UNITED STATES DEPARTMENT OF LABOR
OFFICE OF INSPECTOR GENERAL

Investigative Advisory Report

Weaknesses Contributing to Fraud in the Unemployment Insurance Program

7/24/2015

Table of Contents

I. Introduction

The Office of Inspector General (OIG), Office of Labor Racketeering and Fraud Investigations (OLRFI), prepared this advisory report to provide the Department of Labor (DOL), Congress, and other interested parties with information related to our current investigative efforts to detect and pursue Unemployment Insurance (UI) fraud in Florida. This report also identifies program weaknesses and makes recommendations to reduce risks of fraud in the UI program. While these identified fraud indicators and recommendations are based primarily upon our investigative case work in Florida, they have potential application to other state UI programs and operations as we have found the same vulnerabilities and trends in other states. The states have a mandate to deliver UI benefits to the unemployed quickly, but they also are required to protect the integrity of the program from fraud and abuse.

DOL's Fiscal Year (FY) 2014 Agency Financial Statements estimated that national UI overpayments totaled $5.4 billion, and it is estimated that 3.19 percent of all UI benefit payments were due to fraud as defined by the individual states resulting in an estimated $1.5 billion in losses due to fraud. Over the past five years, the OIG has conducted 750 UI fraud investigations nationwide, which have resulted in 1200 criminal convictions and have identified more than $67.5 million in improper UI payments. Our investigative program has determined that UI fraud through identity theft is particularly prevalent in South Florida, where the OIG has completed 79 UI fraud investigations since 2010, resulting in 50 criminal convictions.

The OIG has identified four main fraudulent schemes related to the UI system:

1. **Single claimant benefit fraud**: An individual files a fraudulent claim for UI benefits they were not entitled to receive, using their own personal identifiers. Often these cases involve the failure to claim current employment during the application process.
2. **Multiple claimant identity theft fraud**: An individual or a group files multiple fraudulent claims for UI benefits using stolen PII data.
3. **Fictitious employer fraud**: An individual or a group creates a company existing on paper only supported by the creation of false documentation to include employee paystubs, W2s, quarterly tax reports, annual tax returns, and other documentation to give the appearance the company is legitimate. The criminals perpetrating this type of fraud file UI benefit claims using the "fictitious" company name which triggers benefits to be paid by the state.
4. **Fraudulent employer fraud**: A legitimate company that takes employees off the official payroll but continues to employ them full-time while paying them unreported cash wages for just part of the hours they work. The employees then file for UI benefits to supplement the compensation. Investigations have demonstrated that these fraudulent employer situations involve agreements between the employer and the employees to file for UI benefits.

While the OIG continues to investigate all types of UI fraud, the Florida cases highlighted in this report primarily involve multiple-claimant identity theft schemes, which have proliferated in recent years. Identity thieves and organized criminal groups exploit program weaknesses by taking advantage of the anonymity of the internet, banking privacy laws, lack of communication amongst the 53 state workforce agencies (SWAs), and existing weaknesses in SWA system capabilities. Investigative efforts have identified the following system vulnerabilities:

1. Use of pre-paid debit cards for the payment of benefits provides anonymity to individuals filing fraudulent claims makes it difficult to trace the activity and use of the funds.
2. Lack of controls to identify the use of the same internet protocol (IP) addresses;
3. Lack of controls to identify fraudulent UI claims that are filed in multiple states using the same personally identifiable information (PII);
4. The completely automated application process utilized by Florida makes it difficult to verify the identity of the person filing the claim ;
5. Unauthorized disclosure of PII information by Florida employees; and
6. Lack of consistent communication between state UI Tax and Benefit Payment divisions to verify corporate UI tax filings against UI beneficiary claims.

These system vulnerabilities along with recommendations to address them are described more fully in this report. First, we provide some background and summary of our investigative efforts in South Florida.

II. Background

The UI program is a federal-state partnership based upon federal law, but administered by state employees under state law. The program is almost totally funded by employment taxes, either federally or through the states. The Social Security Act and the Federal Unemployment Tax Act set forth broad coverage provisions, some benefit provisions, the federal tax base and rate, and administrative requirements.

Within DOL, the Employment and Training Administration (ETA) administers and oversees the UI program. However, each state designs its own UI program within the framework of federal requirements, and sets forth its own benefit and tax structure. In periods of recession, when all states are impacted by high and sustained unemployment, federally funded programs of supplemental benefits have been adopted. For example, the Emergency Unemployment Compensation program provided supplemental federal benefits totaling $1.6 billion from July 2008 through January 2014.

