

U.S. Immigration and Customs Enforcement

STATEMENT

OF

ALYSA D. ERICHS SPECIAL AGENT IN CHARGE HOMELAND SECURITY INVESTIGATIONS MIAMI

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

REGARDING A HEARING ON

"CATCH ME IF YOU CAN: THE IRS IMPERSONATION SCAM AND WHAT IS BEING DONE ABOUT IT"

BEFORE THE

UNITED STATES SENATE SPECIAL COMMITTEE ON AGING

WEDNESDAY, APRIL 15, 2015 – 1:30 PM 562 DIRKSEN SENATE OFFICE BUILDING

INTRODUCTION

Chairman Collins, Ranking Member McCaskill, and distinguished members of the Committee:

On behalf of Secretary Johnson and Director Saldaña, thank you for the opportunity to appear before you today to discuss the efforts of U.S. Immigration and Customs Enforcement (ICE) to combat cross-border financial crimes such as consumer fraud scams.

ICE has the most expansive investigative authority and the largest force of criminal investigators in the Department of Homeland Security (DHS). With more than 20,000 employees and a budget of nearly \$6 billion, ICE has nearly 6,700 special agents assigned to more than 200 cities throughout the United States and 63 offices in 46 countries worldwide. Working with our other federal and international partners, ICE disrupts and dismantles transnational criminal networks by targeting the illicit pathways and organizations that engage in cross-border crime.

Homeland Security Investigations (HSI)

HSI is the investigative arm of ICE and conducts criminal investigations to protect the United States against terrorism and other criminal activity that threaten public safety and national security, and to bring to justice those seeking to exploit our customs and immigration laws worldwide. Notably, in fiscal year (FY) 2014, HSI investigations led to the disruption or dismantlement of 520 transnational criminal organizations. HSI made more than 32,000 criminal arrests and seized more than 2.3 million pounds of narcotics, 20,000 weapons, and \$720 million in currency and monetary instruments.

In its investigative capacity, HSI enforces more than 400 federal laws and regulations, with jurisdiction over the investigation of crimes with a nexus to the U.S. border or functional border. To accomplish its mission, HSI focuses its broad investigative authority on three operational priorities – border security, public safety and counterterrorism/national security. HSI investigates customs and immigration crimes, including transnational criminal organizations (TCOs) engaged in illicit activity related to export enforcement, human rights violations, narcotics, weapons and contraband smuggling, financial crimes, cybercrimes and child exploitation, human smuggling and human trafficking, intellectual property theft and trade fraud, transnational gangs, and immigration document and benefit fraud.

Fraud Schemes

There are many fraud schemes such as tax fraud schemes, bogus lottery and sweepstake schemes, phony investment pitches and business opportunities, and others which are growing increasingly sophisticated and international in scope. According to the U.S. Federal Trade Commission in March 2013, consumers lose hundreds of millions of dollars annually to cross-border financial crimes such as telemarketing fraud. Sadly, in many cases the loss represents the victims' entire life savings.

Perpetrators will victimize consumers of all ages, backgrounds and income levels, but the elderly are disproportionately targeted. Perpetrators take advantage of the fact that elderly Americans may have cash reserves or other assets to spend on these deceptive offers. A survey conducted in 2013 by the American Association of Retired Persons found that 90 percent of respondents reported awareness of consumer fraud, yet two-thirds said it was hard to spot fraud when it is happening. The survey also shows that elderly victims find it difficult to terminate

telephone conversations, even when they say they are not interested in continuing a conversation. Also, the elderly may be reluctant to report the incident for fear of losing financial independence should their families discover the fraud. Scammers will even try to use a variety of schemes, especially when they find a potentially vulnerable victim including those who may suffer from a cognitive impairment.

