Description of document:	List of Department of the Treasury Inspector General (OIG) Investigations closed CY 2018 - CY 2019
Requested date:	24-February-2020
Release date:	16-March-2020
Posted date:	25-May-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

From: Delmar, Richard K. <DelmarR@oig.treas.gov>
Sent: Mon, Mar 16, 2020 6:05 pm
Subject: FOIA - Treasury OIG - closed investigations CY18-19

Responding to your FOIA 2020-03-060 for list of Treasury OIG investigations closed in CY 2018-2019. List attached, with Exemption 7C redactions.

The redactions constitute a partial denial of your request, and thus 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
(202) 741-5770
(877) 684-6448

Rich Delmar
Deputy Inspector General
Department of the Treasury

Number	Title	Complaint Summary	Date Initiated	Date Closed	Current Status
ZZZ-17-0825-I		The New York State, Office of the Attorney General (NYAG) requested the assistance of the Department of Treasury, Office of the Inspector General (TOIG) for investigative research and testimonial support in a criminal investigation. The NYAG investigation uncovered several documents that they believed to be fraudulent Treasury Documents as well as email communications that are believed to be spoofed in order to appear as originating from department servers.	09May2017	15Mar2019	Closed; ROI - Not Forwarded to Bureau
ZZZ-17-0285-I		On November 29, 2016, TOIG proactively requested to assist the Texas Department of Public Safety in Houston, TX, on an identity theft, fraudulent access device, theft, money laundering, and organized criminal activity involving a large group of subjects of Cuban descent. The subjects utilize gas pump skimming devices to fraudulently obtain stolen credit card information and create counterfeit credit cards which are dispersed to several known conspirators to purchase diesel, merchandise, and mechanic tools. At this point in the criminal investigation, the primary subject in the case is known as [redacted] is allegedly responsible for installing the credit card skimmers, obtaining the stolen credit card numbers, manufacturing the new credit cards with the stolen information, dissemination of the stolen cards to make purchases with the profit being split between the Cuban recipients and G[redacted] o. The investigation is in its preliminary phase with the benefit of a cooperating "Confidential Informant".	01Dec2016	14Aug2019	Closed; ROI - Not Forwarded to Bureau
USM-19-0031-P	Sr Mint Official - Retaliation	Complainant states that a senior Mint official is in violation of retaliation in an effort to get her to drop her EEOC complaint. The official is not identified.	07Jun2019	08Oct2019	Closed; Preliminary Inquiry Closure
USM-19-0006-P	Prohibited Personnel Practices US Mint	Complaint received 11/15/2018, via OIG Intake Complaint received OIG Intake regarding allegations of Prohibited Personnel Practices, Vacancy Pre-Selection, sent to the US Mint and New York Times.	21Nov2018	19Feb2019	Closed; Preliminary Inquiry Closure
USM-18-0080-P	Counterfeit Presidential Coins	Complaint received 8/20/2018, via OIG Intake Complaint received OIG Intake regarding six suspected counterfeit Presidential $1.00 Coins, turned over from Granters Pawn Shop in Vallejo CA suspected to be counterfeit.	13Sep2018	28Mar2019	Closed; Preliminary Inquiry Closure

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

USM-19-0048-I	Complaint received 5/6/2019, via OIG Intake Complaint received OIG Intake regarding an incident of an Error/Uncirculated coins found inside of Post #5. Officer [redacted] stated that he discovered a small yellow envelope inside the ASP/Post #5. The envelope had the name [redacted] written on it. The envelope contain an undermined amount of coins however three coins were from The War In The Pacific- Guam 2019 series. The coins are not released for circulation until approximately June 3, 2019. At the base of one coin the word Dollar is missing.	07May2019	27Aug2019	Closed; ROI - Response Received
USM-19-0035-I	Complaint received 2/25/2019, via OIG Intake Compliant received OIG Intake regarding allegations of misconduct by [redacted] a US Mint Contractor, potential procurement irregularities, engaging an individual for support services without authorization and issuing payment via check without the necessary approvals, misuse of a tax identification number. Inappropriate sexual conduct, implying to others he had the authority to make an offer of employment.	06Mar2019	19Sep2019	Closed; ROI - Response Received
USM-19-0034-I	Complaint received 12/19/2018, via OIG Intake IG Referral of United States Mint Police 18-HQ-008 Related Case: USM-18-2276-C Complaint received OIG Intake concerning allegations of misconduct by Lieutenant [redacted]. A Management Inquiry determined by management of the U.S. Mint, PA, that a conflict of interest between position of Police Lieutenant and Secretary of the Lodge, 01F.	06Mar2019	27Aug2019	Closed; ROI - Response Received
USM-18-0107-I	Complaint received 5/18/2018, via OIG Intake US Mint Police Report 18-PH-919 Complaint received OIG Intake regarding Sergeant [redacted] US Mint Mission Leader, purported acts of misconduct reported by Police Officers [redacted]r and [redacted]. Sergeant [redacted]s failed to follow uniform and equipment policy, mislead airport officials, used vulgar language/inappropriate racial comments, and excessive reckless driving while on official government.	16Aug2018	18Sep2019	Closed; ROI - Response Received
USM-18-0079-I	Complaint received 5/7/2018, via OIG Intake US Mint Incident Report Number: 18-PH-905 Complaint received OIG intake from [redacted] Division Director/Commander US Mint Headquarter, regarding Sergeant [redacted] an employee of the US Mint who made unauthorized purchase of $6,240.00, for various Snap-on tools and a rolling chest drawer cabinet, tools to repair police firearms and other equipment. Several days later Sergeant [redacted] was observed on video footage exiting the US Mint what appeared to be a tools inside his back pack in addition to his duty issued weapon.	01Jun2018	27Aug2019	Closed; ROI - Response Received
USM-18-0048-I	Correspondence received via OIG Intake from [redacted] with the USM regarding allegations of error coins being illegally removed and sold from the United States Mint at Philadelphia, PA 18-HQ-001	12Feb2018	10Jun2019	Closed; Memo to File

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

USM-16-2948-I		USMint requested further investigation beyond findings of USM-15-1070-I and provided 14 issues to address and investigate.	29Sep2016	23May2019	Closed; ROI - Response Received
USM-16-0790-I	US DIME STRUCK ON NAIL	Correspondence received via OIG Intake from [redacted] with the USM regarding an article in Coin News detailing the sale of a dime image struck on a nail. 16-HQ-001	04Feb2016	03Dec2019	Closed; ROI - Referral to Bureau for Info Only
USM-16-0041-I		Correspondence received via OIG intake from [redacted] with the USM regarding allegations of unauthorized commitment of funds by [redacted].	05Oct2015	27Jun2019	Closed; ROI - Referral to Bureau for Info Only
USM-12-2285-I		On July 25, 2012, the U.S. Department of the Treasury (Treasury), Office of Inspector General (TOIG), Office of Investigations (OI), developed information from the United States Mint (USM), indicating a fraudulent order was placed with the USM for eight (8) American Buffalo 1oz Gold Proof coins, amounting to $14,884.95.	26Jul2012	16Jul2019	Closed; ROI - Referral to Bureau for Info Only
TIGTA-17-0867-I		On November 29, 2016, TOIG was asked by TIGTA, Dallas, TX, to assist with a criminal investigation involving stolen altered US Treasury checks from Chicago, IL, that were being fraudulently negotiated in the greater Dallas area. Upon initial review, it was determined this case may be related to TIG case #16-2793. Further review showed it was not related to that case.	29Aug2017	17Apr2019	Closed; Memo to File
TFA-18-0090-I		On March 22, 2018, the Department of the Treasury Office of Inspector General (TIG) Office of Criminal Investigations received a complaint from the United States Attorney's Office (USAO) for the Middle District of North Carolina in regards to a wire fraud case. Attorney [redacted] used the financial services of [redacted]., a credit card processing company and OCC regulated organization, to successfully process approximately $251,488.07 in transactions. Of those transactions, 41 totaling $76,933.67 were received as charge-backs for fraud from the credit card issuers. As a result, [redacted]. sustained an estimated loss of $59,036.31.	02Jul2018	26Jun2019	Closed; Memo to File

TFA-18-0078-I	On May 26, 2017, Durham Police Department (DPD) arrested [redacted] for violation of NC Statute 14-120, Uttering Forged Instruments and 14-87.1, Common Law Robbery. [redacted] feloniously did steal, take and carry away United States Currency (USD) in the amount of $300 by force from elderly victim [redacted]) and did cause a forged check in the name of victim [redacted]) to be passed to Bank of America (BOA) as a true financial instrument. The fraud impact has been identified by DPD having a potential fraud loss of $300 and shows that [redacted] having an extensive criminal history in the Durham area for similar violent crimes. On March 26, 2018, this case was referred to the United States Treasury Department, Office of Inspector General, Office of Investigations (TIG) North Carolina Financial Crimes Task Force (NCFCTF) from the United States Attorney's Office Middle District of North Carolina (USAO-MDNC) as a request for investigative assistance.	30May2018	08Aug2019	Closed; ROI - Not Forwarded to Bureau
TFA-18-0051-I	On May 05, 2017, the Winston Salem Police Department (WSPD) arrested [redacted]) for Conspiracy to Commit Felony Larceny and Identity Theft. WSPD identified three suspects, [redacted], [redacted], and [redacted] who were operating a scheme in which they used stolen identities to open cell phone accounts via wire and order phones. The phones were then shipped via UPS where [redacted]n and [redacted] were employed. [redacted] and [redacted]s would remove cell phone packages from their UPS truck and would transfer the packages to [redacted] who would sell them on the "black market". [redacted] and [redacted]s have given confessions to the WSPD in this matter. [redacted] and [redacted]hn have plead guilty in Forsyth County Superior Court to Misdemeanor Conspiracy to Commit Larceny and will be considered a witness in this matter. There are 18 victims of Aggravated Identity Theft which were identified by WSPD having a potential fraud loss over $94,664 with and actual loss of $91,408. On February 02, 2018, this case was referred to the North Carolina Financial Crimes Task Force (NCFCTF) from the United States Attorney's Office Middle District of North Carolina (USAO-MDNC) as a request for investigative assistance.	14Feb2018	13Aug2019	Closed; ROI - Not Forwarded to Bureau

TFA-18-0014-I	FBI Safe Streets Task Force was approached by a source that provided information reference to a fraud group that was operating in Durham, North Carolina. The FBI referred this case to the Financial Crimes Task Force - North Carolina. TOIG met with the Source who provided the following information: [redacted] who is on federal probation ran a group that would steal money from financial institutions through fraud. [redacted] has run the scam since he graduated high school and only stopped the scam while in federal prison for a conviction in the Western District of North Carolina. [redacted] started again after being released from prison and while still on federal supervised release. [redacted] found vulnerable victims by asking them if they needed money. [redacted] typically targeted female victims on the dating website Plenty of Fish and other social media sights. [redacted] and [redacted] sister obtained account information of their victims, especially if the victim held bank accounts at Bank of America National Association (BANA) and North Carolina State Employees Credit Union (SECU). [redacted] and [redacted] would convince the victims to provide their bank cards and account log-in information. [redacted] needed two different victims for his scheme to succeed. [redacted] needed one victim with a SECU account. [redacted] would obtain the online ID, password, debit card, and pin of the victim. This account would eventually be used to deposit counterfeit (CFT) checks into it and with draw the funds that posted before the bank detected the CFT checks. The second victim was needed so [redacted] could order checks using the victims account. [redacted] preferred Bank of America and Wells Fargo Customers when ordering the checks. [redacted] would obtain the victims account number, online ID, and password. [redacted] would then order a book of checks using the victims account. [redacted] would change the Payor section of the check from the victim's information to a legitimate company's information. [redacted] would have the	19Oct2017	27Sep2019	Closed; ROI - Not Forwarded to Bureau