In Florida, the SWA responsible for oversight of the UI Program is the Florida Department of Economic Opportunity (DEO). During the period when this report was drafted, Florida paid an average weekly benefit of $240, which ranked as one of the ten lowest rates in the country (the national weekly average was $318), and the claimant in Florida could collect up to $275 per week for a period not to exceed 30 weeks, or $4,400 over the life of the claim. DEO has established a fraud detection unit that utilizes data analytics to identify trends of potentially fraudulent activity. This unit has primarily focused on detection after the fraud has been committed but recently has begun taking steps toward addressing the prevention of improper payments.

A person applies for UI through Florida's Reemployment Assistance Program by completing an online application on DEO's website, also known as "Connect." Florida uses biometric questions obtained from a third party public records search to prompt the claimant to answer several personal questions. The claimant is required to provide their name, date of birth, social security number, and other personal information. Claim approval is based on several factors, which include a name/social

security number cross match via the Social Security Administration wage database, and a Florida driver's license number/name cross match via the Florida Department of Motor Vehicles.

Once eligibility has been determined, the claimant can then file bi-weekly for benefits by self-certifying online that he/she is still unemployed and eligible for benefits. The entire application process is automated, conducted online, and provides claimants a significant degree of anonymity.

DEO authorizes the Florida Department of Financial Services (DFS) to send unemployment compensation funds to claimants in the form of either a Florida debit card mailed to the applicant, or a direct deposit into the claimant's designated bank account. In December 2014, DEO renewed its contract with a third party debit card/payroll processing vendor to operate the Florida UI debit card system, which includes distributing UI funds, processing debit card withdrawals, and maintaining debit card transaction records.

III. Investigative Efforts in South Florida

OIG receives information from multiple sources that develop into investigative cases. UI fraud referrals are frequently generated from state and local law enforcement agencies, including various municipalities located throughout the South Florida Tri-Counties area of Palm Beach, Broward, and Miami-Dade. Case development usually begins with one of the following:

- Local law enforcement agency will alert the OIG of possible UI Fraud (via evidence recovered as a result of its investigative efforts);

- Complaints concerning misuse of PII and identity theft generated by public and private sector employers, including hospitals, police departments, and city offices.

The OIG, through its partnership with DEO, has direct access to the Florida UI database. DEO, unlike some states, captures vast amounts of data related to UI claims, including IP address utilized to access each claim. DEO provides the OIG with the ability to query the UI database via IP address, bank account information, residential address, and telephone number. This direct access allows for proactive investigations and real-time data queries. Moreover, this partnership with DEO allows the OIG to work jointly with state investigators who can connect with other states, which is significant for access to state electronic data and records as the UI system is managed by state employment offices.

Florida officials have recognized the increasing threat to the UI system posed by identity theft, and they have responded by developing a new ID theft pattern recognition system and by implementing a variety of process improvements in its existing service delivery system. For example, DEO has developed and implemented an automated up-front detection system known as the Fraud Initiative and Rules Rating Engine (FIRRE) that identifies patterns of potential identity theft. Whereas traditional methods for detecting fraud in UI programs have focused on back-end processes, FIRRE has helped address the need for a front-end business process that detects identity theft before any benefits have been paid. The automated FIRRE system has enhanced Florida's ability to assemble pertinent information and data to assist the OIG with respect to cases of identity theft in the UI program. Florida's FIRRE team continues to work closely with OIG agents to improve

communication, and to share information/data in order to enhance the prosecution of those engaging in identity theft.

Additionally, DEO employs approximately 15 fraud investigators to conduct analyses of potentially fraudulent claims, with a focus on single claimant benefit fraud. However, these investigators lack the essential resources to conduct multiple claimant identity theft fraud criminal investigations without the assistance of local, state, or federal law enforcement.

The OIG often investigates UI fraud under the direction of the United States Attorney's Office for the Southern District of Florida, which is responsible for prosecuting the cases in federal court. The OIG also works in conjunction with law enforcement in other federal agencies whose programs are victimized by identity theft, such as the Internal Revenue Service (IRS), the Social Security Administration (SSA) OIG, and the United States Department of Agriculture (USDA) OIG, to ensure successful and coordinated prosecutions.

IV. Fraudulent Activity Using Personally Identifiable Information

PII that is not safeguarded or disposed of properly is at risk of abuse. PII can be misused for fraudulent purposes by individuals and various groups, including street gangs, loose-knit criminal organizations, incarcerated individuals, related family members, and employees of private or public entities having access to PII. The case examples listed here demonstrate how this information has been used to fraudulently apply for UI benefits:

- An investigation was predicated on a complaint from the North Miami Beach Police Department (NMBPD) alleging that a fraudulent UI claim had been filed using the stolen identity of an NMBPD Detective, resulting in a loss of $3,025 to the Florida UI Trust Fund. The resulting investigation uncovered a complex identity theft fraud conspiracy against the Florida UI program and ultimately led to three convictions for aggravated identity theft along with court-ordered restitution of $320,805. While the total fraud loss in this case was $320,805, the defendants attempted to steal $1.7 million from the UI Program.

