ACAMS® | Advancing Financial Crime Professionals Worldwide

Mitigating the Effect of Organized Crime on the U.S. Tax System

Scott Karem, CAMS

Table of Contents[1]

The views expressed in this paper are those of the author.

[1] See Appendix section for descriptions of all acronyms used within this paper.

I. Executive Summary

This paper has been written and prepared for financial crime investigators and representatives of financial institutions tasked with monitoring and mitigating money laundering activities. The objective of the paper is to educate the reader on the nature of tax fraud, explore the criminal act itself, and portray those who perpetrate it against the United States government. Ongoing efforts by the government to curtail money laundering and other criminal acts through tax activity are also examined.

II. Overview of the Problem

Sadly, it is the nature of some people to attempt to exploit gaps in our financial system to benefit themselves. Even the United States tax system is not immune to these criminals who seek to manipulate the system to their own benefit. When you consider that in 2016 alone, the IRS issued $263 billion dollars in federal refunds, you begin to see why both petty criminal and transnational crime syndicates alike make a point of focusing their efforts on manipulating the U.S. tax system.

As noted in a recent report issued by the U.S. Treasury Inspector General for Tax Administration (TIGTA), it is believed that the United States Treasury suffered a loss of more than 21 billion dollars from 2012-2017 because of stolen identity refund fraud (SIRF), which is just one of many types of tax fraud discussed in this paper.

Just how much is 21 billion dollars? According to the International Monetary Fund, 21 billion exceeds the entire nominal 2013 gross domestic product of more than 82 independent nations (International Monetary Fund, 2014). Twenty-one billion dollars would enable us to power more than 600,000 homes across the nation with solar energy (Kinnear, 2015). Those funds would allow the United States to build more than 233,333 homes through Habitat for Humanity (*FAQS for Homeownership Program Applicants, 2016,)* effectively providing housing for every homeless child in the United States (*Family Homelessness Facts, 2017).*

III. Typology of Tax Criminals

"Tax criminals" generally fall into one of two categories:

- Independent tax preparers who attempt to manipulate the system, either to extend their client base or justify increased fees to their clients. These tend to be the less sophisticated, and easier to detect, types of criminals who add extra dependents to returns or claim unwarranted tax credits (such as education credits and fuel tax credits) for their clients.
- Domestic organized crime and transnational criminal syndicates that conduct larger-scale criminal efforts, which are the focus of this paper. These groups concentrate in two efforts: compromising U.S. tax preparers and submitting "fake tax returns" using illegally obtained credentials of U.S. taxpayers.

One example of domestic organized crime is Mr. Corey Williams from Miami Gardens, Florida. According to the Department of Justice, Mr. Williams and his eight co-conspirators successfully stole more than 14 million dollars from the United States Treasury by filing fraudulent tax returns (Department of Justice, U.S. Attorney's Office, Southern District of Florida, 2014). They then laundered the stolen funds through their other businesses attempting to disguise the source of income. Mr. Williams was eventually apprehended and convicted, resulting in a sentence to serve three years in prison and repay 2 million dollars to the Treasury.

Local or national organized crime, such as Mr. Williams, normally lacks the sophistication needed to carry out tax-related crimes in a manner that is both profitable to the criminal and anonymous to the authorities. In relation to tax fraud, the primary vulnerability of domestic organized crime is that it is in fact, domestic. Locations within the geographical boundaries of the United States are subject to search and seizure by law-enforcement officials. IRS Agents can examine tax returns and review files of tax preparation offices. Records from banks and tax offices can be subpoenaed, allowing investigators to follow the money back to the primary beneficiary of the stolen funds. These factors make domestic attempts at tax fraud limited in both scope and success.

While tax crime is not a new concept, the dawning of the age of the internet has paved a way for larger, more complex means of conducting fraud. Enter the transnational criminal syndicates, who operate across multiple countries with little regard for geographical boundaries. But who are they? What type of people are they? What are the skill sets necessary to conduct these types of crimes so seamlessly?

