfeit bonds were first identified when the payment of duplicate bond serial numbers attempted to post to our savings bond database against the legitimate original bond serial numbers which were shown as closed securities.</p>

SCAM-17-0177-I	[REDACTED], et al. (SCAM)	Correspondence received via OIG Intake from OIG Counsel regarding an incoming complaint from complainant with allegations of being scammed out of \$70,000.	
CFIF-12-2286-I	[REDACTED], ET AL. CFIF-12-2286-I	Special Agent United States Secret Service, Atlanta Field Office, contacted TOIG on or about April 19, 2012 regarding a fraudulent tax fraud scheme. Specifically, SA believes multiple subjects are researching defunct transportation businesses in Florida, re-incorporating them in Georgia, and then receiving fraudulent tax refunds for fuel tax credits.	1
BFS-16-2736-I	[REDACTED]	On August 22, 2016, The U.S. Postal Service, Office of the Inspector General contacted TOIG for assistance in the following: The U.S. Postal Service Office of Inspector General (USPS-OIG) received a complaint from a customer, Alexandria, VA. Victim advised a U.S. Treasury check, which had been mailed to her was not received by her, but was deposited into a Navy Federal Bank account on June 27, 2016. On August 22, 2016, USPS-OIG Special Agent contacted victim and she emailed SA an image of the stolen U.S. Treasury check. The U.S. Treasury check was in the amount of \$1939.00 and the payee was the victim. SA contacted postmaster, Alexandria Main Post Office, Alexandria, VA, and requested to know who the carrier was for the address for June 20, 2016 - June 27, 2016. Postmaster provided information, which identified subject postal employee, as the carrier who carried this route on June 22, 2016, June 23, 2016, and June 27, 2016. Further investigation is required in order to determine if a Postal Service employee violated Postal Service policy, federal criminal law, or Commonwealth of Virginia criminal law. TOIG contacted NFCU Investigator who said that approx. 10 US Treasury checks made payable to somebody other than the subject Postal employee have been deposited into his NFCU acct.	1
OIG-17-0071-I	[REDACTED] AND [REDACTED]	Investigators from Escambia Sheriffs Office received information regarding a missing persons case in their jurisdiction. Victim has been estranged/missing since 2004 which is the last time family has spoken to him. Victims sister claims that the subjects confessed to her that they killed the victim and burned his body in their backyard fire pit because of an alleged sexual assault of their child by the victim. Upon further investigation it was determined that the subjects had been writing themselves checks the first of every month in the exact amount of the SSI benefits received by the victim and depositing them in their personal account. Total amount of theft is approximately \$45,000. Escambia County SO request our assistance in the fraud portion of the investigation in hopes that through interviews more information can be gathered regarding the homicide/missing person.	2
DO-12-2147-I	SUNGEVITY (ARRA)	The complaint alleges Sungevity might be inflating costs based upon related-party pricing, 1603 ARRA.	2
BFS-16-0227-I	FLORIDA EAST COAST TRAVEL SERVICES, INC.	Correspondence received via OIG Intake from the BFS regarding allegations of the following: One of the mailroom workers reached out to me and informed me that there were multiple checks returned to us from the Palmetto Lakes Post Office in Hialeah, FL. The Post office box is registered to Florida East Coast Travel Services, Inc and the checks are tax refunds to a variety of people.	2

BFS-15-2074-I	██████████		Complaint received 7/28/2015, via email Complainant alleges subject deposited an altered US Treasury Check in the amount of \$4,688.6. The check was originally issued in the amount of \$688.81. Subject has forged non-government check and owns the Ohio Educational Credit Union over \$5000.00	0
BEP-14-1554-I	██████████	BEP-14-1554-I	Complaint received 5/22/2014, via email from BEP Human Resources Specialist at the Bureau of Engraving and Printing Fort Worth, Texas reporting workers compensation fraud and abuse. BEP alleges - We are being over charged for former employee's care at the Grand Court Tampa senior Living Center. Subject receives payment of \$5284 every 28 days at 75% augmented compensation for living expenses at the Grand Court Tampa Senior Living Center. The Afford ability calculator from the Grand Curt Tampa web site show living expenses start at \$2405 per month or \$80.00 per day. We are being charged for over \$200 per day for care that is available for \$80.00. BEP also points out that the subject's wife may be occupying the room which being up concerns of subject needing assist with caring for himself.	