  An examination of the Florida unemployment database revealed that the initial fraudulent UI claim was filed online in January 2014. Database records disclosed that three separate IP addresses were used to execute the fraudulent UI claim. A total of 510 false UI claims using stolen social security numbers were then filed by the defendants resulting in the issuance of fraudulent UI Debit Cards. Records show that two of these IP addresses were used to query the Florida UI database at least 3,100 times related to these claims. Further analysis confirmed that the IP addresses utilized in the scheme were associated with the defendants and used in support of the crime. Once the debit cards were received, the subjects withdrew the funds at local grocery store ATMs. Surveillance footage obtained from the local grocery store ATMs showed the two main defendants withdrawing funds from cards not belonging to them. In addition, 22 Florida UI debit cards with stolen identities were mailed to the subjects' listed place of residence.

- An OIG investigation revealed that from as early as December 2013 through the summer of 2014, a Florida resident filed more than 90 fraudulent UI claims from his residence using the

stolen identities of his victims, for a fraud loss totaling $236,000. The defendant was ultimately charged and convicted criminally for stealing more than $1,100,000 from the Florida UI program and from other Federal government programs, including programs administered by IRS, USDA and SSA.

During the execution of a search warrant at the defendant's residence, agents seized nearly 2,000 items containing unique identifiers of individuals as well as a credit card "skimmer," which is a device specifically designed to assist in the creation of fraudulent credit and debit cards.

An examination of the seized evidence revealed the defendant had filed fraudulent UI claims with Florida, New York, and Massachusetts. He also filed fraudulent social security claims using the stolen identities of his victims by redirecting legitimate social security claims from the intended recipients to accounts that he controlled.

The investigation resulted in the defendant entering a guilty plea to one count of use of one or more unauthorized access devices to obtain $1,000 in value or more during one calendar year, one count of possession of 15 or more unauthorized access devices, one count of possession of device making equipment, and three counts of aggravated identity theft.

- An investigation was predicated on information that employees of the Florida Highway Patrol and other Florida employees were victims of identity theft with regard to fraudulent filings for UI benefits using their stolen PII. Seized electronic evidence and digital records revealed that two Florida residents used the PII of approximately 1000 unsuspecting individuals to file almost 400 fraudulent claims. After the claims were approved, prepaid UI debit cards were sent to addresses controlled by the defendants, and used to withdraw cash at local ATMs. ATM footage was obtained from several financial institutions, showing the same subject withdrawing money using the Florida UI Debit Cards obtained in the names of the victims. The subjects of the investigation were charged and convicted of aggravated identity theft.

  The investigation revealed that the same IP address was used to file claims using all of the victims' PII, and the defendants had accessed the Florida UI system over 400 times. The OIG was able to gather sufficient evidence to execute a search warrant on a Miami, Florida, residence which resulted in the seizure of ledgers, journals, and sheets of paper containing lists of stolen PII, to include names, social security numbers, dates of birth, and driver's license information. The total loss for the identity theft scheme was determined to be more than $250,000.

- An investigation revealed that a Florida resident filed at least 77 fraudulent UI claims totaling $185,000. The identity theft victims were primarily Palm Beach County Sheriff Deputies, Town of Jupiter, Florida, police officers, and patients from various hospitals and clinics throughout the Palm Beach County area.

The perpetrator was found to be in possession of over 160 access devices which included the 77 Florida UI debit cards, three laptop computers, a credit card encoder/decoder device, and a credit card embosser. He was also found to be in possession of illegal drugs (heroin and marijuana), a bullet proof vest, and various types of ammunition, patient medical files, and several ledgers containing PII of hundreds of individuals. He entered a guilty plea to several charges, including aggravated identity theft related to the UI scheme.

- An OIG joint investigation with the North Miami Police Department disclosed that residents of two homes believed to be members of a well-documented street gang were responsible for stealing the identity of a City of North Miami police officer in order to file a fraudulent UI claim. The homes were identified by the DEO during an IP address search, which revealed that three IP addresses were used for the fraudulent UI claim and that these three IP addresses were utilized from both homes over 1,200 times to update claim information or to recertify for weekly benefits in furtherance of the scheme.

  A search warrant was executed on the two homes, which resulted in the seizure of a .32 caliber revolver, multiple Florida UI debit cards, Florida Food Stamp debit cards, reloadable prepaid debit cards, 10 computers, 14 smart phones and other electronic devices.