Edward L. Federico, Jr., Director of IRS Criminal Investigations, stated before Congress on May 15, 1996, that these people show a "remarkable aptitude for sophisticated white-collar crime. They are mostly well educated, many having advanced degrees in mathematics, economics and the sciences. They are adept at functioning in a black-market economy and they are skilled at corrupting members of a targeted industry." Director Federico additionally calls these organizations "ruthless, employing threats, intimidation and violence to further their goals" (U.S. Congressional Record, 1996).

IV. Transnational Organized Crime

In an interview conducted with Brian G. Thomas, Special Agent, IRS Criminal Investigation Division and National Identity Theft Coordinator of Refund Crimes, Agent Thomas describes the problems of trying to mitigate a transnational crime organization.

Agent Thomas explains that these new criminal organizations are not a united collection of different criminal organizations working together under a common leader to accomplish a task. Previous organized crime syndicates (such as the Italian Mafia or the Chinese Triad) maintain defined roles in a hierarchy, consistent with our traditional perceptions of organized crime. Today's transnational tax criminals operate outside of a traditional leadership structure. These

leaderless, decentralized organizations have risen to thrive in the tax-fraud game because no one member of the organization is vital to the plan. Often members do not know the names or contact information of others working with them. These "cell structures" work similarly to terrorists: the identification of one cell or a member is incapable of collapsing the entire structure (*Tax Crimes*, Telephone Interview, 2017).

A new criminal organization, composed of various cell groups focused on different aspects of the crime, have united not under a single leader, but under the concept of working together for a limited duration to accomplish a single goal. Agent Thomas classifies the various cell members in into four distinct groups:

- hackers,
- preparers,
- launderers, and
- runners

HACKERS

This initial cell focuses on the acquisition of identification data for U.S. taxpayers. What bankers typically refer to as Personally Identifiable Information (PII) is the primary objective of this group. They are searching for W-2's, social security numbers, driver's license information, dates of birth, employer information – anything that can be used to submit a tax return in someone's name and provide enough reasonable information that it passes bank and IRS scrutiny.

The methodologies for acquiring the information can vary, but the more common means include:

- bribing employees of large companies or medical practices to sell their employer's list of customers or patients,
- phishing key personnel in companies to obtain data
- hacking large databases known to contain PII data.

In 2015, a transnational crime syndicate was able to penetrate the IRS itself and compromise the identity of over 300,000 U.S taxpayers. This breach alone allowed for criminals to file fraudulent tax returns that successfully obtained more than 50 million dollars in federal tax refunds.

In 2017, the hacking of the national credit bureau Equifax compromised the vital information of over 145.5 million Americans. This equates to almost 50% of the adult population in the United States. From the breach, the criminals were able to secure names, social security numbers, birth dates, home addresses, some driver's license numbers and credit card numbers for close to 209,000 citizens.

This initial layer of organized crime however does not just specialize in taxpayer data, but also in providing credentials of bank employees, tax software employees, and tax preparers themselves.

Using similar tactics, these cyber criminals will utilize social engineering or keystroke loggers to compromise account user names and passwords.

The unique aspect of this crime is that the "hackers" don't do anything with the data they have successfully stolen. Essentially, their role is limited to obtaining the data. What do they do with it? They sell it on the black market.

Having sold the information anonymously over the dark web, the hackers wash their hands of the crime. They leave very little trace information about themselves, the data, the buyers or even what data was sold. The IRS believes that these criminal organizations don't even know amongst themselves who they are selling the data to or buying it from.

Agent Thomas and his team spend countless hours in sting operations, setting up deals with various organizations that are attempting to sell compromised data. Their goal is to prevent the information to moving into the hands of the second group: the "preparers."

PREPARERS

Unlike the first cells that mastered cybercrime, social engineering, and phishing, the second cell focuses on the preparation of tax returns. To successfully accomplish this goal, the "preparers," must have a workable knowledge of the U.S. Tax Code, as well as the inner workings of tax preparers, the U.S. banking system and tax software.