TFA-17-0859-I	On August 7, 2017, the Department of the Treasury Office of Inspector General (TOIG) Office of Criminal Investigations received a complaint from the United States Attorney's Office (USAO) for the Middle District of North Carolina (MDNC) in regards to an embezzlement and identity theft case. The USAO MDNC received this case via the United States Secret Service [redacted] Resident Office. [redacted] is currently the Director of Financial Management at High Point Regional Hospital (HPRH), now under UNC Healthcare. [redacted] has been employed with HPRH since June 5, 1995. [redacted]), HPRH's Chief Financial Officer (CFO), contacted the High Point Police Department (HPPD) after receiving several anonymous tips stating that [redacted] has been embezzling money from the hospital. [redacted] indicated that [redacted] has been taking money from HPRH's main account. This is the account that receives insurance payments and other payment for services rendered. [redacted] further indicated that he has pulled HPRH Bank of North Carolina financial statements, for the account [redacted] has reportedly embezzled funds, going back five years. [redacted]t is attempting to reconcile checks that he has come across, for this time frame, made out to [redacted] and [redacted] husband, [redacted] cash and an unfamiliar LLC totaling approximately $300,000. [redacted]t has further indicated that [redacted] is not authorized to sign these checks, but has been forging the signature of the authorized signor. [redacted] has numerous examples of legitimate signatures and the forged signatures.	08Aug2017	08Aug2019	Closed; ROI - Not Forwarded to Bureau

TFA-17-0839-I		On January 31, 2017, the Asheboro Police Department (APD) conducted a search warrant at [redacted], Asheboro, North Carolina in conjunction with a counterfeit (cft)/fraudulent credit card investigation. During the search APD located over 100 cft and reencoded credit cards, a card reader device, two computers, and an embossing machine. APD identified both [redacted] and [redacted] as suspects in the cft credit card investigation based off of evidence seized during the search warrant. In February 2017 , APD contacted TOIG and requested assistance with this investigation. Continuing in February 2017, TOIG entered each cft credit card seized during the search warrant through a magnetic card reader and determined they were encoded with credit card numbers from numerous different financial institutions from around the United States. Finally in February 2017, TOIG conducted several database checks and determined [redacted] was a suspect in numerous cft credit card cases in North Carolina. TOIG located case reports from the Raleigh Police Department (2 cases) and Durham Police Department (1 case) in which [redacted] was either a suspect or a defendant (state) in cft credit card cases.	03Jul2017	29Mar2019	Closed; ROI - Not Forwarded to Bureau
SCAM-20-0009-P	SCAM	Complaint received on 11/4/19 via duty agent.	07Nov2019	05Dec2019	Closed; Preliminary Inquiry Closure
SCAM-19-0016-P		Complaint received 2/13/2019, via OIG Intake [redacted] assistant prosecuting attorney in Jefferson County Missouri, requests assistance in a forgery case set for a jury trial wherein a defendant presented a fraudulent U.S. Treasury Check, to pay his county taxes and due to the official looking nature of the check, [redacted] would like someone from the U.S. Treasury to explain that the document presented by the sovereign citizen, is in fact fraudulent. [redacted] request the help of [redacted] or someone else with knowledge and experience in the areas of sovereign citizens.	22Feb2019	29Apr2019	Closed; Preliminary Inquiry Closure

SCAM-19-0010-P	SCAM	Complaint received on 12/11/2018 via hotline telephone Complainant, [redacted], stated that she was in the process of selling her timeshare with [redacted] Resorts in Florida. [redacted] was contacted by a realty company, D[redacted] Realty, located in Texas regarding the sell of her timeshare. [redacted] began working with an alleged realty agent by the name of [redacted]. Allegedly [redacted] would be selling her timeshare to a man named [redacted] located in Nicaragua. [redacted] was told by the subject realty agent that all she had to do was pay the transfer taxes for the property by wiring money to Nicaragua. After wiring $3,750 to a person named [redacted] z at a bank entitled Banco Lafise Bancentro in Nicaragua, [redacted] was contacted by two alleged Special Agents stating they were from the Dept. of the Treasury, Stephen Robey and Michael Rocca. [redacted] was then told by alleged SA Robey that the realty company she was working with was being fined $250k for tax purposes in "dropping the ball on the sale". The subject then told [redacted] that she would be entitled to 40% of that money with the additional money received from the sale of her time share. She was then sent a form titled "FinCEN form 105" where she was instructed to fill it out and return it to SA Michael Rocca. Both subjects told the complainant that she would only have to pay 15% of the sell and she would be given a government grant to assist with those costs. [redacted]. [redacted] began to worry that this was a scam when she continued to ask both subjects for email addresses and they refused to provide them to her. Bank Info: Bano Lafise Bancentro Carretera Masaya KM 5.5 Managua, Nicaragua Beneficiary: [redacted] Acct #: [redacted]8 SUBJECT(s): [redacted] ; [redacted].com) [redacted] [redacted]) [redacted] [redacted] 2) [redacted] [redacted] Managua, Nicaragua)	12Dec2018	03Jun2019	Closed; Preliminary Inquiry Closure
SCAM-18-0078-P		Complaint received 8/22/2018, via OIG Inquiries [redacted] paid [redacted] from approximately 2007- 2010 , and several companies a total of $15,000.00 to sell or rent his timeshare. [redacted] contacted the Attorney General in FL several times to try to recoup some of his funds after finding out realizing these companies were fraudulent.	24Aug2018	17Oct2019	Closed; Preliminary Inquiry Closure

SCAM-16-2152-I	On May 6, 2016, TOIG was contacted by the Guilford County Sheriff's Office (GCSO) in regards to a scam that involved an elderly victim of Guilford County, North Carolina. This scam was the well known lottery scam in which the suspect contacts the elderly victim and notifies them that they have won a type of lottery and a new high end vehicle. On May 2, 2016, the suspect, now known to be[redacted]), contacted the victim by phone and told him that he had won the lottery in the amount of $5.5 million dollars and a 2016 BMW. However[redacted] told the victim that he needed to wire $600 dollars for customs and processing fees to receive his prize. Over the course of the next several weeks, the victim wired[redacted] funds and made direct deposits into account number[redacted] with an associated routing number of [redacted]. By the time family members learned of these financial transactions, the victim had sent close to $32,000 to[redacted]. The above account number has been identified as a Branch Banking and Trust (BB&T) bank account in the name of[redacted].	24Jun2016	02Jul2019	Closed; ROI - Not Forwarded to Bureau

SCAM-15-0905-I	On January 30, 2015 Assistant United States Attorney [redacted] contacted SA [redacted] and requested TOIG assistance with a case involving bank fraud, wire fraud, and fraudulent identities. AUSA [redacted] stated he had been contacted by SunTrust Bank Corporate Security [redacted] who advised they had uncovered a scam in which legitimate bank wires had been redirected to fraudulent corporation accounts which had been opened at SunTrust Bank. Continuing on this date, SA [redacted] t contacted SunTrust Corporate Investigator [redacted] who advised after the deposits were received in the fraudulent accounts they were withdrawn by individuals using counterfeit identification documents. A review of SunTrust video surveillance show at least four different people with numerous identifications making multiple withdrawals of funds from the fraudulent accounts [redacted] advised he had been contacted by numerous financial institutions in regards to this scam. Financial Institutions with who have been victimized by this scam include Bank of America and PNC Bank, both are regulated by the OCC. The loss in this case is estimated to be in access of 1.3 million. Containing on this date, [redacted], was taken into custody in Georgia attempting to make a withdrawal from a fraudulent account. On Febraury, 2, 2015, a second suspect in this case was identified by facial recognition software as [redacted]. Both suspects identified in this case live in Winston-Salem, NC. Also on this date, First Citizens Bank Corporate Security forwarded SA [redacted] t a copy of Treasury ACH transactions in numerous individuals names that were deposited into a fraudulent account related to the suspects in this investigation.	04Feb2015	15Mar2019	Closed; ROI - Not Forwarded to Bureau
SCAM-15-0796-I	On January 22, 2015 Assistant United States Attorney [redacted], Middle District of North Carolina (MDNC) contacted SA [redacted] and requested an investigation into a counterfeit check that was passed in [redacted] North Carolina in December 2013. The check was drawn on the account of [redacted], Inc's PNC Bank Account (OCC regulated bank) in the amount of $26,394.06 and was deposited into the account of [redacted] at Suntrust Bank. The check was returned to Suntrust Bank in March of 2014 after it was determined the check had been altered and was originally issued to "Cogent Power". From December 27, 2013 through December 29, 2013, [redacted] n withdrew all the money from the Suntrust Bank account be making numerous over the counter withdraws, ATM withdrawals, and purchasing official checks.	23Jan2015	29Mar2019	Closed; ROI - Not Forwarded to Bureau

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

OIG-19-0030-P		Complaint received 5/20/2019, via OIG Intake Complaint received OIG Intake regarding a referral that identifies information concerning an executive official with the U.S. Ability One Commission. The information relates to extensive and ongoing, possible structuring bank activity by the executive official and the spouse, and dates back several years.	28May2019	19Nov2019	Closed; Preliminary Inquiry Closure
OIG-19-0002-P		Complaint received on 10/17/2018 via online complaint form The Washington Metropolitan Area Transit Authority (WMATA) OIG-OI was notified in March 2018, of suspicious payroll deduction activity by numerous WMATA employees. WMATA employee Ozoemena Onuigbo has possible shell company, Illegal money service business (MSB) for money laundering scheme, structuring and loan fraud. WMATA OIG is requesting Treasury OIG assistance on the investigation as the violations appear to fall within TIG 's jurisdiction. [redacted] SSA, WMATA OIG. SUBJECT: Ozoemena Onuigbo	23Oct2018	10Jun2019	Closed; Preliminary Inquiry Closure
OIG-19-0009-I	Middle District of North Carolina – Treasury Financial Crimes Task Force - FY 2019	MIDDLE DISTRICT OF NORTH CAROLINA - TREASURY FINANCIAL CRIMES TASK FORCE - FY 2019 - The USAO in the Middle District of North Carolina requested that TOIG initiate and lead a Treasury Financial Crimes Task Force in North Carolina. TOIG initiated the TF on October 1, 2015 to focus on improper payment fraud, MSB fraud, Treasury employee impersonation fraud and other Treasury related financial crimes that fall within the jurisdiction of TOIG. Five local police departments including the Guilford County Sheriff's Office, the Durham Police Department, the North Carolina DMV License and Theft Division, the North Carolina Department of Insurance and the [redacted] Police Department agreed to participate in the task force. IRS-CI also agreed to continue to participate in the TF and lead the SAR review portion of the TF. The U.S. Secret Service has also expressed interest in joining.	01Oct2018	16Oct2019	Closed; Memo to File
OIG-19-0008-I	Miami, Florida General Case Activities - FY 2019	MIAMI, FLORIDA GENERAL CASE ACTIVITIES - FY 2019 - TOIG is proactively initiating cases in Miami and the Southern Region of Florida. TOIG is participating on cases with other law enforcement agencies and the U.S. Attorney's Offices in those areas. This case will be used for investigative activities that are being reviewed and preliminarily investigated by TOIG.	01Oct2018	16Oct2019	Closed; Memo to File
OIG-19-0007-I	Jacksonville, Florida General Case Activities - FY 2019	JACKSONVILLE, FLORIDA GENERAL CASE ACTIVITIES - FY 2019 - TOIG is proactively initiating cases in Florida and the southeastern region of the United States. TOIG is participating on cases with other law enforcement agencies and the U S. Attorney's Offices in those areas. This case will be used for investigative activities that are being reviewed and preliminarily investigated by TOIG.	01Oct2018	16Oct2019	Closed; Memo to File

