U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Field Hearing on Social Security Numbers and Child Identity Theft

Antonio Puente
Special Agent
Office of the Inspector General, Social Security Administration

September 1, 2011

Good afternoon, Chairman Johnson and members of the Subcommittee. It is a pleasure to appear before you, and I thank you for the invitation to testify today. My name is Antonio Puente, and I am a Special Agent with the Social Security Administration (SSA) Office of the Inspector General (OIG), working out of the OIG's Dallas Field Division, in the San Antonio, Texas office. Today, we are discussing ways to improve protection of the Social Security number (SSN) and to guard against misuse and child identity theft.

The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year. Identity theft is prevalent in Texas for several reasons:

- There are about 1.65 million unauthorized immigrants in Texas—the second-largest population in the United States behind California—according to 2010 estimates from the Pew Hispanic Center.
- Unauthorized immigrants in Texas, and across the United States, seek others' personal information like names, birth dates, and SSNs for many reasons, such as obtaining official identification documents, gaining employment, applying for government benefits, and opening financial accounts.
- Unauthorized immigrants seeking others' personal information—as well as all other identity thieves—have access to counterfeit identity documents, often through purchase from fraudulent vendors that have stolen or fabricated personal information.

To illustrate these issues, I want to detail a recent identity theft case that SSA OIG and several Federal, State, and local law enforcement agencies investigated near Austin, Texas.

In late 2010, the Pflugerville, Texas Police Department investigated a certified nurse's aide (CNA) at the Pflugerville Nursing Home and Rehabilitation Center, after a patient allegedly experienced a sexual assault. The investigation revealed the CNA gained employment at the nursing home by using a counterfeit Social Security card and Permanent Resident Alien Card. Pflugerville police took this information to the nursing home's corporate officials, who then conducted an internal audit of all of the CNAs employed at the Pflugerville nursing home. Corporate officials identified 43 employees who may have submitted suspect documents during the employment application process.

Pflugerville police then contacted SSA OIG and requested assistance in verifying the SSNs of the 43 nursing home employees in question. Our search revealed that 28 of the 43 SSNs did not match, meaning there were inconsistencies in names, birth dates, or SSNs. The searches found that seven of the SSNs were assigned to children, and five were assigned to deceased individuals. Moreover, SSA never assigned six of the unmatched SSNs.

Verification of the nursing home employees' alien registration numbers by the U.S. Department of Homeland Security (DHS) also revealed the numbers were valid, but they were not assigned to the individuals in this investigation. Analysis of the individuals' CNA license applications showed each individual provided a fraudulent or counterfeit Social Security card and Permanent Alien Card to the State of Texas.

We presented this information—documentation from the nursing home's corporate office, and results of the SSN verifications—to the U.S. Attorney's Office (USAO) for the Western District of Texas, Austin Division. The USAO opened criminal cases on all 28 individuals in November 2010. SSA OIG obtained arrest warrants, and a multi-agency arrest operation resulted in the arrest of 23 individuals, with five arrest warrants remaining open and active.

A Federal Grand Jury indicted the 23 individuals for SSN misuse and fraud and misuse of visas, permits and other documents. All 23 pleaded guilty to buying a Social Security card; they were each sentenced in June to time served and ordered to pay a $100 special assessment. DHS has identified all of the individuals in this investigation as Mexican nationals unlawfully present in the United States. DHS has processed the individuals, and each is currently in deportation and removal proceedings, with hearings pending.

SSN misuse and identity theft investigations may be criminally prosecuted, but they are more likely to be accepted for prosecution when they involve multiple or vulnerable victims with significant financial losses. According to the *Social Security Act*, criminal SSN misuse includes:

- Willfully, knowingly, and with intent to deceive, using an SSN assigned on the basis of false information provided by the individual or another person;
- With intent to deceive, falsely representing a number to be the SSN assigned to a person;
- Knowingly altering a Social Security card; buying or selling a card that is, or purports to be, a Social Security card; counterfeiting a Social Security card, or possessing a card or counterfeit card with intent to sell or alter it;
- Disclosing, using, or compelling the disclosure of the SSN of any person in violation of the law.