The OIG's South Florida office has investigated many additional cases involving criminal activity in the UI Program. Furthermore, the OIG's Semiannual Reports to Congress contain other examples of UI fraud schemes that have been prosecuted nationwide. However, OIG case statistics do not reflect the full magnitude of UI fraud for various reasons. For example, in many cases only the ringleaders and not all participants of the fraud were prosecuted because of limited investigative and prosecutorial resources. Therefore, these unindicted co-conspirators were often free to initiate their own fraud schemes. In some cases, the initial fraud losses failed to meet financial thresholds for prosecution established by the responsible U.S. Attorney's Office. These cases were declined for federal prosecution, and some were presented to district attorneys for local prosecution. However, these local offices also have resource limitations. Moreover, the OIG has limited resources to investigate UI fraud matters.

V. Improper Payments in the UI Program

The OIG would note that in addition to the fraud within the UI program, the Department faces other issues related to improper payments in the UI program. The OIG's Office of Audit recently issued an audit report titled, "Georgia Department of Labor Missed Opportunities to Detect and Recover Unemployment Insurance Overpayments" that communicated concerns to ETA regarding weaknesses and internal control issues in Georgia's UI program that led to improper payments. Similarly, in another report, "Recovery Act: Effectiveness of Pennsylvania in Detecting and Reducing Unemployment Insurance Improper Payments and Implementation of Employment and Training Administration National Strategies", OIG found that Pennsylvania did not effectively detect, reduce, or recover improper [UI] payments and the integrity of the data Pennsylvania reported to ETA could not be determined. Improper payment audits are currently being conducted in six other states. In addition, OIG's audit to determine whether DOL complied with the Improper Payments Elimination and Recovery Act and the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) found that DOL did not set or publish an FY 2014 reduction target for reducing UI improper

payments and the reported FY 2014 UI improper payment rate of 11.57 percent did not meet the IPERA requirement of "less than 10 percent". The UI benefit program's estimated annual overpayments for FY 2014 were $5.4 billion.

In response to reports such as these, ETA has taken steps to work with the SWAs in order to address improper payments in the UI system. For example, ETA has identified a number of national strategies for state implementation designed to address major root causes of UI improper payments, including fraud detection and prevention, as part of a comprehensive strategic plan. ETA partners with the National Association of State Workforce Agencies (NASWA) to advance the role of the SWAs, to invest in training and professional development, and to coordinate local, state and federal roles. ETA reports that from FY 2011-2014 they provided the SWAs with an additional $624 million in supplemental funding in an effort to support the state's implementation of the core strategies in the strategic plan and to support modernization of the states' UI systems. Of this supplemental funding, approximately $138 million was provided to states for the implementation of projects that may support the detection or prevention of UI fraud. In addition, ETA has begun partnering with the OIG to identify and prevent coordinated, multi-state fraud schemes.

As noted in ETA's response to the Pennsylvania report, one of the steps it took to address the issue of UI improper payments was the establishment of a national UI Integrity Center of Excellence (Integrity Center) through a cooperative agreement with the New York State Department of Labor. The purpose of the Integrity Center is to promote the development of innovative integrity strategies. According to ETA, the strategies and tools being developed by the Integrity Center will be made available to all states and will include the following, among others.

- Data analytics and predictive modeling methodologies to improve UI prevention and detection.
- A secure "fraud portal" for the rapid exchange of fraud information between states. This fraud portal became active in May 2014 and will be upgraded later in 2015 (Note: While the OIG agrees that fraud strategies are being exchanged, this exchange of information remains very limited and should be expanded to include case specific data between the states as noted in our recommendations.)
- Locally adaptable staff training on fraud solutions and integrity practices.
- Development of standard business requirements to be included in state UI modernization efforts that address integrity and prevention.
- Creation of a "model" plan for Benefit Payment Control operations.

According to ETA, they are currently working with the Integrity Center to build upon the existing platform for the exchange of data among the states to establish a cross-match hub for use by state UI agencies. This hub would enable cross-matching claimant information against relevant data to help prevent fraud and improper payments. This project is still being developed but would possibly align with several of the OIG recommendations listed in this report.

Findings and Recommendations

Based on our investigations in South Florida and elsewhere, we have identified systemic weaknesses that make the UI program more susceptible to fraudulent activity. Those weaknesses, and our recommendations to address them, are presented below.

1. Finding - The use of pre-paid debit cards: The use of non-state issued pre-paid debit cards available through retail outlets provides anonymity to those who are submitting fraudulent claims and makes it difficult to trace the activity and use of the funds. These pre-paid cards provide the consumer with a routing number and account number in the same fashion as a traditional bank account. The difficulty presented with prepaid debit cards is that many of them are issued by non-standard banks that do not require the same account establishment safeguards, such as obtaining and verifying identification documents in person. The subjects use automated teller machines at several financial institutions to withdraw funds using various types of debit cards obtained in the names of the victims.