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

OIG-19-0005-I	Gulf Coast Ecosystem Restoration Initiation Activities - FY 2019	GULF COAST ECOSYSTEM RESTORATION INITIATIVE - FY 2019 - Treasury Office of Inspector General has been assigned primary oversight responsibilities for the funds distributed by Treasury related to the Gulf Coast Restoration Act. (RESTORE). As such OI is opening this initiative in IMIS to track information, training and investigative work related to the Gulf Coast Initiative. This case will be closed and re-opened at the beginning of each fiscal year for tracking purposes.	01Oct2018	16Oct2019	Closed; Memo to File
OIG-19-0004-I	Cyber Investigations & Digital Forensics Case Activities - FY 2019	CYBER INVESTIGATIONS & DIGITAL FORENSICS CASE ACTIVITIES - FY 2019 - This CYBER case will be used to track and document non-IMIS assigned investigative, liaison, research and development, attendance at conferences and training, and cyber/digital forensics developmental activities to support OI and the OI Cyber Program.	01Oct2018	16Oct2019	Closed; Memo to File
OIG-19-0003-I	BFS Improper Payment Case Tracking Initiative - FY 2019	BUREAU OF THE FISCAL SERVICE - IMPROPER PAYMENT CASE TRACKING INITIATIVE - FY 2019 In October 2014, the Office of Investigations (OI) continued an initiative surrounding fraud related to the payments made by the Bureau of Fiscal Service (BFS). This initiative will cover payments made including U.S. Treasury checks (CFIF & Non-CFIF) and ACH fraudulent payments including redirected benefit fraud. Tax refund fraud schemes paid by Treasury check or ACH payment are included. The ACH and Treasury check payment system is managed by the BFS and creates a mechanism for BFS to send payments authorized by a federal paying agency to authorized payees. As such OI receives information from BFS and a number of other sources on a monthly basis related to the investigative leads involving ACH and Treasury check fraud. OI is opening a case number in the case management system for OI to allow agents to utilize it for case development, and to document agent activities. This case will be closed at the end of fiscal year 2018 with a brief memorandum summarizing the year's activities.	01Oct2018	11Oct2019	Closed; Memo to File
OIG-19-0002-I	Duty Agent Investigative Activity - FY 2019	DUTY AGENT INVESTIGATIVE ACTIVITY - FY 2019 - This preliminary inquiry number will be utilized to document Duty Agent activity for FY 2018 and will include entity entries, case notes/documents to memorialize time dedicated to Duty Agent activity.	01Oct2018	11Oct2019	Closed; Memo to File
OIG-19-0001-I	MSB & FINCEN SAR TF Case Development - FY 2019	MSB & FINCEN SAR TF CASE DEVELOPMENT - FY 2019 - In October 2014, the Office of Investigations (OI) continued an initiative surrounding fraud related to Money Service Businesses (MSBs) and task forces dedicated to the analysis of Suspicious Activity Reports (SARs). U.S. Treasury oversees the registration of MSBs through the Financial Crimes Enforcement Network (FinCEN). TOIG is opening a case number in the case management system to allow agents to utilize it for case development and to document agent activities. This case will be closed at the end of the fiscal year with a brief memorandum summarizing the year's activities.	01Oct2018	11Oct2019	Closed; Memo to File

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

OIG-18-0023-I	SCAM	Scam - Email received by victim [redacted]). Victim forwarded email to DHS contact for assistance. DHS reached out to TOIG to inquire about whether or not a file or investigation was currently open on the identified subject. No current cases exist. Subject claims to be a Diplomat from the US Treasury. Subject attached photo of ID and photo of a Social Security Card. SSN was run through CLEAR with multiple returns.	15Nov2017	05Dec2019	Closed; Memo to File
OIG-18-0004-I	Cyber Investigations & Digital Forensics Case Activities - FY 2018	CYBER INVESTIGATIONS & DIGITAL FORENSICS CASE ACTIVITIES - FY 2018 - This CYBER case will be used to track and document non-IMIS assigned investigative, liaison, research and development, attendance at conferences and training, and cyber/digital forensics developmental activities to support OI and the OI Cyber Program.	03Oct2017	11Oct2019	Closed; Memo to File
OFAC-19-0028-P	Terrorist Threats	Complaint received 2/21/2019, via Office of Counsel Complaint forward from OFAC compliance division received an email related to an individual calming to be associated with a terrorist organization. Subject Email Address: [redacted]7@yahoo.com (Hello ...i am from iran...i am a terorist...I do now')	16Apr2019	29Apr2019	Closed; Preliminary Inquiry Closure
OFAC-18-0061-P		Complaint received OIG Intake regarding a person that submitted a FOIA request for another person is concerned because in communications between the two, one starts making threats and talks about getting a gun and coming to OFAC.	06Jul2018	12Apr2019	Closed; Preliminary Inquiry Closure

OFAC-18-0111-I		[redacted], NTC's Counter-Network Division, requested TIG investigative assistance regarding the[redacted] Crime Enterprise as it related to OFAC previously designated[redacted] as a Transnational Criminal Organization and Money laundering organization. Most recently SARs were filed for[redacted] and others for utilizing US correspondent banks to launder approximately $160 million for the[redacted] Cartel and subjects linked to Hizbolah. Intelligence gathering and assessment conducted by the NTC, U.S. Customs and Border Protection, resulted in intelligence indicating that Irish national[redacted] aka[redacted], is the patriarch of the[redacted] Criminal Network/Enterprise. Among other crimes, the[redacted] Network is involved in narcotics trafficking in Europe and money laundering utilizing services of individuals associated with Hizballah and linked to Iran. Intelligence also reports that the[redacted] Network is associated with the[redacted] E Drug Trafficking Organization which runs out of Chile and the Netherlands. Based on intelligence gathered by the NTC the[redacted] Network, utilizing a company known as[redacted], is also suspected of involvement in gambling associated with professional boxing and combat sports in the U.S. Identified members of the[redacted] family include: [redacted] JR, son of[redacted] Y[redacted] son of [redacted] son of [redacted] Also associated with the[redacted] Network are[redacted], [redacted] business associate;[redacted]; and[redacted]. [redacted] his sons, and several members of the[redacted] Network are currently residing in Dubai, UAE, where they have fled to avoid retribution in an ongoing shooting war with Irish organized crime network the[redacted] Family, led by patriarch[redacted], aka[redacted] K". [redacted] was resident in California until July, 2018 when his visa was revoked. During his stay	06Sep2018	06Aug2019	Closed; Memo to File
OCC-20-0004-P	OCC Threats/Phishing Emails	Complaint received 8/27/2019[redacted] ntake OCC ID: 19-0827-0834 Complaint received OIG Intake regarding[redacted], SDC and CFO, has recently received several threats via email. In addition concern to SDC[redacted] was a comment regarding a recent vehicle purchase and the knowledge of a prior password.	04Nov2019	04Nov2019	Closed; Preliminary Inquiry Closure

OCC-19-0045-P		From March - May 2017, fifty six (56) BBVA customer accounts were compromised leading to fraudulent withdrawals, totaling $290,000.00, plus an additional $42,900.00 in attempted fraudulent withdrawals. BBVA determined tha[redacted] conducted an Identification Verification on all the affected accounts and accessed an additional 3,688 BBVA accounts during the period of February 2017 to May 2017, outside of his territory and without a legitimate business purpose. [redacted] was subsequently terminated from BBVA in May 2017. [redacted] now works for Bank of America and is under investigation for unauthorized account access. [redacted] was also terminated by JP Morgan Chase Bank for fraudulent activity.	30Sep2019	17Dec2019	Closed; Preliminary Inquiry Closure
OCC-18-0071-P	Theft of Elderly Victims Funds from Multiple OCC-Regulated Banks, Illinois	On 7/11/18, FDIC-OIG referred a complaint allegation it received From BMO Harris Bank, Chicago, regarding allegations that a bank manager stole $68, 446 in deposits of an elderly account couple. A second complaint was received by another bank customer who alleged the same manager at BMO Harris took $100,000 of their deposits. The manager left BMO Harris and went to MB Financial Bank (also OCC-regulated) and allegedly stole $6,500 from an elderly account holder at MB Financial. The manager then transferred went to PNC Bank and took another $25,000 from the same elderly victim whose funds were transferred from MB Financial to PNC Bank. The total loss is $199,946 and the thefts occurred between 2012 and 2017. FDIC-OIG requested TIG's assistance on the investigation.	15Aug2018	24Jan2019	Closed; Preliminary Inquiry Closure
OCC-18-0026-P		Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of the above named subject being arrested for a DUI. OCC ID: 17-1201-1211	09Jan2018	13Mar2019	Closed; Preliminary Inquiry Closure
OCC-19-0045-I	Business Email Compromise of BankNet	Complaint received OIG Intake 3/15/2018 OCC ID Number: [redacted]2 Complaint receive OIG Intake regarding Citibank [redacted]) Unauthorized Access to Bank Net	04Apr2019	10May2019	Closed; ROI - Referral to Bureau for Info Only
OCC-19-0030-I	Variq	Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of the following: OCC ID: 17-1116-1139 allegations made by a former OCC contractor [redacted]) involving violations of US Treasury and OCC whistleblower protection rules.	08Feb2019	05Aug2019	Closed; ROI - Referral to Bureau for Info Only

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

OCC-19-0029-I		This Homeland Security Investigations (HSI) Document & Benefit Fraud Task Force (DBFTF) investigation concerns a fraudulent scheme whereby foreign nationals seeking student visas pay up to $9,000 to individuals to sit for U.S. educational exams on their behalf, using false identification documents, including fraudulent passports, to achieve a desired score. The exam results are then submitted to U.S. educational institutions. DBFTF recently discovered a paid test-taker, [redacted] sitting for an educational exam in Washington, DC, after having presented a fraudulent passport. [redacted] was later determined to have sat for the same U.S. educational exam under approximately 23 different identities in four different countries. Additionally, DBFTF discovered that the ex-husband of the aforementioned paid test-taker is involved in the conspiracy and was determined to have sat for the same U S. educational exam under approximately 12 different identities in the U.S. and Mexico. The subject and her associates are utilizing various OCC regulated banks to facilitate and further their fraudulent scheme. So far, DBFTF has identified thirty-five foreign nationals who have each paid the subject $6,000 to $9,000 to take the exams on their behalf. There are more subjects or cells who have yet to be identified. Possible violations are 18 U.S.C. § 1543, 1028A, 1341, 1343, and 1956(h). This case has been accepted by the U.S. Attorney's Office for the District of Columbia for prosecution.	29Jan2019	04Dec2019 Closed; Memo to File
OCC-18-0106-I		[redacted]) was a victim of a phishing attack that requested Vendor banking (OCC regulated bank Capital One) information/account be changed to a fraudulent account. On January 17, 2018 AGS was made aware that they were a victim of a phishing email that requested to change Vendor [redacted]) banking information. The phishing email was located as launched in June and July 2017. The phishing emails were supposedly sent from [redacted]. The loss to the company is approximately $10,000.00.	14Aug2018	26Nov2019 Closed; Memo to File
OCC-18-0097-I	Bank of China	Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of fraud. OCC ID: 17-0525-0509	18Jul2018	12Jul2019 Closed; Memo to File