These are felonies punishable by imprisonment for up to five years and/or fines of up to $250,000. These penalties are separate from violations of other applicable statutes, such as immigration laws.

During this investigation, the USAO's victim-witness coordinator notified the victims that their SSNs were misused, but the victims in this instance were fortunate that the investigation did not reveal any specific harm. Our office worked with the USAO to provide this notification to victims; we also provided information on how they could review their credit reports and contact their respective local Social Security offices for additional assistance.

SSA has processes in place to assist victims of identity theft. SSA personnel will work with identity theft victims to:

- Review the earnings reported using their SSNs, and correct the record if necessary;
- Take an application for a replacement card, if the victim's Social Security card has been lost or stolen;
- Provide information to victims about the FTC-recommended actions a victim should take to remedy the effects of identity theft; and provide SSA information on identity theft, SSNs and Social Security cards;
- Take an application for a new, different SSN if the victim requests one and is able to provide evidence that he or she is being harmed by the misuse;
- Develop criminal aspects of the case if evidence shows fraud, and refer the case to OIG.

The individuals identified in our investigation purchased their counterfeit Social Security cards and Resident Alien cards from several unknown document vendors located in and around the Austin area within the last year. The vendors reportedly told the individuals that the SSNs on the counterfeit cards were randomly selected. None of the card purchasers provided the vendors' names or contact information to law enforcement.

Vendors that sell SSNs obtain the information through various means, including stealing identity documents or personal information, or carrying out online data breaches. Specific methods can include

simple dumpster diving, pick-pocketing, or stealing postal mail; or more recent schemes such as phishing and pre-texting—posing by e-mail or phone as someone who legitimately needs the information. In some cases, vendors simply randomly select nine numbers, because they are not concerned with the SSN's legitimacy; they simply want to produce a counterfeit Social Security card, so the purchaser is able to fill out a job application or open a credit account.

Before this investigation, the nursing home's corporate office did not use the DHS E-Verify system to determine the eligibility of their employees to work in the United States. SSA OIG met with the corporate council and provided contact information for DHS as well as instructions for using E-Verify.

Also, while this investigation involved a very small sample, we found that of 28 misused SSNs identified, 25 percent belonged to children. At a recent FTC-sponsored forum on child identity theft, experts discussed a trend wherein identity thieves are targeting cyber attacks on schools and pediatric centers to obtain children's SSNs. Therefore, it has become critical for parents to protect their child's number as they would their own, performing regular earnings records and credit checks on the child's number. In 2010, about 8 percent of identity theft complaints came from victims 19 and younger, according to the FTC.

In conclusion, the Pflugerville nursing home case was an excellent example of cooperation among Federal, State, and local law enforcement in an effort to curb SSN misuse and identity theft. The case highlights some of the current identity theft issues in Texas and across the United States. There is a critical need for U.S. employers to remain vigilant and to verify each employee's status as legally permitted to work in the United States using a correct and legitimate SSN. The case also illustrates the threat of undocumented vendors selling counterfeit SSNs and Social Security cards, either by stealing legitimate SSNs, in some cases from young children, or by selecting numbers at random.

I want to thank the many law enforcement agencies that contributed to the investigation: the United States Attorney's Office for the Western District of Texas, Austin Division; U.S. Department of Health and Human Services OIG; Federal Bureau of Investigation; U.S. DHS Immigration and Customs Enforcement (ICE) Homeland Security Investigations and ICE Enforcement and Removal Operations; Texas Attorney General Medicaid Fraud Control Unit; and the Pflugerville Police Department. We in SSA OIG are pleased to see this case successfully resolved, and we remain committed to pursuing similar SSN misuse and identity theft cases throughout the State of Texas and across the country.

Thank you again for the invitation to testify. I am happy to answer any questions.