Almost exclusively submitting the returns electronically, this cell attempts to generate the returns so that they avoid systematic red flags for both banks and the IRS. They specialize in knowing how to manipulate the filings to ensure that the return is profitable yet staying within tolerable ranges so as not to draw attention. A skillset all its own is using business losses, deductions, and tax credits to offset income, all the while avoiding IRS Criminal Investigations or bank Financial Intelligence Unit (FIU) personnel.

For as little as $136.00 USD per person, the fake preparer can purchase a full dossier on a compromised ID directly off the dark web. It includes everything needed to submit a fraudulent tax return - where the person works, where they live, their social security number, date of birth, etc.

LAUNDERERS

The goal of the third cell group is to move the stolen tax refunds into liquidity as quickly as possible by "laundering" them and removing all traces of their origination.
Once the return is submitted, refund proceeds are directed to the criminals through a variety of means. As with legitimate refunds, money is normally first disbursed by ACH deposits, checks, prepaid cards, and wire transfers through the U.S. banking system. As the FBI, IRS, or Department

of Justice have the means to seize the funds as part of an investigation, launderers seek to disguise the source of funds and move it out of the country as quickly as possible. They rely on a variety of means (offshore business transfers, money orders, trade-based money laundering, etc.) to sell these illegally obtained funds, often for pennies on the dollar. Once the negotiation of exchange costs have been agreed to, the money is moved by last known group, the runners.

RUNNERS

"Runners" function as agents of the ultimate beneficiaries of the funds. They utilize various monetary instruments to transport those laundered funds to their destination. Determining who these ultimate beneficiary owners are, however, remains a persistent problem.

V. Mitigating the Problem

How do you mitigate a crime that employs numerous criminal organizations spread across the globe, stretching multiple international boundaries? Further complicating the situation, how do you address an organization that only exists as a single entity for intermediate moments to exchange information and agree on terms of sale, but doesn't physically interact?

There is no "headquarters" or base of operations that we can strike. There is no singular leader controlling all operations that can be neutralized. They have no centralized location where the knowledge or skill sets are concentrated, and most importantly these cells are not reliant upon some larger, organized body to fund their operations (Brafman & Beckstrom, 2006). This developing criminal structure, or rather lack of structure, has enabled criminals to prosper in ways they never have before.

The anonymity provided by the internet has allowed criminal elements to overcome racial biases and natural distrust of each other, in many cases working with ethnic groups traditionally despised by each other.

For investigation purposes, tax-related crimes are in the jurisdiction of the Internal Revenue Service's Criminal Investigations team, commonly referred to as "IRS CI." The IRS CI has agents stationed across the globe in response to transnational organized crime. From offices in Canada, Mexico, Colombia, Panama, Barbados, the Netherlands, England, Germany, China and Australia, agents of the IRS CI work with cooperative nations to enhance and support investigations of tax-related crimes.