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

OCC-18-0092-I	OCC ID: 17-0913-0928 Correspondence received via OIG Intake from [redacted] the OCC regarding allegations of the following: June 21, 2010 [redacted] Former Citizens Bank employee made unauthorized withdrawals from [redacted]. Business Accounts in the amount of $5650.00 June 24, 2010 unauthorized withdrawal of $4900.00 check# 5001 July 2, 2010 [redacted] Former Citizens Bank employee made unauthorized withdrawals from [redacted]. Business Accounts in the Amount of $2500.00 July 8, 2010 [redacted] former Citizens Bank employee made unauthorized withdrawals from [redacted].Business accounts in the amount of $8500.00 July 19, 2010 check # 5002 was unauthorized in amount of $6100.00. July 23,2010 check # 5003 was unauthorized in amount of $15,000.00 July 29,2010 [redacted] Former Citizens Bank employee made unauthorized withdrawals from [redacted]. Business accounts in the amount of $3500.00 August 9,2010 Unauthorized transfers from another [redacted] Business accounts in the amount of $2000.00, $7000,00 and $3500.00 August 9,2010 [redacted] Citizens Bank employee made unauthorized withdrawal from [redacted]. Business Accounts in the amount of $16000.00. Citizens Bank, National Association - CAG # 03127434	16Jul2018	06Aug2019	Closed; ROI - Referral to Bureau for Info Only
OCC-18-0076-I	Complainant received 10/26/2017, via Hotline phone Complainant alleging, [redacted] an OCC employee misusing her position by working another job while on government time and misusing her teleworking and timesheets.	22May2018	27Mar2019	Closed; Memo to File
OCC-18-0050-I	Beginning in October 2017 and currently ongoing, [redacted] allegedly utilized fraudulently obtained personal identifiable information (PII) to add herself as an authorized user on [redacted] (an OCC Regulated institution) credit card accounts. The subject would provide the compromised account numbers along with compromised PII within various retail locations in North Florida where she would proceed to make purchases. Many of these transactions have been recorded on video surveillance footage. On February 5, 2018 the most previous inquiry ran by [redacted] fraud investigations, the loss amount was at $15,000 and 26 accounts had been compromised.	14Feb2018	10Dec2019	Closed; ROI - Not Forwarded to Bureau
OCC-18-0036-I	OCC ID: 17-1024-1034 Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of unauthorized disclosure of information.	04Jan2018	26Sep2019	Closed; ROI - Response Received
OCC-18-0028-I	Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of the above named subject being arrested for narcotic drug possession/use.	27Nov2017	03Jun2019	Closed; ROI - Response Received

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

OCC-18-0027-I	Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of possession/use of a narcotic drug by the above named subject resulting in an arrest.	27Nov2017	16Jan2019	Closed; ROI - Response Received
OCC-18-0026-I	Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of the above named subject being arrested for possession/use of a narcotic drug.	27Nov2017	03Jun2019	Closed; ROI - Response Received
OCC-18-0024-I	On October 31, 2017, the Department of the Treasury Office of Inspector General (TOIG) Office of Criminal Investigations received a complaint from the Randolph County Sheriff's Office (RCSO) in regards to a credit card fraud, bank fraud and identity theft case. During a search warrant on October 24, 2017, the RCSO located numerous counterfeit credit cards, skimmers, computers, an embosser and a large indoor marijuana grow operation. Continuing on October 31, 2017, TOIG reviewed the evidence seized by the RCSO during the search warrant and determined the following: There were numerous amounts of counterfeit credit card stock located in the residence along with a skimmer, computer and an embosser. There were 34 re encoded credit cards located on the property with a large number of the victims being from the piedmont triad area of North Carolina. The re encoded cards had PIN numbers and zip codes written on the back of the cards in order for them to be used in point of sale machines that required a second form of authentication. Suspect [redacted] had numerous counterfeit credit cards embossed with his name on them. Two thumb drives located at the residence contained numerous lines of credit card information that included names and account numbers. A review of the credit card information revealed numerous accounts belonging to OCC regulated banks. TOIG also determined [redacted] is the main suspect in numerous skimming identity thefts along the I-85 corridor. [redacted] is currently charged in four counties in connection in gas pump skimming operations. On November 8, 2017, TOIG and the RCSO met with AUSA [redacted] regards to this investigation and presented the case for prosecution. AUSA [redacted] y requested TOIG continue to investigate the financial side of this case and submit a report to him with the findings.	20Nov2017	20Mar2019	Closed; ROI - Not Forwarded to Bureau

OCC-18-0018-I	Beginning in July 2017, [redacted] utilized fraudulently obtained personal identifiable information (PII) to add themselves as authorized users on Synchrony Bank (an OCC Regulated institution), JC Penny accounts. The subjects would provide the compromised account numbers along with their identification within JC Penny locations in South Florida where they would proceed to purchase large quantities of gift cards. Many of these transactions have been recorded on video surveillance footage. On July 13, 2017, [redacted] were arrested by Coral Springs Police Department in the parking lot of the Coral Springs Mall, 1200 Riverside Dr Coral Springs FL. The subjects were arrested for no driver's license and marijuana. In their possession was PII and JC Penny gift card receipts which were placed into evidence. On August 24, 2017, [redacted] and [redacted] were arrested by Miami Dade Police Department at JC Penny, 7201 SW 88th Miami, FL, in reference to credit card fraud. During the course of the arrest PII was located within their possession. On October 18, 2017, Synchrony Bank fraud investigations indicated the loss amount was at $193,000, and 300 accounts had been compromised.	07Nov2017	12Apr2019	Closed; ROI - Not Forwarded to Bureau
OCC-18-0010-I	Homeland Security Investigations (HSI) Document Benefit Fraud Task Force (DBFTF), Dulles, VA, contacted TOIG and requested assistance with a criminal investigation involving a naturalized U.S. citizen who was utilizing her businesses in Virginia to bring in foreign nationals from Asia and Southeast Asia into the U.S. [redacted] the subject of the investigation, provided fraudulent U.S. visas to foreign nationals in exchange for approximately $1,000 per visa. Some were provided with legitimate student visas, which came with higher fees. After entering the U.S., under the guise of being "students", the foreign nationals would obtain employment with the intention of permanently residing in the U S. From January 2014 through February 2016, [redacted] generated approximately $2,516,369.75 in illicit proceeds by collecting fees from "students" enrolled in one of her businesses, [redacted]. In order to conceal the true source of income, [redacted] egregiously used her family members as nominees for various bank accounts, including accounts at OCC regulated banks. A HSI source stated that [redacted] recently purchased a $580,000 residence in Alexandria, VA, entirely with cash. TOIG's role within this HSI-TOIG joint investigation will be to provide financial expertise, specifically focusing on [redacted] money laundering activities.	06Oct2017	22Nov2019	Closed; Memo to File

OCC-17-0870-I		On October 22, 2014, Homeland Security Investigations, Washington DC (HSI/DC) initiated an investigation on [redacted], a citizen of Serbia, for engaging in marriage fraud to evade immigration law. United States Citizenship and Immigration Services, Office of Fraud Detection and National Security (FDNS) initiated a joint investigation with HSI/DC on [redacted]C. As a result of the joint investigation, approximately two hundred additional marriages were identified as being potentially fraudulent and facilitated to evade immigration law. FDNS is referring to the investigation as "Operation Endless Summer" (OES). HSI/DC is now also referring to this case as "Operation Endless Summer" instead of [redacted]." The name "Operation Endless Summer" alludes to the method by which the beneficiaries of the fraudulent marriages enter the United States. Most of the beneficiaries were originally admitted to the United States as J1 or H2B non-immigrant visa holders to engage in temporary summertime employment. Rather than depart at the end of the summertime employment, these individuals entered into fraudulent marriages to U.S. citizens in order to remain in the U.S. [redacted], were identified by the HSI Document and Benefit Fraud Task Force (DBFTF), Merrifield, VA, as entering into fraudulent marriages in Virginia. In addition to fraudulent marriages, [redacted] set up businesses, [redacted] and [redacted], to defraud U.S. banks by utilizing a "bust-out" and/or kiting scheme. These banks included those regulated by the Office of the Comptroller of the Currency (OCC). To date, [redacted], [redacted], and others have defrauded JPMorgan Chase, Capital One, Citibank, Department Stores National Bank, World Foremost Bank, and Fifth Third Bank of at least $687,278. HSI DBFTF has contacted TOIG and requested	07Sep2017	17Sep2019	Closed; Memo to File
OCC-17-0855-I		Correspondence received via OIG Intake from [redacted] with the OCC regarding allegations of possible unsafe or unsound banking practices and violations of applicable laws, rules and regulations by the above named subject.	02Aug2017	24May2019	Closed; ROI - Referral to Bureau for Info Only
OCC-17-0694-I	CHECK 'N GO JAX	From April - June 2015, Check 'n Go locations in Jacksonville, Florida, were targeted by a counterfeit check cashing ring. The Counterfeit checks were drawn on Wells Fargo Bank and other OCC regulated financial institutions. From September 2015, the Jacksonville Sheriff's Office and TOIG worked with Check 'n Go personnel, obtained check and video evidence for transactions, reviewed evidence, compared video with known photos of subjects and submitted requests for multiple arrest warrants for the subjects that could be identified in the 4th District of Florida.	27Feb2017	01Mar2019	Closed; ROI - Not Forwarded to Bureau

OCC-17-0503-I	From January 28, 2016 to August 4, 2016, in the City of Durham, Durham County, North Carolina, within the Middle District of North Carolina and other States, [redacted] did knowingly convince retail merchants to "force" more than 400 attempted and completed transactions on his behalf, totaling more than $170,000 in attempted credit card purchases using a Bank of America Business Debit Card 5[redacted]7 issued to [redacted] issued to [redacted], a NetSpend Prepaid card, and an American Express Gift Card. [redacted]. took advantage of a particular type of debit card transaction known as a "forced sale," which is used from time to time in regular business dealings and is described briefly below. Ordinarily, when a merchant swipes a credit or debit card, a computerized check is performed to determine whether the account associated with the card is valid. If the account is open and funds are available, the transaction goes through; if the account is closed or funds are unavailable, the transaction is denied. If the transaction is denied, a merchant has two choices: ask the customer for another card, or perform a "forced sale" using the declined card. During a typical forced sale, the merchant calls the card issuer (i.e., the customer's bank or Credit Card Company) and receives an authorization code. The merchant types the code into the credit card terminal and "forces" the transaction, essentially overriding the denial and allowing the sale to go through. At some later date, the merchant and the card issuer settle the outstanding charge. But for technical reasons relating to the forced sale process, it does not actually matter what code the merchant types into the terminal. Any combination of digits will override the denial. So long as the customer provides a fake authorization code and convinces the merchant to enter it into the terminal, the transaction will go through. The merchant is unlikely to discover the fraud	26Jan2017	28Aug2019	Closed; ROI - Not Forwarded to Bureau

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

OCC-16-1366-I	On February 11, 2016, Durham District Attorney's and the US Attorney's Office Middle District of NC requested assistance from TOIG reference a case that was being worked by the Durham County Sheriff's Office. The case involved the embezzlement of $362,728.36 from BASF, a chemical company with a large presence in the Research Triangle Park, by an employee, [redacted] On August 14, 2015 [redacted] CEO of [redacted] contacted [redacted]), a BASF Corporation employee and head of the Communications department in Research Triangle Park, NC. [redacted] reported suspicious requests made by [redacted] explained that [redacted] requested invoice assistance for administrative convenience. Upon his request, [redacted] paid invoices to [redacted] on behalf of BASF. [redacted] explained that [redacted] invoiced BASF the amount on [redacted] invoices plus a standard 2.5% administration fee. [redacted] waited to receive payment from BASF and then paid [redacted] reported that [redacted] became alarmed after further requests by [redacted] and decided to investigate. As a result, [redacted] found that [redacted] is owned by [redacted]' sister. [redacted] contacted BASF and provided relevant information The Corporate Audit found evidence to substantiate the allegation of improper transactions. The audit revealed that between June 2013 and September 2015, Charles authorized invalid invoices and incurred personal expenses on his Corporate T&E card in the amount of $362,728.36 USD. The street address on [redacted] invoices was the same as the address for [redacted] Construction Inc. The law firm [redacted] was found to be associated with [redacted]' father, shared the same address as [redacted] and [redacted] Construction Inc. All payments for [redacted] services were approved by [redacted] although no services were received by BASF. The invoiced services were generally for video production, events and marketing activities. Public records obtained from the State of Missouri's	29Mar2016	02Dec2019	Closed; ROI - Not Forwarded to Bureau
OCC-16-0136-I	Complaint received 10/20/2015, via mail Fayetteville Poli[redacted]t. investigating USAA Federal Savings Bank, notifying TOIG and Homeland Security for additional resources. Fayetteville Police Dept. claims to have investigated hundreds of cases involving USAA and their fraudulent bank practices.	20Oct2015	16Jul2019	Closed; ROI - Not Forwarded to Bureau