USM-16-0320-I	██████████	USM-16-0320-I	Correspondence received via OIG Intake from the USM regarding allegations of officer misconduct by the above named subject.	3
BFS-16-1199-I	██████████	BFS-16-1199-I	Correspondence received via OIG Intake from the BFS regarding allegations of payments belonging to payee being deposited into someone else's account.	2
OCC-16-0523-I	██████████	OCC-16-0523-I	Correspondence received via OIG Intake from the OCC regarding allegations of the above named subject for violation of the standards of conduct-seeking other employment	3
BEP-16-0101-I	INAPPROPRIATE SEARCH OF BEP EMPLOYEES	BEP-16-0101-I	Complaint received 10/15/2015, via email ***COMPLAINANT REQUEST CONFIDENTIALITY*** NTEU alleges BEP has started strip searching its employees, two strip searches happened within the past several months. NTEU reports these searches humiliated the employees, the employee were forced to remove their clothes in the company of their peers. Consequently, the NexGen notes were found in the BPS machine located in the single note inspection cage#3 on Sept. 2015. However the agency claimed to have dismantled the BPS machine prior to initiating the strip search on May 2015. Additionally NTEU reporting BEP participating in pre-selection hiring and has led to several prohibited personnel practice violations. Reference	0

DO-17-0376-I	OFR VANDALISM		On December 19, 2016, TOIG Counsel was notified of a vandalism incident at Treasury Departmental Offices - Office of Financial Research (OFR). OFR Counsel related that there were drawings on some of the windows when he entered the building Monday morning. Phallic drawings were found on several of the OFR Director, office windows. OFR Director's office is on the 6 th floor. The same drawing was found, along with the words "You are a" on the door of OFR Deputy Director. Deputy Director's office is on the 12 th floor. The words "Get Fired" were found on the door of Data Center Acting Associate Director. Associate Director's office is on the 11 th floor. Deputy Director stated he was in the office on Friday until approximately 7pm and the drawings were not there when he left. Deputy Director was notified at approximately 7:30 am on Monday that his office had been defaced. TOIG agents spoke to Director, Deputy Director and OFR Counsel regarding the events mentioned above. They confirmed the information previously stated and provided information pertaining to the atmospherics and overall climate of the OFR.	
USM-16-2613-I	██████████	USM-16-2613-I	Correspondence received via OIG Intake from the USM regarding allegations of the above named subject assaulting another employee.	3
USM-15-1619-I	██████████	USM-15-1619-I	The US Mint explicitly requests that the TOIG investigate the allegation that US Mint employee appears improperly to have validated her time and attendance records on multiple occasions, crediting herself with working time that she did not actually work.	
DO-16-2387-I	██████████	DO-16-2387-I	Complaint received 7/20/2016, via email IT specialist Departmental Office, volunteered to coordinate a water club for OCIO staff and contractors and to facilitate deliver of water jugs and payment. Participants volunteered to provide payments in return for access to water jugs on their floor. As of today \$1,100.20 of funds collected have not been applied to drinkmore invoices.	3
BFS-14-1581-I	TSP FERS / STOLEN US TREASURY CHECK	BFS-14-1581-I	Complaint received 5/22/2014, via email Complainant alleges requested funds of \$18,800.00 from TSP FERS retirement account. A TSP Representative stated the funds would be mailed out and the complainant would received the funds within 15 business days. After a waiting period of time the complainant called TSP to inquire on the status of the check and was told by TSP representative the check had been cashed and the complainant would receive forms to verify her hand writing along with a copy of the check.	2
USM-15-2113-I	██████████	USM-15-2113-I	Correspondence received via OIG Intake from the USM regarding allegations of time card fraud by the above named subject.	0
FMS-12-2357-I	██████████		On July 30, 2012, TOIG Special Agent received an allegation from Special Agent, Social Security Administration (SSA), that in May 2012 approximately 300 SSA recipients, in the Pinellas County, FL area, had not received their monthly benefit checks. SSA discovered that the checks were cashed at small businesses in Tallahassee FL, Live Oak, FL, Tampa, FL and South Georgia.	1
OCC-17-0213-I	██████████	OCC-17-0213-I	Correspondence received via OIG Intake from the OCC regarding allegations of the above named subject abusing his position.	