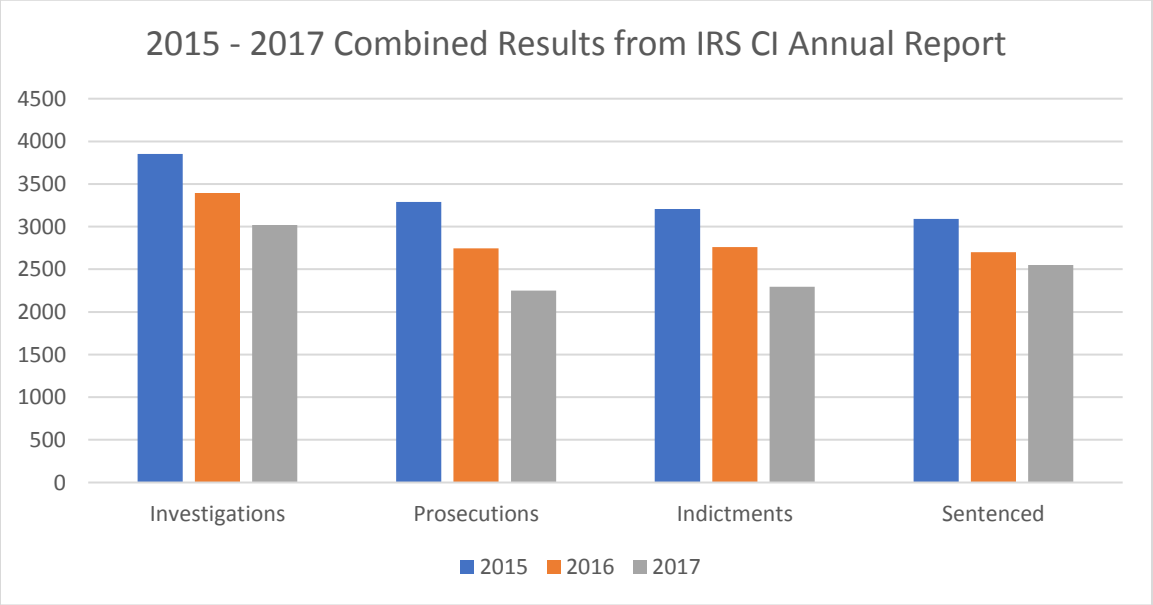
Unfortunately, not all foreign nations are sympathetic to the desire of U.S. law-enforcement personnel seeking to identify and prosecute their citizens for crimes committed against the United States. For many smaller government powers, it can be an issue of not having either the available resources or technological capabilities to track down cyber criminals.

For nations hostile towards U.S. interests, these governments may not only refuse to cooperate with investigations but may directly aid and support the criminal activity directed against the

United States. The idea of financially inuring the United States may in fact, be a state sponsored activity or objective. For example, terrorists could intentionally exploit weaknesses in the U.S. tax system to inflict significant harm on the U.S. economy. Anti-Terrorist financing experts have labeled this type of crime which is not centered on economic gain, as "not for profit money laundering."

Consider a concentrated effort by terrorist organizations to submit hundreds of thousands of fraudulent tax returns to the IRS, within a very limited amount of time. Unable to determine legitimate tax returns from fraudulent submissions, the IRS would be forced to suspend the annual tax collection and return process until it could decipher the legitimate returns. The financial impact to the United States would be catastrophic to both the federal government and states that rely upon the collected revenue. Additionally, many low-income U.S. citizens rely upon their annual tax refund as a significant source of funds.

Further complicating issues is the reduction in staffing at the Internal Revenue Service. Budgetary restrictions forced the IRS to eliminate 6,200 positions of criminal investigators and revenue agent officers between 2010 and 2016 (Internal Revenue Service, 2016). The loss of these positions alone has accounted for the IRS conducting fewer investigations and audits each year, as the sophistication and intensity of the attempted crimes against them has continued to escalate.



VI. The Role of Financial Institutions

The decreased IRS budget and resulting reductions in revenue officers and criminal investigators has caused a heavier reliance on the financial industry as a partner in mitigating tax fraud. With the increased pressure by criminal elements to defraud the U.S. Treasury, the IRS is in a position

where it must establish and strengthen relationships with banks and financial institutions to compensate for its own diminished resources.

One step taken to strengthen the bond between the federal government and the private sector has been the creation of the American Coalition for Taxpayer Rights (ACTR). ACTR is an organization comprised of representatives from tax software providers, tax preparation companies, banks, and financial settlement companies who work within the tax industry. To combat SIRF, ACTR not only serves as a "think tank" for the IRS, but also has worked to form agreements within the industry to address and report criminal activity to the IRS.

Another recent development has been the creation of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC). This online tool was designed as a means for the IRS and state taxing authorities to disseminate information between each other and financial partners in the tax industry. The intent being to mitigate exposure by quickly providing information that would allow for the government, banks or financial institutions to shutdown fraudulent behavior. The ISAC provides for a means of relaying information regarding attempts at fraud, identified trends, suspicious behavior, and I.P. addresses associated with deceptive behavior.

However, with their knowledge of the U.S. banking system and the tax industry, tax-fraud criminals have a remarkable adaptability to circumvent processes and procedures put into place specifically to curtail their activities. When focused on a barrier or obstacle, their collective abilities often allow them to stay two to three steps ahead of most financial institutions and tax preparation companies.

So, what can banking institutions and financial companies do to eliminate or at least reduce the threat of tax fraud? Awareness of the problem is the first step toward finding a meaningful solution. To those outside of the tax industry, the problem of tax fraud is virtually unknown.

While the federal government does not deny the fact that it continues to lose millions of U.S. dollars every year to transnational organized crime syndicates, it does not actively advertise the facts either. This silence works in favor of the various criminal elements that prosper in anonymity.

VII. Identifying Tax Fraud

To launder tax-fraud money, organized crime actively seeks out smaller banks, credit unions, and financial institutions where they can structure accounts in a manner that is unfamiliar to an institution's FIU. As this pattern of money laundering does not conform to standard industry practices, only those familiar with its patterns and timing can usually detect and respond to the activity before the funds are transferred or withdrawn by the runners. Most people in the traditional banking system only become aware of the problem after being served either legal

notice from an investigating body or a 314b request from another bank's FIU team attempting to piece together the puzzle left behind by the criminals.

Tax criminals are masters of identity theft, and they open depository accounts across the United States each year for the sole purpose of laundering their illicit gains. To combat this practice, banks and credit unions must adopt policies and procedures that don't just aim to meet the minimum regulatory guidelines for a Customer Identification Program (CIP), but rather establish new account opening procedures that provide enhanced due diligence for unknown account applicants.

Account dormancy is a red flag that should raise suspicion for FIU teams. Criminals posing as legitimate tax preparers within the tax industry tend to establish depository accounts long in advance of the annual tax season. To successfully register with a tax software program and a bank that specializes in monetary transactions for tax preparers, the criminal will need to provide an account number where they wish to have their "fee for their services as a tax preparer" deposited.

Establishing checking accounts across the country, the criminals utilize a process referred to as "synthetic identification," in order to create deposit accounts that will leave very few, if any clues to the owner's true identification. Synthetic Identification is a process of creating the appearance of a legitimate person by utilizing various pieces of factual information from several people, and combing that information into a new identity. When law enforcement or bank investigators begin to take a harder looker at the account data in the hopes of following the money or leading them back to the criminal, they will find that the data leads to a dead end.

The transnational crime syndicates do not value these accounts, as their objectives are not to collect the relatively few dollars they enter on each stolen refund application. The accounts are essentially only created as a means of attempting to legitimize their appearance as a true tax preparer. As such, the accounts will generally sit in a dormant status until the beginning of the tax season, which is traditionally mid-January.

The true goal from the criminal's perspective is in the tax refunds themselves, often valued anywhere from $2,000 to $10,000 dollars each. Normally, the refund proceeds will not be deposited into the same account established for their professional fees. Both the IRS and tax-refund facilitators have FIU teams that monitor for red flags, such as a preparer routing taxpayer refunds to the same account designated for their own preparation fees. As such, tax criminals need several accounts to structure their funds in a way that does not draw unwarranted attention.

Recently, the IRS discovered that some criminals will open and maintain accounts for years before ever utilizing them for their intended purpose. The intent of the criminals is to establish a history with their financial institution, in the hope that longevity with a bank will buy them some consideration before the bank begins to investigate recent deposit and transfer history.

The moment the tax season begins, the criminals are in a race against time itself. For SIRF to work, criminals need to submit a tax return to the IRS prior to the legitimate citizen doing so. As such, criminals will submit as many returns as possible, as quickly as possible, at the very beginning of the tax season. They don't know which or how many of the returns the IRS is

going to honor, nor do they know how much time they have to file before authorities and financial institutions will begin to take a closer look at their activities.

To this end, activity on these accounts will be sudden and short-lived. Within a matter of six to eight weeks, the criminals will have drained millions from the U.S. Treasury, as well as starting to drain the deposit accounts and begin the money-laundering process.

VIII. Bank and Financial Institution Response to Tax Fraud

For bank and financial institution compliance and FIU departments tasked with account monitoring and risk mitigation, the following systematic alerts are recommended:

- *25% or more growth in a business account's depository history in less than 24 months.*
- *Returned mail sent to a new client of the bank, both individuals and businesses.*
- *Low balances maintained in accounts for extended periods of time.*
- *Active accounts becoming dormant after April.*
- *Dormant accounts becoming active in January.*
- *Accounts with increased wire transfers and ACH's during the months of January – March.*
- *Business accounts changing physical address on file with the bank within 90 days of account registration.*
- *Personal and business accounts changing contact information on file with the bank within 90 days of account registration.*
- *Multiple U.S. Treasury Trace requests concerning any account.*
- *Multiple I.P. addresses used to access client accounts.*
- *Purchase of numerous monetary instruments in January – March.*
- *Disconnected telephones numbers for accounts recently opened.*
- *Contact information (such as email addresses or telephone numbers) that are repeated on multiple accounts that have no discernable connections.*
- *Accounts sharing a same mailing address yet having different owners.*

During the months of December through March, bank FIU teams are also encouraged to closely monitor press releases from the Economic Crimes Unit of the Department of Justice (DOJ). As the IRS takes legal action against those committing tax fraud or SIRF, the DOJ will release press articles citing business names and owners. This information should be used to scrub against a bank's book of business to ensure assets are quickly frozen, to prevent transfer.

With a timeline that is so narrow, bank personnel need to utilize every tool available to remain aware of trends and attempted fraud within the financial community. Staying informed of threat

actors and their various methods will enable FIU and compliance personnel to quickly respond to new threats. Joining ISAC and registering for notifications is strongly recommended for every financial institution as a way of staying informed of tax fraud attempts and potential vulnerabilities.

Additionally, banks should invest in training opportunities to keep their compliance and FIU teams up-to-date on modern techniques and efforts being employed by those committing SIRF. These criminal organizations have continued to develop and alter their tactics in a real-time manner to thwart the efforts being made by the IRS and financial institutions.

One provider of such training opportunities is the IRS itself, which holds multiple tax forums across the United States each year to better educate both tax professionals and the financial institutions working with them. Trends and concerns about fraud within the tax industry, as well as regulatory changes and requirements, are among the topics discussed at length.

Beyond the tax summit forums themselves, financial institutions should utilize the IRS Criminal Investigation teams that are stationed at all major municipalities in the United States. As these CI teams are specifically trained in financial crimes and money-laundering techniques used by criminals across the globe, they make for excellent guest speakers at regional banking events and training sessions. The IRS CI teams also teach classes available to local bank investigators, to better protect bank assets and understand the nature of tax crime. As an additional benefit, establishing contacts with the local IRS CI teams will provide a financial institution's Financial Intelligence Unit with valuable resources to address issues of suspected tax fraud or SIRF.

IX. The Future of Tax Fraud

With the ability to successfully commit a crime that nets criminal organizations millions of dollars annually while providing anonymity through remote access, this crime will continue to occur until effective controls are put into place that diminishes the value of the gain to a point where criminals will seek other, easier targets of opportunity. Combined with businesses desire to find faster ways to do business and store data on the web, the availability for criminal elements to find and capture the necessary data on tax payer's PPI is virtually limitless.

The IRS recently began employing "Dark Web Investigators," in an attempt to gain advanced knowledge of different schemes and tactics to devise effective strategies aimed at the prevention of tax fraud. Some of the things that they discovered included…

- sights offering to sell CPA account login credentials to the IRS website.
- multiple bank employee and software vendor credentials
- chatrooms dedicated to how to commit tax fraud and best practices
- stockpiled bank pre-paid and debit card inventory
- and discussions on social engineering techniques focused on identity theft

The IRS does not have the means of controlling the problem without the direct assistance of banking and financial institutions. Without FIU and compliance personnel actively working with the IRS and state taxing authorities, the United States will continue to suffer millions of dollars in loss.

X. Summary

For the last several years, the United States Treasury has been the victim of a recurring, highly orchestrated criminal effort directed at defrauding the government of millions of dollars annually. Simultaneously, those tasked with preventing this crime have continued to suffer staff reductions and government cutbacks, which have limited their effectiveness to combat this crime without direct aid from private-sector financial institutions.

Transnational crime organizations operating in multiple cells have presented the tax industry with a new model of criminal hierarchy - one that has no single leader or command structure and can be easily disassembled. The criminal organizations work across multiple national boundaries, including those hostile towards U.S. interests.

In and of themselves, the standard red flags for AML and anti-terrorist financing are not adequate to detect tax fraud activity within a bank's portfolio. The seasonality of the crime also acts to obfuscate the activity: the window of transactions is very limited, usually lasting only two to three months before funds are laundered.

Under the circumstances, the IRS will only be able to effectively mitigate this threat to the U.S. Treasury by working with the Financial Intelligence Units and Compliance Departments of banks and other financial organizations. Banks must develop enhanced CIP procedures and specific tax-fraud alerts aimed at quickly identifying threat actors, in order to prevent the reintroduction of stolen funds back into circulation. In turn, the IRS must push for statutory and system changes to share information that is vital to the effectiveness of the private-sector efforts. All parties must enhance their employee training as a tool to quickly identify and respond to tax-fraud crimes.

XI. Appendix

ACTR	American Coalition for Taxpayer Rights
AML	Anti-Money Laundering
CIP	Customer Identification Program
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FIU	Financial Intelligence Unit
IRS	Internal Revenue Service
IRS CI	Internal Revenue Service Criminal Investigations
ISAC	Information Sharing and Analysis Center
PII	Personally Identifiable Information
SIRF	Stolen Identity Refund Fraud
TIGTA	U.S. Treasury Inspector General for Tax Administration

XII. References

Brafman, O., Beckstrom, R., (2006). *The Starfish and the Spider.*

Internal Revenue Service. (2016). *Management's Discussions and Analysis*

Thomas, Brian. (2017, December 12th). *Tax Crimes.* Interview by S.Karem (telephone).

Internal Revenue Service. (2017). *IRS: Criminal Investigation 2017 Annual Report. Retrieved from: https://www.irs.gov/pub/foia/ig/ci/2017_criminal_investigation_annual%20report.pdf*

Kinnear, John. (2015). *How Much Does it Cost to Install Solar on an Average US House? Retrieved from: https://www.solarpowerauthority.com/how-much-does-it-cost-to-install-solar-on-an-average-us-house/*

Habitat for Humanity. *FAQS for Homeownership Program Applicants. Retrieved from:* http://habitatlafayette.org/homeownership/faqs-for-homeownership-program-applicants/

Greendoors, Homes Through Community Partnership. *Family Homelessness Facts. Retrieved from: http://www.greendoors.org/facts/family-homelessness.php*

International Monetary Fund. (2014). *World Economic and Financial Surveys. World Economic Outlook Database.*

Federico, Jr., Edward. (1996). *U.S. Congressional Record. Russian Organized Crime. Committee on Governmental Affairs: Permanent Subcommittee on Investigations.*

Department of Justice, U.S. Attorney's Office, Southern District of Florida. (2014). *Four Defendants Sentenced In Stolen Identity Tax Refund Scheme Resulting in Millions of Dollars in Fraudulent Activity.*