OCC-15-2222-I	On Friday 04/03/15, Corporate Investigator [redacted] received a telephone call from LRM Fraud Investigator, [redacted] concerning a fraud claim she was investigating. [redacted] said client, [redacted] was reviewing his Investor's Deposit Account when he discovered two withdrawals noted on his account that he did not make. One of the withdrawals was a counter check that was issued on 03/05/15 in the amount of $10,000.00 and the other was also a counter check that was issued on 03/31/15 in the amount of $5,000.00. Research by [redacted] confirmed that both transactions were conducted by Branch Banker [redacted] Video of the transactions confirmed that [redacted] was on the teller line; however, a client was not present at the time of either transaction. [redacted] contacted the branch to follow up with the Teller Supervisor, but during the conversation, [redacted] inadvertently became aware of the inquiry. Due to [redacted] response to questions, [redacted] was afraid [redacted] would not return to work on the following Monday now that she knew an investigation into the two transactions was ongoing. [redacted] sent copies of the two fraudulent counter checks to [redacted] with supporting documentation. After receiving the copies, [redacted] went to the branch and met with [redacted] During a subsequent interview, [redacted] initially denied remembering anything about the two counter checks, but after further questioning, she admitted to forging and uttering the two counter checks drawn on [redacted] s account. [redacted] alleged she had a seizure on 03/04/15 due to brain surgery she had in 2011, and the seizure made her act impulsively. Due to her condition, she forged and uttered the check for $10,000.00 on 03/05/15 and took the money from the transaction home and hid it in a diaper bag that was in her closet. She spent the money on gifts for her children and also put $1,000.00 into her daughter's BB&T Savings Account. On 03/30/15 she had another seizure and was out of work; however, when she returned on 03/31/15 she forged and	27Aug2015	29Mar2019	Closed; ROI - Not Forwarded to Bureau

OCC-15-1486-I	On April 8, 2015 SunTrust Bank Corporate Security Investigator [redacted] contacted TOIG in reference to an employee misconduct investigation involving SunTrust employee [redacted] advised TOIG that SunTrust "back office" had noticed a series of losses incurred by the bank on business accounts opened by branch manager [redacted] in Mt. Pleasant, South Carolina. [redacted] and another SunTrust investigator interviewed [redacted] who admitted he had used Personal Identification Information (PII) from customers at his previous employer, Regents Bank, to open business accounts so that he could "kite checks and wires" through the accounts. [redacted] then used the "kited money" in the accounts for his own personal gain and to pay bills in order to maintain his lifestyle. A search of [redacted] Office revealed numerous Regents Bank documents with the PII of several of [redacted] former customers. [redacted] provided [redacted] with a written statement outlining how he had conducted the fraud. [redacted] also retained the PII information located in [redacted] Office. Possible charges in this case are: Bank Fraud 18 USC 1344 Aggravated Identity Theft 18 USC 1028(A) Wire Fraud 18 USC 1344 On April 13, 2015 TOIG contacted USSS SA [redacted], Charleston RO, in regards to this investigation. After discussing the facts of this case it was agreed this would be joint investigation between TOIG and USSS-Charleston. On April 15, 2015 TOIG was contacted by [redacted] Attorney [redacted] in regards to this investigation. [redacted] requested TOIG/USSS conduct a proffer interview with [redacted] stated [redacted] was willing to provide a full confession in regards to this matter and would cooperate with investigators completely. An interview with [redacted] is tentatively scheduled for April 28, 2015 in Charleston, South Carolina. On April 17, 2015 AUSA [redacted] was verbally briefed on the facts of this case and verbally accepted it for federal prosecution. [redacted] requested TOIG and USSS meet with him on the afternoon	22Apr2015	29Mar2019	Closed; ROI - Not Forwarded to Bureau

OCC-15-1398-I		On April 8, 2015 AUSA [redacted] requested TOIG assistance with a bank fraud investigation in Winston-Salem, North Carolina. The bank fraud was committed by a BB&T employee who has been the subject of numerous internal investigations by the bank. [redacted] was employed by BB&T Bank from August 30, 2010 until the end of March 2015 as teller. During the early part of her employment with BB&T [redacted] also worked for [redacted] at [redacted] in Winston-Salem, North Carolina. On January 8, 2015 BB&T Corporate Security Investigator [redacted] began investigating numerous suspicious transactions in an account held by a customer named [redacted] i. [redacted] reported unauthorized withdrawals from his account that appeared to have originated with forged counter withdrawal slips. [redacted] examined all 126 counter withdrawal slips for the year 2014 and determined 49 appeared to be forged. [redacted] asked [redacted] i to review the suspected forged withdrawal slips and he confirmed 46 were in fact forged and unauthorized. [redacted] determined all 46 known forged withdrawal slips had been processed or cashed by teller [redacted] It was determined that $7,060 had been removed from [redacted] account without his authorization from May 14, 2014 through December 12, 2014. BB&T Corporate Security attempted to interview [redacted] on January 15, 2015 in regards to this investigation. That attempt was met with negative results due to the fact [redacted] made her self unavailable by claiming illness and refusing to come out of the rest room. A records check for [redacted] at the Winston-Salem Police Department (WSPD) revealed she had been listed as "involved otherwise" in a Larceny report (WSPD #1 [redacted]) in which [redacted] was the victim. The report stated four checks had been stolen from his place of business at [redacted] l Associates. The stolen checks were from his business account at PNC Bank (OCC Regulated) and were forged and cashed for a total	09Apr2015	10Dec2019	Closed; ROI - Not Forwarded to Bureau
OCC-13-1711-I	AURORA BANK: OCC INVESTIGATION	Office of the Comptroller of the Currenc [redacted] enior Advis [redacted] notifies the OI that on 05/31/2013, "the OCC opened a formal investigation into Aurora Bank, FSB, Littleton, CO. Issues include backdating practices, making false statements to mislead the [Office of Thrift Supervision], and the failure to file a suspicious activity report (SAR)." Also, "[o]n June 4, 2013, the bank filed a SAR on three employees . . . for potential obstruction of the OTS's examination process. The SAR is numbered [redacted]."	18Jun2013	08Feb2019	Closed; ROI - Not Forwarded to Bureau

NCUA-16-2343-I		Investigation referred by the Portsmouth, VA Sheriff's Office to TOIG on 6/28/16. New Bethel Federal Credit Union (Portsmouth, VA) was closed voluntarily (conservatorship) by the NCUA on 4/30/15. It was a church- related FCU for New Bethel Church. Sheriff's investigation determined $35,000 in seven fraudulent loans received by the credit union's CEO and Portsmouth City council member [redacted]. The loans were taken in 2013 to pay off a property tax lien of $161,500 for the New Bethel Church. The lien was not paid and the disposition of the loan funds was undetermined. The $35,000 in loan funds were paid back by [redacted] in 2014 after pressure by the NCUA. The 7 fraudulent loans were made in $5,000 amounts; they were made to church and family members; their identifications and signatures were forged as were the social security numbers of two unrelated Virginia residents.	14Jul2016	10Dec2019	Closed; ROI - Not Forwarded to Bureau
NCUA-16-2012-I	First Hawaiian Homes Federal Credit Union	[redacted] and [redacted], employees of First Hawaiian Homes Federal Credit Union embezzled over $1,000,000 according to an NCUA analyst. The embezzlement forced the NCUA to close the credit union.	13Jun2016	29Jan2019	Closed; ROI - Not Forwarded to Bureau
MSB-13-1500-I		It is alleged that [redacted], who is the Owner and/or Manager of [redacted] and other unknown individuals conspired to cashing fraudulent U.S. Treasury checks through his business belonging to other individuals. It is alleged that [redacted] cashed 37 U.S. Treasury checks, in excess of $200,000.00, through his business in Dallas, TX, that belong to New York City residences. It is further alleged that [redacted] is a registered MSB, and failed to file SARs.	22May2013	10Jun2019	Closed; ROI - Not Forwarded to Bureau

IRS-16-0181-I		On October 13, 2015, SSA [redacted] informed TOIG of a complaint from the Stokes County Sheriff's Office (SCSO) involving an IRS Phone Scam. [redacted] advised the SCSO had taken a report from a female who stated she had been contacted by an individual who stated he was with the IRS and that she needed to pay $5600 in back taxes immediately or she would be arrested. The female then withdrew money from her bank and proceeded to the Bank of America (BOA) on University Drive in Winston-Salem, North Carolina and deposited $5600 into the account of [redacted], account [redacted] as she had been instructed. Continuing on this date, TOIG conferred with BOA security and determined there had been numerous counter credits deposited into account [redacted] over a ten day period from October 6, 2015 through October 15, 2015. On October 14, 2015, TOIG requested a and was granted a federal grand jury subpoena for BOA account [redacted] under the Middle District of North Carolina (MDNC) SAR review team's open matter in the United States Attorney's Office. On October 19, 2015, TOIG reviewed the subpoenaed documents from BOA account [redacted] and determined the numerous counter credits from the ten day period of October 6, 2015 through October 15, 2015 were suspicious in nature and were consistent with an IRS Phone Scam.	26Oct2015	29Mar2019	Closed; ROI - Not Forwarded to Bureau
FinCEN-19-0008-P		Complaint received 11/29/2018, via OIG Intake Complaint received OIG Intake regarding a phone call, and subsequent email, from an attorney with [redacted] & Company, a broker dealer, stating that they have been contacted by an individual representing themselves as a FinCEN Special Agent in an attempt to extract money from the account at the broker dealer in the name of a deceased relative. The attached email is directly from the broker dealer, and contains information on the individual's actual identity. Their email also contains several attachments that were sent from the individual. Subject Telephone Number: [redacted]	29Nov2018	05Jun2019	Closed; Preliminary Inquiry Closure
FinCEN-19-0065-I	Mexican Articles	FinCEN [redacted] forwarded a complaint regarding protected financial information (or misinformation) about Mexican Minister [redacted] that has been reported in Mexican articles and attributed the source and/or confirmation of the validity of the information to the U.S. Treasury (or United States).	27Sep2019	05Nov2019	Closed; ROI - Referral to Bureau for Info Only

FinCEN-19-0032-I		TIG received a phone call from [redacted], Chief, Washington Metropolitan Airports Authority Police, advising that he pulled over a vehicle for speeding on the Dulles Access Rd. The driver claimed that he was a Department of Treasury, Policy Advisor. The driver was driving a POV, Crown Victoria type vehicle. The vehicle has red/white rear deck lights. [redacted] said he has a concealed carry permit. [redacted] said that driver claimed that he was given the lights as "courtesy lights".	21Feb2019	23Aug2019	Closed; ROI - Response Received
FinCEN-19-0026-I	[redacted] LP (MSB)	On August 1, 2018, TIG was contacted by the FDIC-OIG and Homeland Security Investigations (HSI), Calexico regarding an MSB that is suspected of structuring large foreign exchange transfers from Mexico into the U.S. The source of funds and their repatriation to banks in the U.S. has also raised suspicion. [redacted] LP and its sister entity, [redacted]) is registered with FinCEN as an MSB (registration number [redacted]) and is owned by [redacted] and other family members. It provides check cashing, currency exchange, and money order sales. There are numerous concerns: 1. It moves large quantities of bulk cash. Between a 5 month period in 2017, [redacted] moved $158.8 million dollars. 2. [redacted] is transferring currency from Mexico via its foreign sister [redacted] to the US for deposit into US banks, one of which is City National Bank of New Jersey. Funds are moved from [redacted] in Mexico and driven across the US border to [redacted] and deposited into a US bank. [redacted] is "blocked off" from the transaction and relies upon its sister entity, [redacted], to provide customer identifying information. By lacking this information ("know your customer"), the source and purpose of the repatriated funds are unknown. 3. The identify of checks presented for deposit by merchants and customers are unclear and the amounts are in round dollar amounts which are known indicators of money laundering. 4. ACH deposit credits lack identifying information and [redacted] utilizes Western Union to receive ACH credits, many of which are lacking customer information. 5. The movement of cash from Mexico to the U.S. is considered to be repatriation of funds and is a known vehicle for money laundering. FDIC-OIG & HSI will make a case presentation to USAO SDCA on 9/19/18.	14Dec2018	07Mar2019	Closed; Memo to File