I understand the Committee is particularly interested in the scenario where the perpetrator impersonates a person of legal authority, such as an Internal Revenue Service (IRS) Agent, attempting to collect a tax or a fee, that the victim allegedly owes the government. The scammer claims a tax or fee must be paid immediately over the phone or a warrant will be issued for the victim's arrest, or more urgently, the warrant has been issued and will be served following the call if the victim does not pay the amount requested immediately. However, HSI investigates several other types of fraud schemes as well.

One of the most common types of telemarketing fraud is the lottery or sweepstakes scam. These schemes typically involve fraudulent telemarketers identifying themselves as a lawyer, customs official, or lottery company representative to a potential victim. In a typical fraud scenario, potential victims are led to believe that they have won an international multimilliondollar sweepstakes. The scammers tell the victims that in order to receive their winnings, the victim will need to pay an advance fee. This fee is usually described as a tax, insurance payment or customs duty that must be paid to release the winnings. The victims are instructed to send the funds via mail, courier, or wire transfer. The winnings are invariably non-existent and the scammers steal the victims' money.

Scammers will also try to impersonate a relative, as perpetrators can often find names of a vulnerable senior's loved one listed in an obituary. The impersonator will claim to be a loved

one, state that he/she has been arrested in Canada for driving under the influence and needs money to pay a fine to avoid being sent to jail. A similar scenario is a perpetrator impersonating a senior's relative claiming, while on travel, they were injured and had to be hospitalized so they need money immediately for the medical treatment until their insurance can be processed to cover their medical care.

As you can see from just this small sample of scenarios, the stories are quite varied but the results are the same. Scammers will utilize any scenario to convince the victim to transfer his or her money to the perpetrator over the phone.

Most of these scammers are articulate and can often involve a variety of partners to defraud the victim over the course of a period of time, a strategy that serves to increase the complexity of the matter and leads to greater credibility to the scheme. Scammers have also been known to repeatedly bombard their victims with non-stop calls, even employing verbal abuse to coerce victims to comply. Intimidated, confused and exhausted, victims yield to the scammer's demands.

Impersonating IRS and Government Officials

HSI, along with other law enforcement agencies, has been investigating a growing and pervasive scam where scammers, frequently operating overseas, will contact American victims. The scammers pretend to work for government agencies, like the IRS, and they will falsely and fraudulently tell victims that they have a tax lien, or have committed some crime and must pay a fine. HSI's primary focus is the underlying fraud and the related money laundering. In all instances, HSI seeks to ensure full investigative collaboration with the appropriate investigative

entities from the agency that is being impersonated. In cases where an IRS agent is being impersonated, HSI collaborates with the Treasury Inspector General for Tax Administration.

The scammers will then tell the victims to make a payment to the government agency using a third-party money transfer system. The scammers will work with partners in the U.S. to obtain and launder the fraudulent proceeds, before attempting to transfer them out of the country. Law enforcement estimates that this is a multi-million dollar scam.

For example, we have seen scammers call individuals and claim to work with a local "Attorney General's" office. The scammer tells the victim that he/she will be charged with fraud, but that the victim could pay some sum of money to avoid being charged. Victims will agree to pay all or part of the amount demanded, and then the scammers instruct them to purchase a third-party money transfer card, and later provide them with information on the card. At that point, the scammers will have all the information they need to collect the fraudulent proceeds. The scammers have even obliged requests for tracking or confirmation numbers, and provided addresses for real government offices.

The money is then frequently transferred onto a pre-paid debit card, which can be used to purchase money orders at a variety of reputable establishments. U.S.-based co-conspirators for the scammers purchase these pre-paid debit cards, load them up with fraudulent funds, and then purchase money orders at supermarkets and other locations. The money orders can then be deposited into bank accounts the scammers control. In one case, scammers stated they purchased approximately \$5,000 in money orders each day, six days a week. Over the course of nine months, investigators estimated these scammers facilitated the transfer of \$900,000 from victims to scammers operating overseas.