   More importantly, the SWAs have no way of identifying whether the account number/routing number provided to them during the application process belongs to a standard bank or to a pre-paid debit card account. In some cases, identification of the account holders has only been successful by tracing the account to the original retailer who sold the prepaid debit card, obtaining retailer surveillance media, and hoping the subject is known to local law enforcement. Access to these debit card records often requires investigators to subpoena various financial institutions to review the fraudulent transactions of a single claimant only to find that there is no identifiable account holder information. This presents an internal control challenge for the SWAs as there is no way to verify that the person receiving the funds is the intended beneficiary.

   The OIG and DEO have worked closely to identify some of the pre-paid debit cards by identifying routing numbers that have been used by criminal groups to commit fraud. As a result of this collaboration, those identified routing numbers belonging to the pre-paid debit cards can no longer be used to receive UI funds in Florida. However, due to the rate at which new cards are made available, it is difficult for the OIG or DEO to identify them all. In addition, some traditional banks use the same routing number for pre-paid debit cards and traditional bank accounts, making it difficult to shut down that particular routing number.

   Recommendation: ETA should recommend that SWAs require that all claims be paid by physical check, direct deposited into a checking or savings account, or deposited on a debit card issued by state approved vendors, similar to the debit cards used by the USDA-Supplemental Nutrition Assistance Program (SNAP). These cards provide for account holder verification. USDA reports that the use of these debit cards has contributed to a significant reduction in benefit fraud over the last decade.

Recommendation: ETA should consider a policy that requires all states to grant the OIG unfettered access to their UI records. This would eliminate the need for subpoenaing UI debit card transaction records by contractually providing OIG access to the following: 1) complete UI records, and 2) UI debit card transaction records, similar to the access given to USDA for the SNAP program. The USDA program uses an electronic "audit trail" from debit card transactions to identify suspicious activity. Their anti-fraud system monitors electronic transaction activity and identifies suspicious activity for analysis and investigation. Currently, some of the SWAs, to include NY, require a subpoena before OIG is permitted access to UI records. Other states, like VA for example, require the OIG to pay a service fee for access to the records. These added steps are cumbersome and often cause unnecessary delays in OIG criminal investigations.

2. Finding - IP Addresses: Most claims are filed and managed 100 percent online, making it difficult for DEO to verify the identity of the claimant. The use of anonymous IP addresses (masked or without personal identifiers), mobile internet hotspots that have no identified owner, and the use of stolen internet connections, make it difficult to identify the correct identity of the individual filing a claim. The ability to file claims from public locations such as local coffee shops and hotels that offer free internet access also provides a higher degree of anonymity to the filer. ETA noted that many SWAs have begun blocking claims filed using IP addresses that originate from outside of the United States. The OIG suggests that this practice be encouraged with all 53 SWAs.

   The Integrity Center has already started working on data analytics projects that identify multiple claims from the same IP addresses and has begun sharing that information with all 53 SWAs. However, the data is only being supplied by 16 of the 53 SWAs and still has limited application. The OIG suggests that all 53 SWAs supply IP address data to the Integrity Center for cross matching between the states.

   These same data analytics projects could also be applied to collecting and analyzing data related to common separating employers, common claimant addresses, common post office boxes, common PII information and common bank accounts. Our investigations have demonstrated that commonalities in the above referenced data are very often strong indicators of fraudulent activity. Some SWAs currently collect and share this information. For example, Hawaii collects IP information in a usable data format that can be shared with other SWAs and law enforcement. ETA has noted that some SWAs have contracted with private data analytics companies to conduct fraud detection projects. These data analytics projects are based on individual state requirements and are not uniform amongst the states. The UI Integrity Center of Excellence's strategic plan calls for the development of business requirements to be included in state UI modernization plans. A national data analytics program would be a helpful tool in the detection and prevention of UI Fraud nationwide and would align with the Integrity Center's strategic goal.

   Recommendation: ETA should recommend that SWAs develop a plan to identify multiple claims that originate from the same IP addresses, or from IP addresses from outside the United States, to minimize threats and fraud. In addition, consideration should be given to

development of a database where all 53 SWAs will begin recording and sharing incoming IP addresses using a central data collection and exchange point, where common IP addresses can be researched using data analytics to identify and share information concerning potential fraud rings.

Recommendation: In order to reduce claimant anonymity, ETA should recommend that SWAs consider additional verification within 30 days of initial filing if the claim was filed from an identified anonymous IP address or with other fraud indicators. Current regulations permit the SWAs to request photo IDs to validate identity. States should suspend payment of benefits and conduct further investigation if requested information is not provided or the information provided does not resolve identity concerns.

3. Finding - Claims filed in multiple states: Investigations found defendants had filed fraudulent UI claims in multiple states during the same timeframe using the same PII data, which is not permissible. In addition, our investigations have revealed that these claims filed in multiple states contained much of the same information to include: IP addresses, claimants' addresses, prior employment history, post office boxes and bank accounts.

   Recommendation: ETA should recommend that SWAs provide all identified fraudulent claimant information into a shared database that can be queried to identify the filing of fraudulent claims against multiple states. One possibility would be to use the existing ETA Fraud Portal, which would make the portal a powerful tool in UI Fraud detection for the SWAs.

4. Finding - Automated Application Process: In most instances, once the claimant enters their PII into the Florida UI system, the system auto-populates the application with the claimant's employment history, making it easier for the claimant to complete the application process. In a recent OIG investigation, a cooperating defendant verified that this procedure assisted him in completing fraudulent applications. This procedure provides all of the past employment history, which may not have been known to fraudulent claimants, thereby allowing them to complete the claim and facilitate improper payments. The employment information self-generated by the system also provides the subjects with the valuable information needed to file fraudulent IRS tax refund returns, which we became aware of during our joint investigations with IRS.

   As discussed above, the claimant is also required to answer several biometric questions that are automatically generated by "Connect" through a contract with a third party records vendor. However, OIG investigations have found that there are many different online third party record providers from which this information can be purchased. Bank records obtained during investigations have demonstrated that subjects purchased information from these types of providers.

Recommendation: ETA should recommend that SWAs remove auto-populating of any data, specifically employer data, in their systems. Claimants should be required to fill out all employer contact information correctly and completely.

5. Finding - Employee Integrity: OIG investigations have identified that, in some situations, state employees abused their positions of trust by misusing confidential PII to enable UI fraud.

   Recommendation: ETA should work with all SWAs to strengthen existing systematic audit controls to track access to PII information. This access data can then be used by investigators and/or a data analytics team to determine if an employee accessed an account that they should not have accessed, or to identify trends of employee access connected to fraudulent claims.

   Recommendation: ETA should recommend that SWAs conduct pre-employment and periodic background and credit checks for those employees with direct access to PII data related to the UI program, and take appropriate actions with regards to employees who have negative results related to periodic suitability investigations.

6. Finding - Verification of Tax Data: Through our investigative communications with the Florida Department of Revenue, which maintains the Florida unemployment employer tax records, as well as our communications with DEO, we learned that there is a lack of consistent or structured communication between these agencies to verify corporate UI tax filings against UI beneficiary claims. This in turn makes it difficult to identify fictitious employer schemes where fraud rings create companies to conceal their fraudulent activity should anyone try to contact the employer for verification. While the Department of Revenue shares their employer tax information with DEO, the data is difficult to manipulate in order to conduct proactive research on potential fictitious employer schemes or to identify fraudulent separating employers.

   ETA has identified some states that demonstrate effective communication between the tax operations and the benefit operations. For example, Utah has established a program that identifies and flags as potential fraud cases employers where 30% or more of all employees have filed for UI benefits and where one of a list of additional fraud indicators exists. In addition, Utah conducts weekly data cross matches to find fictitious employers and identity theft cases.

   Recommendation: ETA should identify best practices and strategies for communication between tax operations and benefit operations, and work with the SWAs to adopt them.

   Recommendation: ETA should consider as a part of their national strategy the establishment of a data analytics project that focuses on delinquent employers who have failed to pay unemployment taxes and cross match that data against existing UI claims. These projects should be consistent among the SWAs to ensure that data can be shared between the SWAs through the use of the fraud portal or the UI Integrity Center of Excellence.

VI. Conclusion

Our investigative casework clearly demonstrates that the UI program is vulnerable to fraud and abuse. As detailed in this report, identity thieves and organized criminal groups have found ways to exploit program weaknesses, and the OIG views this fraud as a significant threat and financial attack on the UI program. Further, there is a very tangible and deleterious impact on those persons whose identities have been compromised. The OIG recognizes that ETA has been working with the SWAs to develop the UI Integrity Center of Excellence. However, the deficiencies which we have identified in Section VI suggest that more can be done by ETA working with the states to strengthen the integrity of the UI program.

VII. Acronyms and Abbreviations

AIGI	Assistant Inspector General for Investigations
DEO	Florida Department of Economic Opportunity
DFS	Florida Department of Financial Services
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
ETA	Employment and Training Administration
EUC	Emergency Unemployment Compensation
FUTA	Federal Unemployment Tax Act
FY	Fiscal Year
IG	Inspector General
IP	Internet Protocol
IPERIA	Improper Payments Elimination and Recovery Improvement Act of 2012
IRS	Internal Revenue Service
NDNH	National Directory of New Hires
NMBPD	North Miami Beach Police Department
OIG	Office of Inspector General
PBSO	Palm Beach County Sheriff's Office
PII	Personal Identifiable Information
PO	Post Office
SNAP	Supplemental Nutrition Assistance Program
SRT	Special Response Team
SSA	Social Security Administration
UI	Unemployment Insurance
USDA	United States Department of Agriculture

U.S. Department of Labor

Assistant Secretary for
Employment and Training
Washington, D.C. 20210

JUL 2 2 2015

MEMORANDUM FOR: LESTER FERNANDEZ
Assistant Inspector General
For Labor Racketeering and Fraud Investigations

FROM: PORTIA WU
Assistant Secretary
Employment and Training Administration

SUBJECT: Investigative Advisory Report – Weaknesses Contributing to Fraud in the Unemployment Insurance Program
Tracking No. 50-15-001-03-315

Thank you for the opportunity to respond to the final draft Investigative Advisory Report – Weaknesses Contributing to Fraud in the Unemployment Insurance Program. The Employment and Training Administration (ETA) and its Office of Unemployment Insurance (OUI) share your concerns about the escalating sophistication of fraud schemes being perpetrated against the Unemployment Insurance (UI) program and recognize the need to accelerate state adoption of new strategies to improve prevention and detection of fraud schemes. We are pleased to report that we have already begun efforts to address these complex issues and we look forward to a continued partnership with the Department of Labor's Office of the Inspector General (OIG) in these efforts.

Your report focuses heavily on Florida and we agree that there has been significant learning from the recent fraud schemes that emanated from Florida but impacted a significant number of other states. It increased our understanding of types and scope of more recent fraud schemes and it has already spurred new actions on ETA's part and on the part of states.

We appreciate your acknowledgement of ETA's existing work with states on integrity issues overall, including our focus on fraud. ETA already works to coordinate information sharing about identified fraud schemes with our regional offices and the state workforce agencies. This effort is providing the regions and states with characteristics of fraudulent claims, such as Internet Protocol (IP) addresses identified as part of these schemes. States are using these characteristics to detect additional questionable claims and refer them for investigation.

Also, as you mentioned, ETA has funded and participates in the UI Integrity Center of Excellence (Integrity Center) which is actively working on a number of initiatives targeted at fraud prevention and detection, including, but not limited to, the following:

1) **Data Analytics.** The Integrity Center is conducting a pilot project with two states that is designed to demonstrate the use of data analytics and predictive modeling tailored to state specific needs with the goal of making the tool available to all states that may need it.

Some states already have data analytics initiatives underway and our goal is to leverage the learning and tools from the pilot as well as expose states to other best practices from the implementation of data analytics.

2) **Integrity Center Portal.** One of the first accomplishments of the Integrity Center was to launch an Internet portal to enable states to share information on new fraud schemes as well as best practices on all program integrity activities. The Center is continuing to expand the functionality of this portal to include the immediate and secure exchange of information related to fraud schemes and to promote its use by states.

3) **Centralized Data Hub for States.** The Integrity Center is currently scoping a pilot project to determine the feasibility of creating a centralized data hub for a wide array of data sources to support state prevention, detection, and recovery of UI improper payments and to prevent and detect fraud using the Interstate Connection Network (ICON). The vision for this data hub is to make available both public and private sector data sources that are most valuable to state UI agencies and to explore how to overlay data analytic capabilities that will help states prioritize the information received from cross matches with the data. In addition, the data hub may also become a repository for states to share information on claimants and employers who have been found to engage in fraudulent behavior.

4) **Continuous Collection and Dissemination of State Best Practices.** A critical function carried out by the Integrity Center is to capture and disseminate state best practices, including practices associated with addressing fraud. States are actively working to identify new solutions to address fraud and the Integrity Center provides a way to quickly share those solutions and support adoption by additional states.

I would also call to your attention the recent meeting we convened with your assistance to bring together similar Federal benefit programs and their respective OIGs to start a dialogue on opportunities to share information on program fraud and strategies to address it across programs. We expect to enable broader fraud information sharing across agencies and create opportunities to learn about new innovations in addressing fraud from our sister agencies.

Turning to the specific recommendations in your report, below are ETA's responses which are numbered in accordance with the report findings and recommendations:

1) **Recommendation:** ETA should recommend that State Workforce Agencies (SWAs) require that all claims be paid by physical check, directed deposited into a checking or savings account, or deposited on a debit card issued by state approved vendors.

   Response: ETA agrees that non-state issued pre-paid debit cards present a challenge for tracking fraudulent collection of UI benefits and is committed to working with states to identify solutions to address this issue. States currently have significant flexibility with regard to overall administration of the federal/state unemployment insurance program, including how they deliver the benefits. ETA currently has no statutory authority to require states to use specific benefit delivery processes. It would require Federal

legislation to create such a mandate. However, ETA is happy to make appropriate recommendations to states on this issue. This is a complex issue and ETA could benefit from additional input on appropriate state strategies. We would welcome the opportunity to work with the OIG to further research options for states to prevent claimants' use of non-state issued pre-paid debit cards to commit fraud.

Recommendation: ETA should consider a policy that requires all states to grant the OIG unfettered access to their UI records.

Response: ETA understands that the OIG has an interest in accessing state UI data to support fraud detection and OIG investigations. However, disclosure of confidential UI data is subject to both Federal and state laws. ETA will work with the Solicitor's Office to conduct a legal analysis of what is feasible under current law and what may require legislation.

2) **Recommendation:** ETA should recommend that SWAs develop a plan to identify multiple claims that originate from the same IP addresses, or from IP addresses from outside the United States, to minimize threats and fraud. In addition, consideration should be given to development of a database where all 53 SWAs will begin recording and sharing incoming IP addresses using a central data collection and exchange point, where common IP addresses can be researched using data analytics to identify and share information on concerning potential fraud rings.

   Response: ETA agrees that increasing state sharing of fraudulent IP addresses is important and will continue to work with the Integrity Center and states to implement these strategies. As noted above, ETA is already supporting state strategies related to identifying IP addresses associated with fraud schemes. Several states currently block claims for benefits from foreign IP addresses and ETA has held this practice up and recommended it to all states. In addition, states were provided the opportunity to apply for supplemental funding to implement this strategy in the last two supplemental funding opportunities (UI Program Letters No. 13-14 and No. 16-15).

3) **Recommendation:** ETA should recommend that SWAs provide all identified fraudulent claimant information into a shared database that can be queried to identify the filing of fraudulent claims in multiple states.

   Response: ETA agrees that sharing fraudulent claimant and/or employer information among states is desirable. However, there is currently no existing infrastructure to enable such sharing and development of such infrastructure will require both ETA and state resources. This strategy has complexities that arise from the fact that the identity being used to commit the fraud may have been stolen and the individual whose identity has been identified as fraudulent is actually a victim. This strategy also involves personal identifying information (PII) which brings with it the need for significant security requirements. ETA will work through the Integrity Center to further explore this strategy as one that may be facilitated through the creation of the data hub described above.

4) **Recommendation:** ETA should recommend that SWAs remove auto-populating of any data, specifically employer data, in their systems. Claimants should be required to fill out all employer contact information correctly and completely.

   Response: ETA agrees with this recommendation and will recommend that states cease auto-populating data in their systems.

5) **Recommendation:** ETA should work with all SWAs to strengthen existing systematic audit controls to track access to PII information

   Response: ETA agrees with this recommendation and will work with states to improve audit controls relative to access to PII information.

   Recommendation: ETA should recommend that SWAs conduct pre-employment and periodic background and credit checks for those employees with direct access to PII data related to the UI program, and take appropriate actions with regards to employees who have negative results related to periodic suitability investigations.

   Response: ETA agrees that it is reasonable to encourage states to implement strategies that ensure staff handling PII information are not at risk for misusing the information. ETA will work through the Integrity Center to identify current state strategies and to explore additional strategies that may be effective and appropriate to address this recommendation.

6) **Recommendation:** ETA should identify best practices and strategies for communication between tax operations and benefit operations, and work with the SWAs to adopt them.

   Response: ETA agrees that states can benefit from strong communications and collaboration among benefit and tax operations to support prevention and detection of UI fraud. ETA will collaborate with the Integrity Center to capture and disseminate best practices and encourage state adoption of those practices.

   Recommendation: ETA should consider, as a part of its national strategy, the establishment of a data analytics project that focuses on delinquent employers who have failed to pay unemployment taxes and cross match that data against existing UI claims.

   Response: ETA agrees that many UI fraud schemes involve fictitious employers and/or employer collusion. ETA is committed to working with the Integrity Center and states to explore how data analytics and predictive modeling can better identify employers that may be fraudulent actors, including exploring whether employers with tax delinquencies are more associated with potential fraud.

In summary, ETA appreciates the OIG's interest and commitment to working with us to improve the prevention and detection of fraud in the UI program and looks forward to our continued collaboration.

If you have questions regarding this response, please contact Diane Easterling, ETA's liaison with the OIG, at easterling.diane@dol.gov or (202) 693-2625.