FinCEN-17-0875-I	On August 30, 2017, the USAO for the Northern District of Oklahoma requested TOIG lead an investigation into allegations of bank fraud and bankruptcy fraud. The case was referred to NDOK by the Office of the U.S. Trustee. [redacted] alleged that [redacted] and his company, [redacted], committed loan fraud in the amount of $4,951,957. The U.S. Trustee alleged that [redacted] intentionally misstated inventory; initially [redacted] claimed $3,327,648 in inventory, and later amended it to $12,642.	25Sep2017	16Aug2019	Closed; ROI - Not Forwarded to Bureau
FinCEN-17-0869-I	Subject is alleged to be laundering large amounts of currency obtained while operating a mid/high level narcotics trafficking organization between New Jersey and Northern Virginia.	01Sep2017	12Apr2019	Closed; Memo to File
FinCEN-17-0832-I	Beginning in or about September 2016, [redacted] has been operating an illegal gambling business in Dallas, TX. The business consists of 94 machines. The proceeds are laundered by an employee, [redacted], converting cash deposits into his account into cashier's checks, which are then deposited into an account for [redacted], which is owned by [redacted]d and his wife [redacted] Dallas PD estimates that each of the 94 machines earns approximately $345/week (~$12,400/week total, ~$129,700/month).	05Jun2017	12Apr2019	Closed; ROI - Not Forwarded to Bureau
FinCEN-16-2102-I	Correspondence received via OIG Intake from Rich Delmar with TOIG Counsel regarding the following: [redacted] is a [redacted] currently assigned as an intelligence analyst at FinCEN, a position he has held for approximately 16 months. On Friday, June 3 rd , our office was notified by [redacted], the FinCEN [redacted], that a significant issue existed with [redacted]'s TS clearance.	20Jun2016	26Apr2019	Closed; Memo to File

DO-19-0034-P	Complaint received 7/24/2019, via OIG Intake Complaint received OIG Intake regarding a Treasury employee, [redacted], (a Presidentially Appointed, Senate confirmed position) has been delayed due to a disagreement between Treasury and the Office of Government Ethics (OGE). [redacted] is a non-career SES [redacted] in the Office [redacted] and was appointed to his position on May 1, 2017. He has provided occasional information technology assistance to his father's [redacted] practice for which he was compensated as a 1099 independent contractor. He received $3,300 in 2017; $2,700 in 2018; and approximately $1,500 in 2019. He described the duties as database management and help desk support. Specifically, he stated that he occasionally fielded questions to troubleshoot problems such as restoring internet service and accessing network drives. He formally terminated all contractor work on July 1, 2019. [redacted] did not disclose this position or the income received on his new entrant financial disclosure report; 2018 annual financial disclosure report; his nominee financial disclosure report; or his 2019 annual financial disclosure report. It is our understanding that the filer did report this 1099 income on his tax returns but inadvertently omitted it from his financial disclosure reports. Treasury became aware of the 1099 income through an inquiry from the Senate. Treasury has advised [redacted] of the requirement to amend his nominee financial disclosure report to include the 1099 income. The amendment process will require OGE certification. Due to OGE's position on potential noncompliance with EIGA, OGE will move forward with certifying the amendment when it receives confirmation that Treasury's Inspector General and/or the Civil Division, Department of Justice, will not pursue action on the matter.	24Jul2019	24Jul2019	Closed; Preliminary Inquiry Closure

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

DO-19-0026-P		Complaint received on 12/17/2018 via online complaint form Complainant alleges the following regarding the subjects: "Issue 1: That [redacted] appeared to portray its suite of IT products as a fully integrated product during its response to a Request for Quote in the Spring of 2017. Team [redacted] made assertions of integration, in writing as part of formal responses, and were so material of fact that companies who did not have a fully integrated software suite were not allowed to compete past an initial round. During the implementation of the suite of products, Team [redacted] provided statements proving its product was not fully integrated as required – and it could not meet contract requirements. This cost the government tens of thousands of dollars in extra costs. Issue 2: That [redacted] appeared to have engaged in a regular pattern of directing the shifting monies between accounts in violation of signed agreements with Treasury Bureau customers. One specific shift of funds occurred in and around the ITM project, during which [redacted] directed the shifting of roughly $300K from other accounts to the [redacted] Judging by conversations heard in the [redacted] Ops office, the shifting of funds through the COBRA system is a regular occurrence. However, the shifting appears to violate law as the former head of the shared services fund told me, directly, that such shifts could not happen, legally. Issue 3: That [redacted] appeared to fail to manage a modification to Task Order 3 (T[redacted]) allowing the vendor to thus far not deliver a capability clearly laid out in the Task Order modification (indeed it was the focus of the modification) and a capability that Team [redacted] promised to provide instead of receiving financial compensation for Team [redacted] failure to perform. The financial compensation could have netted hundreds of thousands of dollars in savings to Treasury. Issue 4: That [redacted] and [redacted] independently decided to not implement a compensation capability of the [redacted] software, even though	[redacted]	[redacted]	
[redacted]		[redacted] contract with the City of Gainesville, Florida. This solar farm was transferred and sold three times before it was built and had received federal grant money in the amount of 1.769 million dollars. The Government and the beneficiaries were tricked into signing papers that allowed the Government to be tricked into receiving federal grant money. The amount awarded was $981,272.00 and $788,531.00 to [redacted]. This was [redacted] solar contract and land before he died on April 3, 2010. I am reporting State Fraud and Federal Grant Fraud and transferring real property solar contract and land without any witnesses or notary, that's Florida Law.	02May2016	19Nov2019	Closed; Preliminary Inquiry Closure
DO-16-0591-I	Primary Dealers	Correspondence received from DOJ Senior Trial Attorney [redacted] regarding allegations of possible Treasury Securities fraud.	02Jan2016	08Feb2019	Closed; Memo to File

DO-16-0141-I		Correspondence received via OIG Intake from [redacted] with the Department of the Treasury regarding an incoming complaint from [redacted] with allegations of fraud. This case was referred to the Office of DC Pensions from the Bureau of Fiscal Service on August 21, 2015.	21Oct2015	12Apr2019	Closed; ROI - Referral to Bureau for Info Only
DO-15-2094-I		Correspondence received via OIG Intake from [redacted] with DC Pensions regarding allegations of the following: The caller included information regarding the previous POA, [redacted], who reportedly had given [redacted] and [redacted] a card, maybe a money card, with which [redacted] retirement funds can be accessed. The caller also reported that before per the police report, [redacted] passed away on December 4, 2014. The caller stated that [redacted] and [redacted] kept the card and is splitting the money from [redacted] retirement. (It is not clear from the police report what type of card was given to [redacted] and [redacted].) Keywords: LEC (LEC) Law Enforcement Contact Vulnerable Population DC Pension	30Jul2015	12Apr2019	Closed; Memo to File
DO-15-1074-I	[redacted]	[redacted], National Renewable Energy Laboratory (NREL), contacted TOIG as well as [redacted], Program Manager, 1603 Program stating that he had new information regarding [redacted]). TOIG had investigated [redacted] previously (Case DO-12-0367-I) but found issues were mostly civil complaints filed by dissatisfied customers and contractor and not federal loss. The new complaint by [redacted] is that [redacted] is providing false information regarding the production of wattage in properties. For example, for [redacted], the property's owner died, and the new owner has no knowledge of a leasing agreement for the panels, and [redacted] continues to file annual documentation with Treasury / NREL with former owner's name and wattage that appears to be falsified by [redacted] writes: "The original homeowner died in 2013, the current homeowner owns the solar property with no lease agreement, but [redacted] and [redacted] keep filing falsified annual reports as though nothing has changed. Out of curiosity, I also compared [redacted] estimates to NWREL's filed report since [redacted] is claiming their annual reports are based on [redacted] calculations. As you can see from the production (normalized), [redacted] properly displays a higher level of production in summer and lower level in winter."	26Feb2015	12Apr2019	Closed; ROI - Referral to Bureau for Info Only

DO-15-0006-I		In August 2014, the U S. Department of the Treasury (Treasury), Office of Inspector General (OIG) Office of Investigations (TOIG), received information as part of an initiative with Housing and Urban Development, OIG, Office of Investigations (HUD-OIG), that [redacted], Owner, [redacted]), received approximately $240,792 in grant funds from [redacted]) relating to 645 mortgage counseling clients serviced by [redacted]. The funds are congressionally appropriated and disbursed by the U.S. Department of the Treasury. An [redacted] compliance review of [redacted] discovered no less than 383 of the 645 [redacted] clients were either non-owner occupants or entirely invalid addresses. [redacted] has also received HUD grant funds for similar counseling services.	02Oct2014	24Jan2019	Closed; ROI - Not Forwarded to Bureau
DO-14-0601-I	HOMETOWN NATIONAL BANK	Correspondence received via OIG Intake from [redacted] with the OCC regarding a SAR filed on the above mentioned bank and the following: The Control Group is comprised of [redacted], [redacted], [redacted], [redacted] and [redacted].	14Feb2014	10May2019	Closed; ROI - Referral to Bureau for Info Only
DO-12-2590-I	Development Bank of American Samoa, et al. (ARRA)	Complaint received 9/12/2012, via email *** COMPLAINANT REQUESTS CONFIDENTIALITY *** Complainant alleges - The federally funded section 1602 program was rushed through and some projects were awarded to friends and relative of development Bank of American Samoa board members and bank officials.	12Sep2012	26Nov2019	Closed; ROI - Referral to Bureau for Info Only
CYBER-18-0055-P	Digital Forensic Support to CNCS OIG and NARA OIG	Provide digital forensic support (laptop and mobile phone examination) to a joint CNCS OIG and NARA OIG investigation	22Jun2018	10May2019	Closed; Preliminary Inquiry Closure
CDFI-19-0021-P		Complaint received 3/14/2019, via OIG Intake Complaint received OIG Intake regarding a FraudNet hotline complaint, New Markets Tax Credit (NMTC) program. The complaint alleged an individual named [redacted], via a Community Development Entity (CDE), may have misappropriated funds generated from the Community Development Financial Institution (CDFI) program's NMTC tax credit allocation authority. It was further alleged that [redacted] had a documented history of funds misuse associated with government administration.	21Mar2019	12Jul2019	Closed; Preliminary Inquiry Closure