West African Transnational Criminal Organizations- Romance Scams

Over the past several years HSI investigators have also seen an increase in fraud scams against the elderly via West African Fraud syndicates, mainly through a scheme known as the Romance Scam. West African Fraud organizations strategically target recently widowed seniors due to their vulnerabilities and access to cash. The Romance Scams target the elderly via online dating sites, establishing a virtual relationship with them, and utilizing fictitious profiles. The organizations exploit the relationship by portraying an emergency and requests the victim "loan" them \$5,000 to \$10,000. If the victim attempts to discontinue their relationship with the organization, the scammer exploits the victim's embarrassment and attempts to employ them in conducting other fraudulent schemes, on behalf of the scammer, such as the cashing of fraudulent checks. If the victim contacts the scammer to tell him/her that they have been approached by law enforcement, the scammer in turn tells the victim that he/she is the police and they should continue working together.

Interagency Partnerships

In order to combat criminal organizations involved in romance scams, telemarketing, and government impersonation fraud schemes, HSI works closely with other DHS law enforcement components such as the U.S. Secret Service, U.S. Customs and Border Protection, the DHS Office of the Inspector General and the Office for Civil Rights and Civil Liberties, as well as with the Federal Bureau of Investigation, the U.S. Postal Inspection Service, the Treasury Inspector General for Tax Administration, and the IRS. In addition, because of the multijurisdictional and international challenges that these TCOs pose to U.S. law enforcement, operating in many U.S. states and in countries such as Canada, Nigeria, Australia and India, HSI and its partner agencies have teamed up with DOJ to produce a more coordinated enforcement

and prosecution effort. This effort involves law enforcement working jointly with prosecutors, our foreign law enforcement partners, and the financial industry. This, in turn, has led to a more collaborative law enforcement effort that will eventually lead to the disruption and dismantlement of these TCOs that are victimizing our senior citizens.

Cornerstone – Forging Partnerships with the Private Sector

The HSI Cornerstone Outreach Initiative was launched in July 2003 and has grown into a robust, unparalleled financial outreach program. The success of the program is due in large part to the personalized collaboration with financial industry partners.

HSI recognizes that our financial industry partners have critical and actionable information related to illicit financial activity and are the first line of defense against money laundering. ICE Special Agents also serve as subject matter experts in money laundering methods involving fraudulent schemes. Bringing together the expertise from government and non-government spaces is the core of the Cornerstone Program in addressing financial vulnerabilities exploited by TCOs.

HSI is actively engaging the financial industry's anti-money laundering executives to forge one-on-one partnerships, developing and sharing red flag indicators based on review of the financial flows relating to consumer fraud activity. These partnerships enable ICE to leverage the banking industry, money service businesses, and prepaid card issuers for intelligence and cooperation in investigating and prosecuting TCOs.

Payment Mechanisms

As the earlier example in my testimony demonstrates, the TCOs involved in these fraudulent schemes want to receive illicit proceeds quickly and anonymously. As I tried to show, one emerging method employed by scammers is to use money mules from the United States. Money mules serve as money consolidation points in the U.S., and eventually laundering illicit proceeds out of the U.S. to the source countries where the TCOs are based. The choice payment methods for the TCOs are money service businesses and prepaid cards. Money service businesses allow them to receive funds through structured payments made under reportable currency thresholds. Prepaid cards allow for the instantaneous transfer of funds. The funds can be loaded by a victim virtually on the internet or at a retail location. The prepaid card can also be mailed to the organization for use outside of the United States. Currently, U.S. law does not define prepaid cards as monetary instruments, limiting law enforcement's ability to investigate illicit prepaid cards encountered at any U.S. Border.

CONCLUSION

Thank you again for the opportunity to appear before you today to discuss our efforts to combat consumer fraud scams which target our seniors, particularly those schemes where perpetrators try to impersonate IRS or other government officials to attempt to collect a made-up tax or fee. We look forward to working with you to reduce the potential for these criminals to identify susceptible targets, move their illicit funds, and address the issue of the penalties for these crimes meeting the seriousness of the harm they inflict on our senior citizens.

I would be pleased to address any questions you have at this time.