USM-16-2350-I	██████████	USM-16-2350-I	Correspondence received via OIG Intake from the USM regarding allegations of the above named subjects assaulting another employee.	1

OCC-16-1417-I	██████████	OCC-16-1417-I	Correspondence received via OIG Intake from the OCC regarding allegations of the above named subject soliciting sexual acts from an online sight called "Backpage"	2
OCC-16-2547-I	██████████	OCC-16-2547-I	Correspondence received via OIG Intake from the OCC regarding allegations of the above named subject being arrested for leaving a minor child in the car unattended.	3
USM-17-0826-I	██████████ (SENIOR STAFF MISCONDUCT)		Complaint received 3/3/2017, via email *** COMPLAINANT REQUEST CONFIDENTIALITY*** Complainant alleges ██████████ for the US Mint in CA , is newly promoted to ██████████ position and currently has surrounded himself with preselected individuals, ██████████ has failed to supervise his employees properly, allowing a SGT under his command to avoid his duties and leave early, ██████████ leaves anytime he wants and other supervisors are forced to cover for him. The complainant states the incident has been reported by other supervisors but nothing has been done.	0
BFS-15-0989-I	██████████		The Bureau of the Fiscal Service (BFS) reports that private citizen submitted to Morgan Stanley Wealth Management a number of fraudulent documents, purporting to draw on funds with the US Treasury, for redemption; Morgan-Stanley contacted the BFS and was informed that the documents are worthless. Note that subject appears for similar fraud attempts in our records.	1
DO-16-0975-I	THEFT OF GOVERNMENT PROPERTY		Deputy Secretary reported loss of Treasury Issued iPad on 2/6/2016, along with personal Apple Laptop (this was the 2nd incident) from their residence. There was another loss, (unreported) of initial Treasury issued iPad and personal Apple Laptop on 10/2/2015. CODE MCPD Incident Report - 16006356 dated 2/9/2016, Detective, Criminal Investigations, Takoma Park Police	1
OCC-16-2344-I	██████████	OCC-16-2344-I	Correspondence received via OIG Intake from the OCC regarding allegations of unauthorized disclosure of sensitive bank information.	1
OCC-16-2596-I	██████████████████████	OCC-16-2596-I	Correspondence received via OIG Intake from the OCC regarding allegations of unauthorized disclosure of sensitive bank information.	1
DO-17-0837-I	██████████		Correspondence received via OIG Intake regarding allegations of the above named subject making a threat to another government employee.	2
OCC-16-2567-I	██████████		Correspondence received via OIG Intake from the OCC regarding allegations of an arrest of the above named subject.	2

OCC-18-0011-I	U. S. Bank - CAG # 03096983	<p>From OCC whistleblower complaints April 2017: The complainant, an employee of U.S. Bank, (Requested to Remain Anonymous) stated he submitted a whistleblower tip through the CFTC website. Both the CFTC and SEC referred him to submit a tip under FIRREA through OCC. The complainant alleges U.S. Bank policies and procedures related to foreign exchange transactions pose risk to deposit holders. He states the Foreign Exchange Credit Policy does not properly identify or measure market risks associated with current movement. Credit is underwritten for a value considered the "marginal credit exposure to the bank. This MCE is built upon poor market risk measurement of foreign exchange movement and the resulting credit exposure approved by Credit is vague, with system compliance gaps that create opportunity for Sales to trade with clients on exposures dramatically different than what was intended as part of the credit approval process. Furthermore, US Bank does not reserve capital for foreign exchange exposures nor prevent sales from taking excessive market risk related to market and credit risk policy failures. In addition, he states the combination of the above mentioned creates risks to the bank that can be greater than intended, and any potential adverse movement in the market can put risk to client deposits.</p>	2	
BFS-16-0937-I	██████████	<p>Correspondence received via OIG Intake from the BFS regarding allegations of the following: The check was originally issued to an Estate for \$250 and going to Bogota, Colombia. It was altered to \$143,600 and made to ██████████ Law Firm in Maumee, OH. ██████████ Law Firm, LPA is located at the same address that the check was altered to. The BOFD is Key Bank (in OH). I spoke with Key Bank, verified that the account number written on the back of the check does in fact belong to ██████████ Law Firm and the account signer is ██████████.</p>	2	
OCC-16-2551-I	██████████	OCC-16-2551-I	<p>Correspondence received via OIG Intake from the OCC regarding allegations of violations of federal ethics regulations concerning impartiality in the performance of official duties and misuse of a government position.</p>	3
DO-16-0610-I	██████████████████	<p>Correspondence received via OIG Intake from the Department of the Treasury regarding allegations of suspected fraud. Deceased victim was receiving benefits from the DC Police Officers and Firefighters Retirement Plan, passed away April 2015 however her benefits were still being cashed from April 2015 to September. Six payments totaling \$13, 752.00.</p>	3	

OCC-17-0828-I	██████████		In March 2017, Assistant United States Attorney (AUSA) referred this case to TOIG and the NC-TFCTF for investigation. The suspect was on supervised release for access device fraud at the time of this incident which occurred in Raleigh, North Carolina. AUSA advised he was going to file a motion with the court to violate subject's supervised release and requested TOIG to investigate the new incident in Raleigh and present its findings to the United States Attorney's Office for the Eastern District of North Carolina. TOIG reviewed the information provided by AUSA and determined the following: On September 25, 2016 the Raleigh Police Department (RPD) arrested the subject for credit card fraud after answering a call for service at the Belk Department Store located at 7500 Old Wake Forest Road. RPD performed a traffic stop on the vehicle being operated by the subject as it attempted to lave the parking lot of the business. Subject threw his wallet out of the car window during the traffic stop and it was recovered by RPD. RPD discovered 11 encoded credit cards with different name embossed on them and a fraudulent South Carolina Drivers License in the name with the subject's photograph. RPD also located numerous items purchased from different merchants and the receipts associated with those purchases. RPD was able to match up the encoded credit cards with the receipts and returned the fraudulently purchased merchandise to the proper vendor. A BIN Search of the encoded numbers revealed all of the numbers belonged to First Citizens Bank located in Raleigh, North Carolina. Subject is currently in the custody of the Federal Bureau of Prisons after having his supervised release conditions revoked.	0
BFS-17-0031-I	██████████	BFS-17-0031-I	Complaint received 10/5/2016 Complaint referral from the BFS regarding an employee performing autoeroticism while in the facility restroom during an administrative investigation by Workforce Relations Branch the employee admitted to the activity as three times over the last 6 months	0
OCC-17-0821-I	██████████	OCC-17-0304-P	Correspondence received via OIG Intake from the OCC regarding allegations of the above named subject's OCC issued equipment being stolen.	1
BFS-15-0124-I	██████████	BFS-15-0124-I	Subject appears to be obtaining and altering Treasury checks and cashing them at Wal-Marts in the Chicago, Illinois, region. Losses to date are approximately \$40,000. NOTE the potential relationship among this intake and Intake Number 15-0157 (also Chicago) and 15-0156	0