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

CDFI-19-0012-P		Complaint received 11/14/2018, via OIG Intake Complaint received OIG Intake regarding [redacted] former President and CEO of Shreveport Federal Credit Union (Shreveport FCU) and a staff member, [redacted]), misappropriated approximately $1.572M, which may include CDFI Fund awards. NCUA also notified the CDFI Fund that Shreveport FCU was liquidated on 10/2/17. Red River Employees Federal Credit Union of Texarkana, TX purchased and assumed the majority of Shreveport FCU's assets and liabilities, which included their cash accounts, and which may have included the remaining CDFI grant funds. NCUA indicated that all legal liabilities were retained by NCUA. The CDFI Fund is in the process of working with NCUA to confirm whether or not the CDFI grant award funds were acquired.	18Dec2018	17May2019	Closed; Preliminary Inquiry Closure
CDFI-18-0095-I		Complaint received 12/5/2017, via Online Complaint Form Complainant alleges, Tax fraud and untruths by omissions on all NMTC applications submitted to the CDFI Fund. Company officers, board members and other investors using personal funds in related-entity NMTC loans to personally enrich themselves. Repeated and willful fraud waste and abuse of the NMTC program.	16Jul2018	10Jan2019	Closed; Memo to File
BFS-20-0006-P		Complaint received 10/3/2019, via OIG Intake Complaint received OIG Intake regarding allegations of [redacted] used government funds to travel to San Francisco for personal medical reasons. [redacted] scheduled a procedure to overlap with an agency meeting, at the Federal Reserve Bank, San Francisco. Prior to the meeting [redacted] announced the date of her medical procedure which coincided with her travel to San Francisco. Once in San Francisco [redacted] behavior suggested that she was present only as a tactic to claim her appearance to justify her travel to San Francisco. Her supervisor during this period was [redacted]. He approved her travel to San Francisco knowing full well that she did not have business being in attendance and that it was a cover for personal travel.	05Nov2019	10Dec2019	Closed; Preliminary Inquiry Closure
BFS-20-0003-P	Comerica Bank/Direct Express fraud	Complaint received 10/3/2019, via OIG Intake Complaint received OIG Intake regarding a call received from a Detective [redacted] in Charlotte, NC. The Detective alerted Comerica that he has received 25 to 30 police reports in the last week regarding funds stolen at Wells Fargo offsite ATMs using Direct Express cards. The Detective is with the Charlotte / Michlenburg, North Carolina police department and his phone number is [redacted]	04Nov2019	11Dec2019	Closed; Preliminary Inquiry Closure
BFS-19-0036-P		Complaint received 7/26/2019 via email The Pennsylvania State Attorney General's Office went onsite to the BFS in Philadelphia and escorted one of the employees out in handcuffs, the subject. The charge is child pornography.	29Jul2019	09Oct2019	Closed; Preliminary Inquiry Closure

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BFS-19-0019-P		Complaint received 3/14/2019, via OIG Intake Complaint regarding OIG Intake regarding a former employee [redacted] has SBU data posted on his LinkedIn page to included 16 pages of PIV presentation with options as well as EFTPS product roadmap and strategic alignment.	19Mar2019	17Apr2019	Closed; Preliminary Inquiry Closure
BFS-19-0018-P		Complaint received 3/8/2019, via OIG Intake Complaint received OIG Intake regarding several fraudulent documents received from the Federal Reserve, attempting a scam using various agencies names.	08Mar2019	17Apr2019	Closed; Preliminary Inquiry Closure
BFS-19-0014-P		Complaint received 2/4/2019, via OIG Intake Referral Number: RM-2019-001 Complaint received OIG Intake regarding a Treasury Direct account R-799-923-399, which was established fraudulently in [redacted] name. The account was established with stolen bank account, Pacific Continental Bank account number [redacted], and a 4-week bill was purchased on 11/23/2018 for $17,273.57. The security matured for $17,300.00 on 12/18/2018 and was redeemed to Wells Fargo bank account number [redacted] on 12/20/2018. Wells Fargo confirmed there are no funds left to retrieve in the account. The bank account was set up with the following information.	04Feb2019	23Apr2019	Closed; Preliminary Inquiry Closure
BFS-19-0013-P		Complaint received 12/18/2018, via OIG Inquiries Complainant alleges [redacted] We verified the check through the online verification system on the United States Treasury site. After verifying her and the check's information we cashed the check for the customer. We were just notified, over a year later, that the customer put in a claim about the check. She stated that she did not cash the check, however attached are photos of the customer cashing the check, along with a copy of her identification.	18Dec2018	27Feb2019	Closed; Preliminary Inquiry Closure
BFS-19-0001-P	ITALY BOND ASSISTANCE	Brigadier General [redacted], Italian Garda di Finanza, invited TIG SSA [redacted] to the Italian Embassy in Washington, DC to discuss an ongoing organized crime investigation in Italy. General [redacted] advised TIG that during the course of a transnational organized crime group (Bosnian) investigation for money laundering, the Garda seized US monetary notes and bonds from 3 different garages. The total face value of all notes and bonds totaled $189.7 billion. The Garda are requesting initial assistance from TIG in the form of authenticating the bonds. General [redacted] agreed to also share the suspects names for deconfliction and a potential parallel case in DC.	19Oct2018	24Jan2019	Closed; Preliminary Inquiry Closure

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BFS-18-0062-P	Unauthorized/Fraudulent ACH Payment Notification	Complaint received OIG Intake regarding RoundPoint Mortgage Servicing Corporation has identified transactions tied to a Treasury "Secret" account fraud scheme. These transaction utilized an ABA number tied to the Bureau of The Public Debt. The below information captures data points we collected in connection to ACH transfers which have been flagged as unauthorized. As such, we followed the appropriate reporting avenues as outlined in the fraud reporting section of your website.	10Jul2018	12Apr2019	Closed; Preliminary Inquiry Closure
BFS-19-0016-I		Contact by Londonderry NH Police Department. Requested assistance with an investigation involving U.S. Savings Bonds	23Oct2018	15Mar2019	Closed; ROI - Not Forwarded to Bureau
BFS-19-0015-I		Complaint received 6/20/2018, via OIG Intake Complaint received OIG Intake regarding a possible Pension fraud case for [redacted] referred to the Office of DC Pensions from BFS. , Pension Payroll received a stop payment request for 32 payments issued after death for [redacted] from August 1, 2015 – March 1, 2018. All of these retirement payments were sent electronically to Wells Fargo Bank.	18Oct2018	16Jul2019	Closed; Memo to File
BFS-19-0010-I	Direct Express CBA Program (FL)	In August 2018, MoneyGram reported that they noticed a large number of suspicious transfers from Comerica Bank (Direct Express Contractor) to their receiving agents in the Miami, Florida area, from June 2018 - August 2018. Comerica advised they received data from MoneyGram and identified more than $175,000 that was transferred from the Direct Express Cardless Benefit Access (CBA) program to the Miami area during June to August 2018. To prevent further loss, the CBA Program was terminated in August 2018. The leads in this case were limited to two fraudulent transactions for victims, [redacted] i and [redacted], who were immediately reimbursed by Comerica Bank.	02Oct2018	17Dec2019	Closed; ROI - Not Forwarded to Bureau
BFS-18-0113-I	Direct Express	On 27 March, 2018, I received a call from [redacted], SVP, Comerica Bank regarding a "refund fraud scam" where approximately 356 Direct Express cards were being utilized to accept returned merchandise refund "uploads" at various merchants in the Oklahoma City area. The DE cards were then used at various ATMs for withdrawing the funds and for various purchases. The money uploaded onto the cards were not deposits from federal government paying agencies. All of the cards being utilized are part of the Treasury Direct Express program and the [redacted] are either SSA or VA beneficiaries.	10Sep2018	14Aug2019	Closed; ROI - Not Forwarded to Bureau
BFS-18-0109-I		Complaint received 8/31/2018, via OIG Intake Complaint received OIG Intake regarding an anonymous complaint from the Culture Tag Line Survey, stating [redacted] hid 30,000 cases and 12,00 + bank errors over payment and underpayments. [redacted] reported 4K to the Treasury.	05Sep2018	23Sep2019	Closed; ROI - Response Received

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BFS-18-0108-I	TIG was contacted by the Virginia State Capital Police who were investigating a card cracking case in Richmond, VA which occurred at a Virginia Credit Union on Capital grounds. It was discovered that a U.S. Treasury routing number used by "Eagle Cash" Stored Value Card was listed on the fraudulent checks. The checks were presented to the Federal Reserve Bank, but returned. US Postal Inspection Service was also contacted due to fraudulent checks also found using the Postal Money Order routing number. [redacted] was identified as the recruiter through a local Craigslist job listing advertisement. [redacted] is seen on bank photos making the deposit of counterfeit checks into the bank account. A state search warrant was executed at [redacted] apartment at The James, a local apartment complex on July 10, 2018. Check stock, blank card stock, a credit card encoder, counterfeit checks, a litany of debit cards in other people's names, a fake ID with [redacted] picture and a Bank of America debit card in the same name were all recovered. In addition, several USPS Express mailings from several states were seized that matched up with some of the recovered debit cards. One debit card was found to be re-encoded with another number and seized. Multiple credit cards and mailing were seized in the name of [redacted], who is believed to be an identity theft victim. [redacted] phones and computer were seized during the search warrant. Over twenty-five Western Union money orders were seized, which appear to be legitimate, but are probably stolen and have been fraudulently filled out with amounts just under $1,000. USPS money orders were also recovered, several of which were for $1 and $2. Postal records indicate these money orders were used as the basis for fake checks, in that the routing number and serial number were duplicated in the creation of counterfeit checks. This is a recent trend occurring throughout New York and New Jersey. The actual loss has not been calculated until the accounts associated with the debit cards can be	21Aug2018	11Mar2019	Closed; Memo to File
BFS-18-0103-I	Complaint received OIG Intake regarding 35K in counterfeit Treasury checks with multiple leads	07Aug2018	03Dec2019	Closed; Memo to File

BFS-18-0102-I	Unknown Subject - Treasury Direct Case	On July 2, 2018, the US Attorney's Office, Western District of Texas, Austin, TX requested the investigative assistance from TIG regarding the theft of approximately $32,000 from the Bank of America (BOA) savings account of a [redacted], the oldest [redacted] who resides in Austin, TX. From February 15, 2018 to June 7, 2018, there were seven separate ACH withdraws from [redacted] n's BOA account to the US Treasury Direct to purchase US Treasury securities. Fraud Detective [redacted], Austin, TX Police Department (APD) and the Federal Bureau of Investigations (FBI), Austin, TX are the lead initiating investigators. Assistant US Attorney (AUSA) [redacted], Western District of Texas, Austin, TX, will be handling the federal prosecution of this case. The investigative request for TIG is to assist with obtaining the US Treasury Direct information to develop potential criminal leads.	07Aug2018	24May2019	Closed; Memo to File
BFS-18-0069-I	DDos Attack on Treasury.Gov	Complaint received via OIG Intake Correspondence received via OIG Intake regarding, www.clevelandfed.org was DDoSed, allegedly by an Anonymous-affiliated threat actor who took credit for that attack by posting several tweets indicating that www.clevelandfed.org was tangodown. That actor, Twitter handle [redacted], hash tagged those claims aligning the attacks with [redacted] and #[redacted]. [redacted] and [redacted] had resurfaced on December 7, 2017, via announcements through various social media platforms; a target list that included several US government sites was posted to Pastebin. At the time, from a Treasury perspective, only the IRS was listed as a target and there was no direct targeting of Fiscal Service. Outside of the Treasury/IRS, Pastebin targets in the US Government included The State Department, The White House, Social Security Administration and the public website of The Federal Reserve Board of Governors.	05Apr2018	28Oct2019	Closed; ROI - Referral to Bureau for Info Only
BFS-17-0845-I		BFS, [redacted], Document Analyst, reports that [redacted] claimed non-receipt of his VA ACH payment. Several different people are currently receiving VA payments into the account where [redacted] 's payment was sent. On the spreadsheet provided the first tab shows the names of those receiving payments. [redacted] t contacted the bank and determined that the account owner's information didn't match any of these names on the payments going into the suspect account. The account owner information is: [redacted] No phone number was provided	18Jul2017	26Mar2019	Closed; ROI - Referral to Bureau for Info Only

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BFS-17-0842-I	[redacted] converted over $61,000 of her father's SSA benefit funds to her own use without her father's knowledge and forged documents causing the withdrawal of over $300,000 of his 401-K funds. She also opened several credit card accounts in the name of her father. The victim did not become aware of the theft until he received a demand from the IRS for back taxes for the funds withdrawn from the 401-K. TOIG is providing investigative assistance at the request of SSA.	13Jul2017	11Mar2019	Closed; ROI - Not Forwarded to Bureau
BFS-17-0830-I	On October 18, 2016, TIG Jacksonville was contacted by Secured Investment Lending in Florida, regarding [redacted] attempts to pay off a mortgage with documents purporting to be issued or backed by the U.S. Treasury.	28May2017	07Nov2019	Closed; ROI - Not Forwarded to Bureau
BFS-16-2502-I	The United States Postal Inspection Service and the United States Secret Service requested the assistance of TOIG in the investigation of newly opened accounts at Capitol One, where fraudulent United States Treasury Department checks are being negotiated.	05Aug2016	14Aug2019	Closed; Memo to File
BFS-16-1737-I	Correspondence received via OIG Intake from [redacted] with the BFS regarding allegations of the above named subject being arrested and charged with felonious burglary and wanton endangerment with a firearm	11May2016	19Jul2019	Closed; ROI - Response Received

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BFS-16-1736-I	TFO [redacted] was conducting a cross check using the BSF spreadsheet of treasury payments with the Durham Police Departments Report Management System (RMS). TFO [redacted] was searching the addresses that received a large number of treasury payments to see if there were any corresponding local complaints. The Durham address [redacted] showed 71 Treasury payments sent to this address. A search through RMS showed that this location was a Tax Preparation Business owned and operated by [redacted]. On 01/04/2016 [redacted] reported that two ex-employees, [redacted] and [redacted] had possibly stolen customer's files which contained PII after they were fired (Durham Incident Report 16-000326). I ran [redacted] phone number [redacted] through RMS and it was linked to a [redacted]. [redacted] o's name was listed as a suspect in Durham IR 16-015823. This report alleged that for tax season 2014 [redacted] or [redacted] nominee deposited at least 28 treasury checks into [redacted] and the nominee's (identified by the bank as [redacted] o's baby sitter) Latino Community Credit Union accounts Some of the checks had since been reclaimed by the Department of Treasury. On 05/03/2016 [redacted] went to the Latino Community Credit Union Carborro Branch and deposited at least 11 more Treasury checks into multiple accounts not held by [redacted]. The account holders were also not the listed payee's on the account, though the addresses on the Treasury Checks were the same as the account holder that [redacted] deposited the checks into. Some of the checks had multiple payees sharing the same physical address. TFO [redacted] contacted the Bank Employee with Latino Community Credit Union, who was the reporting party, reference DPD IR 16-015823. She provided the Treasury checks that were deposited for tax season 2014 and 2015. Some of the Department Treasury Claims that were provided to the Bank Employee listed Fraud as the reason for the claim. TFO [redacted] contacted Postal Inspector [redacted] out of the	11May2016	14Aug2019 Closed; Memo to File
BFS-16-1465-I	SSA-OIG requested TOIG assistance in investigating benefits paid after the death of a SSI recipient. Death records indicate that [redacted] died on 7/11/1988 in Miami, Florida. In 2015, Social Security Administration (SSA) attempted to make personal contact with [redacted] at the address of record, [redacted]. The address was an abandoned house. Proof of death was located and SSA documented [redacted] s as deceased on their database on 10/08/2015. As a result, [redacted] s benefits were suspended. The most recent treasury checks cashed were on 10/03/14, 01/02/2015 and 02/03/2015.	11Apr2016	11Dec2019 Closed; Memo to File

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BFS-16-0963-I	Correspondence received via OIG Intake from [redacted] regarding the following: myRA Director on potential fraudulent behavior with myRA accounts. myRA is managed by Comerica and as noted they are conducting their incident assessment. Yesterday, and each of the prior two Tuesdays, we saw surges in enrollment that Google Analytics attributed to Miami, FL and the city of Grapevine, TX. The nature of these account openings - sudden, all from direct traffic, extremely high completion rate per visit, and all from computers with the same operating system and browser - was unlike anything we had seen before. It seemed possible that a couple very active VITA sites were having success. While exploring some options, [redacted] also alerted Comerica so they could check to see if the cause was fraud. Comerica is early into its investigation, but fraud does appear to the cause, with 100 accounts identified as fraudulent by various means (e.g. the name on the email not matching the name of the account opener). To date, only one of those accounts had been funded; all have now been frozen.	17Feb2016	08Oct2019	Closed; Memo to File
BFS-15-2283-I	On August 28, 2015, the U.S. Department of the Treasury (Treasury), Office of Inspector General (OIG) Office of Investigations (TOIG), received information from the U.S. Postal Inspection Service (USPIS) alleging attempted purchase of a Lexus using a fraudulent Treasury security. Specifically, the USPIS reported that on August 14, 2015, [redacted] and [redacted] contacted Sheehy Lexus of Annapolis and advised they wanted to purchase a used Lexus. On August 22, 2015, a fraudulent U.S. Treasury security in the amount of $39,574.00 was presented to Sheehy Lexus of Annapolis to purchase a Lexus. [redacted] requested the vehicle be delivered on September 1, 2015, to an address purported to be [redacted]'s new home.	10Sep2015	07Feb2019	Closed; Memo to File
BFS-15-0156-I	BFS employee [redacted] reports discovering a pattern of Social Security benefit checks being issued, altered, then re-issued. NOTE the potential relationship among this intake and Intake Numbers 15-0124 and 15-0157.	21Oct2014	29Mar2019	Closed; ROI - Not Forwarded to Bureau

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BFS-14-2367-I	TIG received this referral from the Bureau of Fiscal Services (BFS) regarding several negotiated US Treasury Checks being negotiated in the Atlanta, Georgia area with the co-signed name of '[redacted]". The Treasury checks appear to have been stolen and deposited into a Bank of America (BOA) checking account which was opened on-line by a[redacted] A possible suspect in this case is[redacted], possible half-brother to[redacted], who has been identified as cashing checks from the[redacted] BOA account. The violations applicable to this case are 18 USC 641 – Theft of government money, 18 USC 1344 Bank Fraud, 18 USC 1343 Wire Fraud, and 18 USC 1028A Aggravated Identity Theft.	28Jul2014	12Apr2019	Closed; ROI - Not Forwarded to Bureau
BFS-14-2362-I	Bureau of the Fiscal Service Document Analyst[redacted] reports the discovery of numerous fraudulent US Treasury checks, all of which appear to have been created from a single, legitimate, original US Treasury check that was issued and cashed in March of 2014. Some of the fraudulent checks show "Slan Fin" under the field for "Check Originator Info," and a search on that name comes back to a company names "SLANT/FIN."	28Jul2014	15Mar2019	Closed; ROI - Not Forwarded to Bureau
BFS-14-1542-I	This investigation was initiated under case number BFS-14-0050-P (BFS - Payment Fraud Case Development Initiative). From May - August 2013 the United States Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG) was contacted by the Bureau of the Fiscal Service (BFS [redacted], LLC located in Brownsburg, IN. Specifically, each payee submitted a "Claim Against the United States for the Proceeds of a Government Check," FMS Form 1133, stating they did not receive and negotiate a U.S. Treasury check they were expecting to receive via the U.S. mail. According to BFS records and research via the Treasury Check Information System (TCIS), the original checks were negotiated at[redacted], LLC. TOIG examined approximately 80 checks totaling $246,345.26. The examination revealed that the checks were addressed to payees residing in New York, Florida and Massachusetts.	19May2014	15Feb2019	Closed; ROI - Referral to Bureau for Info Only
BEP-14-3194-P	[redacted] appear to be working together to defraud the Bureau of Engraving of Printing (BEP) by internet using fraudulent credit card transactions. The dollar value of the 13 fraud attempts made so far is $13,7770, and actual losses to the BEP so far are $1,400. BEP Case Number BEP-SI-2014-077	19Sep2014	20Nov2019	Closed; Preliminary Inquiry Closure

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan

BEP-19-0021-I		On 22 October 2018, Maurice [redacted] Background Investigator, Bureau of Engraving and Printing, reported possible retaliation to TIG. M [redacted] reported that his Branch Manager, [redacted] asked him to withdraw a previous TIG complaint that he and three other investigators submitted to TIG in 2017. [redacted] refused to do so. Since his refusal, he has noted an increase in caseload for himself and the other investigators involved in the complaint. [redacted] reported that [redacted] has threatened the investigators with administrative paperwork and Performance Improvement Plans if they do not keep up with the work load. Additionally, [redacted] was notified on 22 Oct 2018 that the case load for the investigators had been doubled, from 4 to 8 cases per month. Currently, each of the 4 investigators averages 18 open cases. [redacted] to withdraw the TIG complaint.	06Nov2018	06May2019	Closed; ROI - Referral to Bureau for Info Only
BEP-19-0020-I		Correspondence received via OIG Intake from TOIG Counsel regarding allegations of unethical employment practices by the above named subject.	06Nov2018	06May2019	Closed; ROI - Referral to Bureau for Info Only
BEP-18-0100-I	ODNI Assistance	ODNI requested specific investigative assistance from SSA [redacted] related to an active operation. DAIGI was aware of the TS/SCI briefing and approved SSA Harding/TIG investigative participation.	07Aug2018	07Mar2019	Closed; Memo to File
BEP-18-0093-I		On 2/15/2018, TIG was contacted by [redacted], Special Agent, IRS, requesting assistance on a case involving [redacted]. SA [redacted] that she is investigating [redacted] for frivolous filings. SA [redacted] said that [redacted] is an employee at the Bureau of Engraving and Printing in Washington, DC and requested his BEP employee file.	16Jul2018	14Aug2019	Closed; Memo to File
BEP-18-0034-I		Correspondence received via OIG Intake from TOIG Counsel with allegations of potential violations of 18 U.S.C §1001 (False Statements) and/or 18 U.S.C § 1621 (Perjury).	27Dec2017	19Jul2019	Closed; ROI - Response Received
BEP-17-0824-I		Correspondence received via OIG Intake from [redacted] with the BEP regarding allegations of the above named subject committing health insurance fraud. BEP-SI-2017-015	02May2017	19Jul2019	Closed; ROI - Response Received

BEP-16-2009-I		Correspondence received via OIG Intake from [redacted] with the BEP alleging theft by [redacted], Program Manager, Office of Currency Production, of approximately $16,758 35 from the Federal Manager's Association (FMA) Post 216, BEP Union bank account at the BEP Federal Credit Union (BEP FCU). Reportedly, the FMA National President sent email letters to several BEP FMA members stating a debt to the national organization of over $16,000 as a result of unpaid dues. Several executive members of the BEP FMA contacted the BEP FCU and subsequent review of the BEP FMA account revealed multiple cash withdrawals from the account beginning in 2015 and totaling $11,017.35. In addition, at least seven checks in varying amounts were written against the BEP FMA account and payable to [redacted]r. The combined loss to the FMA Post 216 from the cash and check withdrawals is $16,758.35 - approximately six quarters of unpaid dues. [redacted]r is the individual with signatory authority on the account.	13Jun2016	20Sep2019	Closed; ROI - Referral to Bureau for Info Only
BEP-16-1449-I	THEFT OF GOVERNMENT PROPERTY - COUNTERFEIT NOTES	Correspondence received via OIG Intake from [redacted] with the BEP regarding allegations of theft of government property. BEP-SI-2016-019	08Apr2016	19Jul2019	Closed; ROI - Response Received

This document is the property of he U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordan