COMBATING ORGANIZED RETAIL CRIME—THE ROLE OF FEDERAL LAW ENFORCEMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

NOVEMBER 5, 2009

Serial No. 111–96

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

53–231 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
LUIS V. GUTIERREZ, Illinois
TAMMY BALDWIN, Wisconsin
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SANCHEZ, California
DEBBIE WASSERMAN SCHULTZ, Florida
DANIEL MAFFEI, New York

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM ROONEY, Florida
GREGG HARPER, Mississippi

PERRY APELBAUM, *Staff Director and Chief Counsel*
SEAN MCLAUGHLIN, *Minority Chief of Staff and General Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

ROBERT C. "BOBBY" SCOTT, Virginia, *Chairman*

PEDRO PIERLUISI, Puerto Rico
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
ANTHONY D. WEINER, New York
DEBBIE WASSERMAN SCHULTZ, Florida
MIKE QUIGLEY, Illinois

LOUIE GOHMERT, Texas
TED POE, Texas
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TOM ROONEY, Florida

BOBBY VASSAR, *Chief Counsel*
CAROLINE LYNCH, *Minority Counsel*

CONTENTS

NOVEMBER 5, 2009

Page

OPENING STATEMENTS

The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1
The Honorable Louie Gohmert, a Representative in Congress from the State of Texas, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 4
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary 5
The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Member, Subcommittee on Crime, Terrorism, and Homeland Security 7

WITNESSES

Mr. David J. Johnson, Section Chief, Violent Crime Section, Criminal Investigative Division, Federal Bureau of Investigation, Washington, DC
Oral Testimony 9
Prepared Statement 11
Ms. Janice Ayala, Deputy Assistant Director, Office of Investigations, United States Immigration and Customs Enforcement (ICE), Washington, DC
Oral Testimony 14
Prepared Statement 16
Mr. John R. Large, Special Agent in Charge, Criminal Investigations Division, United States Secret Service, Washington, DC
Oral Testimony 24
Prepared Statement 26
Mr. Zane M. Hill, Deputy Chief Postal Inspector, United States Postal Inspection Service, Washington, DC
Oral Testimony 34
Prepared Statement 36

APPENDIX

Material Submitted for the Hearing Record 47

COMBATING ORGANIZED RETAIL CRIME—THE ROLE OF FEDERAL LAW ENFORCEMENT

THURSDAY, NOVEMBER 5, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:31 a.m., in room 2141, Rayburn House Office Building, the Honorable Robert C. "Bobby" Scott (Chairman of the Subcommittee) presiding.

Present: Representatives Scott, Conyers, Lofgren, Quigley, Gohmert, Smith, and Goodlatte.

Staff present: (Majority) Bobby Vassar, Subcommittee Chief Counsel; Joe Graupensperger, Counsel; Veronica Eligan, Professional Staff Member; and (Minority) Robert Woldt, FBI Detailee.

Mr. SCOTT. Good morning. First we have an announcement to make: Because the full Committee markup from yesterday unexpectedly went over to today the hearing previously scheduled for noon on python snakes in Florida, which was originally scheduled for noon today, will be moved to 10 o'clock tomorrow morning.

Subcommittee will now come to order, and I am pleased to welcome you today to the hearing before the Subcommittee on Crime, Terrorism, and Homeland Security about the role of Federal law enforcement in combating organized retail crime.

Theft from retail establishments has long been a problem, but the problem gradually grew beyond simple, isolated incidences of shoplifting and burglary into something more complex. It wasn't until the 1980's that organized retail crime was recognized as a phenomenon, but the problem has continued to grow in volume, sophistication, and scope.

What has emerged are sophisticated, multilevel criminal organizations that steal large amounts of high-value products, focusing on small and easily resalable items, and then resell the goods through a variety of means, including flea markets, smaller stores, and increasingly over the Internet. Sales over the Internet have evolved to a point where they have become a new crime phenomenon referred to as "eFencing."

Organized retail crime is now a significant issue that has been—that has a big impact on the retail industry and our economy. According to the National Retail Federation there are now more than 1.6 million retail establishments in the United States with more than 24 million employees—approximately 20 percent of our work-

force—with sales of $4.6 trillion in 2008. Clearly protecting the health of retail businesses is extremely important.

And so it impacts everyone from the big box retailers to the small, independent stores. I have seen estimates that organized retail crime amounts to between $30 billion and $42 billion a year in losses.

This type of crime obviously has a direct impact on those from whom the items are stolen. They have fewer items in their inventory to sell and their profits suffer. To make up for it they must often pass along the burden to consumers in the form of higher prices.

Organized retail crime also harms the public in several other ways. To try to stop the thefts retailers engage in a variety of loss prevention efforts that costs them money and also results in higher prices for consumers. Lost sales to retailers also means loss of tax revenue for State and local government who are under extreme financial pressure in this economy.

Consumers are also at risk when retail crime organizations steal consumable products, especially the over-the-counter drug items and infant formulas, two popular items for organized retail theft rings. In many cases, after the merchandise has been stolen the products are not stored properly, which can render the products ineffective or even dangerous.

Retailers spend a lot of time and resources trying to prevent thefts and catch thieves, but it is becoming increasingly more difficult to do so. I commend the efforts of retailers who normally compete with each other on a daily basis, but they come together and learn from each other about how to deal with emerging threats in retail crime by sharing their collective wisdom on loss prevention.

While there have been significant disagreements between retailers and online marketplaces about how to best deal with thieves selling stolen goods using Internet sites such as auction sites or direct sale sites, some progress has been made. Accordingly, I encourage retailers and online marketplaces to continue to work together with law enforcement in catching and prosecuting organized retail thieves and to try to forge a more cooperative effort to identify and weed out those bad actors to stop and prevent them from selling stolen goods over the Internet.

I have introduced legislation on this problem of eFencing, and I will certainly continue to work with retailers, Internet market representatives, and law enforcement to do all we can to bring about effective solutions to the problem. Today the Subcommittee will focus on the role of the Federal law enforcement agencies.

Organized retail crime poses some difficult challenges to law enforcement. For example, theft rings often operate in multiple jurisdictions, making it impossible for any one State or local law enforcement agency to investigate and prosecute them effectively.

The Internet has also made it much more—much easier for some such sellers to access a national or even international market of buyers of stolen goods. In addition, the proceeds of these crimes are often laundered with tremendous sophistication.

These types of cases can be very resource-intensive. Even in the best of circumstances there are many—circumstances where it is

obvious that items offered for sale are stolen, and it may be the case that a seller is offering store brand-named items in large qualities—quantities—and at prices substantially lower than retail value.

However, even these relatively obvious cases can be very expensive and time-consuming for law enforcement to investigate and bring charges. Large amounts of resources are needed to engage in the necessary investigatory techniques such as stakeouts, sting operations, development of sources, financial analysis, video and audio surveillance, undercover meetings, wiretaps, and PIN registers.

These cases are even more difficult and more expensive to investigate if it is not obvious which retailer the goods were stolen from, and this is why it is important that law enforcement agencies have sufficient resources to take down these types of criminal enterprises.

The FBI has indicated how serious the problem of organized retail crime is. When speaking about organized theft and reselling of infant formula Director Mueller, of the FBI, said that "in a number of our cases the subject of these investigations are suspected of providing financial support to terrorist organizations."

I believe we have taken some positive steps in law enforcement in this area in recent years. In 2006 the FBI created its organized retail crime task force. A year later the FBI collaborated with the National Retail Federation and the Retail Industry Leaders Association to launch the Law Enforcement Retail Partnership Network, called LERPnet—thank you, LERPnet—which is a secure national database that allows retailers to share information with each other about incidences of organized retail crime and other types of crime.

ICE has launched a pilot program to get a better understanding of the problem and how to combat it. The Secret Service uses capabilities with respect to investigating activities such as credit card fraud, which are often tied to organized retail crime schemes. The U.S. postal inspectors take action against those involved in this type of crime who ship stolen products through the mail.

And I am pleased that our law enforcement agencies have the investigative expertise and jurisdiction to investigate many of the aspects of organized retail crime. And while State and local law enforcement agencies are on the front line of combating local incidences of these crimes, the Federal law enforcement is uniquely positioned to take down large investigated multi-state operations.

So if we can learn from these agencies what Congress can do to better equip them to do this type of crime—to pursue this kind of crime more vigorously and to coordinate their efforts with specific purpose of breaking up these crime rings. To this end, we see the beginning of a dialogue with and between these agencies and the businesses affected with the goal of enhancing Federal enforcement efforts in this area.

We will hear from law enforcement—federal law enforcement agencies today about their experiences with organized retail crime and what they are doing to investigate it, and I look forward to their testimony.

I will now recognize the Ranking Member of the Subcommittee, the gentleman from Texas, Judge Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman, and thank you for holding this hearing on such an important issue on organized retail crime. While I was still on the bench as a judge handling felonies, I recall the law enforcement talking to be about this new thing of people going in and stealing massive amounts of baby formula, and at first they weren't really sure where this was all going but then it became very clear.

This problem of organized retail crime is growing. It involves the theft of large quantities of retail merchandise. Organized retail crime is not necessarily a high-profile crime, but it certainly is a high-volume crime and a very costly one.

Unlike shoplifters or small-time thieves who steal for their own personal use, organized retail thieves steal merchandise in order to sell it back into the marketplace. What is worse, apparently much of the proceeds are often used to fund even more devastating crimes.

These criminals typically target merchandise that can be easily stolen and easily resold. The stolen items range, of course, from low-cost products such as razor blades, baby formula, or batteries, to expensive products that include electronics or appliances. Organized retail thieves, commonly referred to as boosters, will sell the stolen merchandise at flea markets, pawn shops, swap meets, and increasingly on the Internet.

According to the FBI, organized retail crime accounts for between $30 billion and $37 billion in losses annually. The Coalition Against Organized Retail Crime estimates that States with sales tax annually suffer over $1.5 billion in lost tax revenue due to organized retail theft.

In 2005 Congress directed the attorney general and the FBI, in consultation with the retail community, to establish a task force to combat organized retail crime and create a national database or clearinghouse to track and identify organized retail crimes across the country. The result of this legislation is the Law Enforcement retail Partnership Network, LERPnet—you have got to like that—which was launched in 2006. This national database allows retailers to share information about suspected theft with each other and law enforcement officials.

In addition, the FBI has created major theft task forces to identify and target multijurisdictional and organized retail crime rings. There are currently nine FBI-led major theft task forces staffed by FBI agents and State and local law enforcement officers located in FBI field offices across the country.

I am looking forward to learning more about not only the FBI's efforts to combat organized retail crime but also the efforts of the U.S. Secret Service, U.S. Immigration and Customs Enforcement, and U.S. Postal Inspection Service. I understand the work of these agencies has led to the prosecution of numerous perpetrators of organized retail crime.

For example, in 2008 the U.S. Secret Service investigated a case involving four thieves who used fraudulent credit cards to purchase more than $1 million of Target and Walmart gift cards. This led

to the arrest of all four thieves, three of whom are serving Federal sentences ranging from 44 months to 84 months in prison.

The restaurant servers from whom the four conspiring thieves obtained credit card numbers were also arrested. After getting credit card numbers from the restaurant the four primary conspirators created fraudulent credit cards to purchase Target and Walmart gift cards, which were then resold online at eBay and in person to acquaintances. The eBay seller was arrested in addition to the restaurant servers and the four conspiring thieves.

Several bills have been introduced in this Congress to prohibit organized retail theft, and in particular eFencing—the sale of stolen goods at online auction sites. Auction sites such as eBay and other online marketplaces, including Amazon.com, have expressed concerns about these bills.

I appreciate the desire to craft legislation that addresses innovative criminal conduct, but I am wary of legislation that deviates from using the knowing or intentional mental states that are commonly used in criminal offenses—because criminal offenses are intended to impose penalties against those who consciously act to commit a crime or consciously act in furtherance of a crime. Another alternative to the use of intent would be massive civil fines to get people's attention even if they do not act with criminal intent.

With these concerns in mind, I look forward to hearing from our witnesses and getting their perspectives on the Federal agencies enforcing the law today. We need to learn more and do all we can to investigate and prosecute perpetrators of organized retail crime and those who assist them, and we need everyone—retailers, online marketplaces, and law enforcement—working together in the most efficient way possible toward this end.

With that I yield back the balance of my time.

Mr. SCOTT. Thank you.

The Ranking Member of the full Committee, Mr. Smith, from Texas.

Mr. SMITH. Thank you, Mr. Chairman, and thank you and the Ranking Member for having this hearing today on an especially important subject. And I hope as a natural outgrowth of this hearing we will, as a Subcommittee and a full Committee, be able to enact legislation that will address some of the problems that we are going to hear about today.

Organized retail crime affects millions of Americans each year. Unfortunately, Federal law enforcement agencies lack adequate resources to combat this growing crime.

Organized retail crime involves the theft of large quantities of merchandise from retail stores by an organized criminal organization. Unlike shoplifters, these thieves steal the merchandise with the intention of selling it back into the marketplace.

According to FBI estimates, organized retail crime rings cost businesses more than $30 billion a year in losses. A 2007 organized retail crime survey by the National Retail Federation found that 79 percent of the retailers polled were victims of organized retail crime.

For these reasons the FBI established an organized retail crime initiative to identify and dismantle large, multijurisdictional orga-

nized retail crime rings. This initiative included the formation of a National Retail Federation-FBI Intelligence Network. The network is intended to establish an effective means of sharing organized retail crime information and to discuss trends as they relate to specific sectors and regions of the retail market and to identify and target the more sophisticated criminal enterprises.

Congress should increase funding to the FBI's organized retail crime initiative. That is why last month I sent a letter to the Chairman and the Ranking Member of the Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies requesting that Congress authorize additional funds to help the FBI fight organized retail crime.

The FBI is not the only Federal agency pursuing organized retail crime. The U.S. Secret Service, U.S. Immigration and Customs Enforcement, and the U.S. Postal Inspection Service also combat these criminal organizations.

For example, the Postal Inspection Service and Immigration and Customs Enforcement investigation worked last year to uncover a refund scheme involving the use of counterfeit serial numbers to obtain new video game hardware. The wrongfully obtained hardware was then sold on eBay for the gang's profit.

The cost to Target and other retailers, including Walmart, of just this one scam was a half a million dollars. The thieves' activities were tracked in seven States before they were arrested and prosecuted, thanks to the good work of these Federal agencies here today.

Examples like this one are encouraging, but there is still too little prosecution of organized retail crime. State felony thresholds, which require that the value of the stolen goods must amount to $500—or $1,000 in some States—for the offense to be a felony are too high to prosecute organized retail crime effectively. The Federal threshold for prosecution for the crime of transportation of stolen goods and interstate commerce is even higher, as the value of the stolen goods must exceed $5,000 to trigger Federal criminal liability.

To help Federal agencies combat the phenomenon of organized retail crime more effectively, earlier this week I introduced H.R. 4011, the Organized Retail Crime Prevention and Enforcement Act of 2009. This bill reduced the Federal felony threshold from $5,000 to $1,000 for the sale of stolen goods through online marketplaces. The bill also provides that "the attorney general shall establish multijurisdictional task forces to initiate investigations of organized retail theft and dismantle organized retail theft criminal enterprises in the six United States district court districts with the greatest incidence of organized retail theft."

Mr. Chairman, I think this bill is a good start, and I look forward to hearing from our witnesses what more we can do to combat the serious problem of organized retail crime in America. And you don't need to answer this question now, but I would hope that a piece of legislation—perhaps the one I introduced—could be the subject of a bipartisan effort to try to address this serious problem of organized retail crime.

And I will yield back.

Mr. SCOTT. Thank you. And I will answer. I have introduced a bill on this subject, but I don't have any pride in authorship. We should consider everything that can address this problem, so that will certainly take place.

We usually ask other Members to put their statements in the record, but my colleague from Virginia has been hard-working on this issue, and I understand you have a statement to make.

Mr. GOODLATTE. Well, Mr. Chairman, thank you very much for your kind words and for allowing me to give this statement. I want to thank you especially for the hard work that you have put into this issue over a few years now, and I hope we do make progress and look forward to working with you and Mr. Gohmert and Mr. Smith on that.

Organized retail crime, or ORC, is a huge and growing problem in the United States. Retailers estimate their losses from ORC to be in the tens of billions of dollars. ORC groups target anything from everyday household commodities, to health products, to baby formula that can be easily sold through flea markets, swap meets, shady storefront operations, and through online marketplaces.

Thieves often travel from retail store to retail store stealing relatively small amounts of goods from each store but cumulatively stealing significant amounts of goods. Once stolen, these products are sold back to fencing operations, which can dilute, alter, and repackage the goods and then resell them, sometimes back to the same stores from which the products were originally stolen.

When a product does not travel through the authorized channels of distribution there is an increased potential that the product has been altered, diluted, reproduced, and/or repackaged. These so-called diverted products pose significant health risk to the public, especially the diverted medications and food products.

Diverted products also cause considerable financial losses for legitimate manufacturers and retailers. Ultimately the consumers bear the brunt of these losses as retail establishments are forced to raise prices to cover the additional cost of security and theft prevention measures.

Even more troubling is where the money is going. Our witnesses today will explain that oftentimes this money is being sent overseas and is being used to fund international organized crime and even terrorist organizations.

At the State level, organized retail theft crimes are normally prosecuted under State shoplifting statutes as mere misdemeanors. As a result, the thieves that participate in organized retail theft rings typically receive the same punishment as common shoplifters. The thieves who are convicted usually see very limited jail time or are placed on probation.

I believe that the punishment does not fit the crime in these situations. Mere slaps on the wrist of these criminals has practically no deterrent effect. In addition, the low-level criminals actually stealing these goods from the shelves are easily replaced by the criminal organization's higher-level coordinators.

During my 7 years working on ways to combat ORC, I found that the Federal law enforcement community believed it had adequate Federal laws to prosecute ORC crimes but that communication and

coordination among outside groups and State and local law enforcement was lacking.

In order to improve the communications and intelligence-sharing between industry and law enforcement, I offered an amendment to the Department of Justice Reauthorization bill back in 2005 that created a Federal definition of organized retail theft crimes and directed the FBI to contribute to the construction of a national database housed in the private sector where retail establishments as well as Federal, State, and local law enforcement could compile evidence on specific organized retail theft crimes to aid investigations and prosecutions.

I was my hope that this database, which has now become the current LERPnet, would help to put the pieces together to show the organized and multistate nature of these crimes as well as provide important evidence for prosecution. I am pleased to see in the written testimony today that law enforcement believes this initiative is proving helpful.

In addition, in December of 2003 the FBI established an organized retail theft initiative to combat this growing problem. While this is a good start, I look forward to hearing the FBI's plans to bolster its efforts to combat these crimes which are increasing in frequency, posing greater threats to consumers, and resulting in greater losses to businesses.

Recent busts have shown how widespread this problem truly is. We need more arrests like this to effectively combat organized retail theft.

I am also pleased to hear about ICE's ORC pilot program, and I hope that this program will lead to more information about how these crime rings operate and how we can more effectively shut them down. I continue to look for new ways to help law enforcement combat ORC.

In fact, I joined with Ranking Member Smith this week to introduce H.R. 4011, which would lower certain monetary thresholds in the criminal law and give law enforcement more resources to combat these crimes. I urge the Members of this Subcommittee to consider this approach when contemplating legislation in this area.

And, Mr. Chairman, I look forward to continuing to work with you to find additional approaches to solve this problem.

One concern I have had is that we need to make sure that legitimate online businesses, like eBay and craigslist and a whole host of other online businesses, are accommodated in the sense that we need to find ways where they can cooperation with law enforcement without having legislative requirements that are too intrusive in terms of their business model relative to others who are a part of the overall network that is a problem for organized retail crime.

These entities want to be helpful, want to cooperate with law enforcement, and I think we can find ways to enhance their cooperation without making them subject to unreasonable requests for information that would make it difficult for them to continue to operate.

Thank you, Mr. Chairman, for holding this important hearing.

Mr. SCOTT. Thank you.

Our first panelist will be David Johnson, section chief of the violent crime section of the Criminal Investigation Division of the FBI.

He began his FBI career at the San Jose resident agency serving on the Violent Crime Squad and the Mexican Drug Trafficking Organization Squad. He was promoted to supervisory special agent of the Asian Organized Crime Squad. He also served as assistant special agent in charge for the San Francisco division and the unit chief of the Crimes Against Children Unit at FBI headquarters.

Our second panelist will be Janice Ayala, assistant director of the Office of Investigations of ICE. In this position she has management oversight of all investigative programs and initiatives for the Office of Investigations. Previously she held several positions—several other positions at ICE, including deputy assistant director for Financial, Narcotics, and Public Safety Division. In that position she had direct oversight of the financial, narcotics, and national gang programs conducted by ICE throughout the United States.

The third panelist will be John Large, special agent in charge of the Criminal Investigative Division of the U.S. Secret Service. In this position he is responsible for planning, reviewing, and coordinating all domestic and international criminal investigations involving counterfeiting, financial crimes, and electronic crimes.

Our fourth panelist will be Zane Hill, deputy chief inspector of the United States Postal Inspection Service. In this position he is directly responsible for the Inspection Service's criminal investigation programs in the areas of fraud, money laundering, and asset forfeiture.

Each of our witnesses' written statements will be entered into the record in its entirety. I will ask each witness to summarize his or her testimony in 5 minutes or less, and I ask you to help stay within the time there is a lighting device at the table that will start green, turn yellow when there is 1 minute left, and turn red when your time has expired.

Mr. Johnson?

TESTIMONY OF DAVID J. JOHNSON, SECTION CHIEF, VIOLENT CRIME SECTION, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC

Mr. JOHNSON. Good morning, Chairman Scott, Ranking Member Gohmert——

Mr. SCOTT. Could you move your microphone a little closer to you?

Mr. JOHNSON. Absolutely.

Mr. SCOTT. These don't work very well.

Mr. JOHNSON [continuing]. Of the Subcommittee. I appreciate the opportunity to testify before you today on the FBI's efforts to combat organized retail theft in the United States. Each year organized retail theft is responsible for significant economic losses to retailers, which are then passed on to the American consumer. While it is difficult to pinpoint the exact annual dollar loss caused by this crime problem, retailers estimate all crimes where they are victims result in billions of dollars in losses.

The tax revenue losses attributable to organized retail theft also negatively impact States. In the face of the current economic downturn, the hundreds of millions of dollars in revenue losses to our States can be considered catastrophic.

The unsuspecting consumer also faces potential health and safety risks from legitimate products which may have been mishandled by the criminal enterprises who stole them for resale to consumer. Also of concern for the FBI in particular is the potential nexus between organized retail theft syndicates and other criminal enterprises.

There are many challenges on the road to combating organized retail theft. Lack of available resources to State and local police departments who have the primary responsibility for investigating most retail crimes is a huge hurdle. Sharing information between public and private enterprise is another.

As with other forms of criminal enterprises, there is a loose hierarchy within organized retail theft groups. Specifically, these groups utilize low-level boosters—those who actually steal the merchandise—and higher-level fencers, who frequently coordinate booster thefts. Often these boosters are illegal immigrants working off a debt or individuals suffering from some form of addiction. If these low-level boosters are removed from the criminal enterprise others will simply step in to take their place.

These criminal groups are also particularly nimble, able to easily change their appearance, alter their method of operation, and particularly adept and circumventing security devices and procedures. Further, the wide reach of the Internet and online auction sites has provided global marketplaces for savvy entrepreneurs and, not surprisingly, criminal enterprises.

Sophisticated organized retail theft groups can best be dismantled—a coordinated and cooperative effort between law enforcement and the retail industry. In December 2003 the FBI establish an organized retail theft initiative to identify and disrupt multijurisdictional groups using Federal statutes such as conspiracy, interstate transportation of stolen property, and money laundering.

Additionally, Congress passed legislation signed by the President in January of 2006 that required the attorney general and the FBI, in consultation with the retail community, to build a system for information-sharing, to include intelligence as well as lessons learned and best practices regarding organized retail theft. As a result, the Law Enforcement Retail Partnership Network, or LERPnet, was subsequently launched in 2007.

The database, which is housed and run by the private sector, allows retail members to track and identify organized retail theft via a secure Web portal. To date, nearly 100,000 retail locations are included in the data, which represents $1.17 trillion in retail sales or nearly 25 percent of all retail sales in 1 year.

With a recently signed memorandum of understanding, law enforcement will also be able to access LERPnet via the FBI's Law Enforcement Online to search reported incidents and track organized retail theft throughout the country. This partnership between law enforcement and private industry provides for greater efficiency in intelligence gathering and dissemination, enabling increased arrests, prosecutions, and recoveries of stolen merchandise.

In addition to LERPnet and coordination with the retail industry, the FBI is identifying and targeting multijurisdictional groups utilizing existing task force resources. Staffed by FBI agency and other Federal, State, and local law enforcement officers, the task

forces are responsible for conducting investigations in the major theft areas of organized retail theft, cargo, vehicle, and jewelry theft crimes. Further, in cases where an organized retail theft enterprise can be tied to other criminal entities, additional FBI or law enforcement resources may be able to assist.

The use of the task force approach to combating crime coupled with successful partnerships within industry is seen by the FBI as one of the most effective and efficient tools by which to identify, disrupt, and dismantle any criminal enterprise. That strategy is working.

For example, in May 2008, 23 organized crime associates of the Gambino crime families, including a Gambino crew supervisor, were arrested based on a racketeering indictment charging them with operating an illegal enterprise involved in illegal gambling, extortion, fraud, and labor racketeering.

The fraud schemes pertained to eight or more associates involved in wire fraud because they created and used counterfeit UPC labels to obtain merchandise from numerous retail outlets. This 6-year investigation was conducted by the FBI as well as our partners at the U.S. Department of Labor, Office of Inspector General, Internal Revenue Service, the New Jersey State Police, and the Union County Prosecutors Office.

In August of that same year, the FBI and its law enforcement partners at the Internal Revenue Service, U.S. Immigration and Customs Enforcement, and the Broward County Sheriff's Department, participated in a raid of PharmaCare Health Services in Sunrise, Florida. The resulting indictments charged transportation of stolen goods, money laundering, conspiracy, and fraud.

According to court documents, PharmaCare was actually a wholesaler that often purchased bulk quantities of mixed and damaged stolen products. Its employees were subsequently convicted of selling millions of dollars worth of over-the-counter medications, health and beauty aids that had been stolen from Walgreens, Target, CVS, and Rite Aid.

Chairman Scott, Ranking Member Gohmert, and Members of the Subcommittee, I appreciate the opportunity to come before you today and share the work that the FBI is doing to address the problem posed by organized retail theft syndicates in this country. I am happy to answer any questions.

[The prepared statement of Mr. Johnson follows:]

PREPARED STATEMENT OF DAVID J. JOHNSON

Good morning, Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee. I appreciate the opportunity to testify before you today on the FBI's efforts to combat organized retail theft (ORT) in the United States. We prefer to use the term "organized retail theft" because the term "organized crime" has a specific meaning within the context of law enforcement. Therefore referring to the criminal activity as "organized retail crime" creates confusion.

ORT THREAT

What is called Organized Retail Theft or ORT by Retail Loss Prevention Professionals, can generally be described as professional burglars, boosters, cons, thieves, fences and resellers conspiring to steal and sell retail merchandise obtained from retail establishments by theft or deception. 'Boosters'—the front line thieves who intend to resell stolen goods—generally coordinate with 'fences' who may sell the items outright at flea markets or convenience stores or online; or repackage them for sale to higher level fences. The problem is significant for its negative economic

impact, the safety issues it brings to unsuspecting consumers, and its potential link to other criminal enterprises.

Each year, organized retail theft is responsible for significant economic losses to retailers, which are then passed along to the American consumer. While it is difficult to pinpoint the exact annual dollar loss caused by this crime problem, retailers estimate all crimes where they are victims results in billions of dollars in losses.

The tax revenue losses attributable to ORT also negatively impact states. In the face of the current economic downturn, the hundreds of millions of dollars in revenue losses to our states can be considered catastrophic.

This crime problem also has the potential to negatively impact consumer health and safety. Specifically, the unsuspecting consumer faces potential health and safety risks from legitimate products which may have been mishandled by the criminal enterprises who stole them for resale to consumers. In many cases, stolen infant formula, pharmaceuticals, and other consumables are not stored under proper conditions. When these items are reintroduced into the retail market, they may pose a significant health risk to the consumer. The potential threat is perhaps most evident in cases in which infant formula is stolen, repackaged and then resold to both knowing and unknowing wholesalers, who then sell the infant formula to government food programs and discount stores. In addition to these concerns, the potential for intentional product tampering prior to the reintroduction of the stolen merchandise into the retail market is significant.

Also of concern for the FBI, in particular, is the potential nexus between organized retail theft syndicates and other criminal enterprises. In 2006, for example, nine members of an alleged Michigan smuggling operation were arrested, accused of taking part in a global scheme involving bootlegged cigarettes, phony Viagra and counterfeit tax stamps, and sending a cut of their illicit profits to Hezbollah.

The FBI has also investigated criminal ties between members of the international street gang MS-13 and fencing rings suspected of trafficking in millions of dollars in stolen medicine and other retail goods.

CHALLENGES

There are many challenges on the road to combating organized retail theft. Lack of available resources to state and local police departments, who have the primary responsibility for investigating most retail crimes, is a huge hurdle. Sharing information between public and private enterprise is another.

As with other forms of criminal enterprise, there is a loose hierarchy within organized retail theft groups. Specifically, these groups utilize low-level 'boosters'—those who actually steal the merchandise and higher level 'fencers,' who frequently coordinate booster thefts. Often, these boosters are illegal immigrants working off a debt or individuals suffering from some form of addiction. If these low-level boosters are removed from the criminal enterprise, others will simply step in to take their place.

These criminal groups are also particularly nimble—able to easily change their appearance, alter their method of operation, and particularly adept at circumventing security devices and procedures. Groups typically utilize methods ranging in sophistication from the development and use of counterfeit receipts and UPC codes to refund and check/credit card fraud to something as basic as the 'grab and run.' They frequently identify store locations with Global Positioning Systems (GPS), identify escape routes, use false identification, utilize rented or borrowed vehicles, and employ diversionary tactics in stores. They are known to travel from state to state or city to city following interstate corridors around large cities.

Further, the wide reach of the Internet and online auction sites has provided global market places for entrepreneurs and, not surprisingly, criminal enterprises.

LAW ENFORCEMENT/PRIVATE INDUSTRY RESPONSE

Sophisticated ORT groups can best be dismantled through a coordinated and cooperative effort between law enforcement and the retail industry. In December 2003, the FBI established an ORT Initiative to identify and disrupt multi-jurisdictional ORT groups, using federal statutes such as Conspiracy, Interstate Transportation of Stolen Property, and Money Laundering. Increased information sharing and cooperation between law enforcement and the private sector will enable both to gain a better understanding of the full nature and extent of the threat ORT poses, as well as to identify the best methods for law enforcement and the retail industry to attack this crime problem.

Additionally, Congress passed legislation signed by the President in January 2006 that required the Attorney General and the FBI, in consultation with the retail community—specifically, the National Retail Federation (NRF) and the Retail Industry Leader's Association (RILA)—to build a system for information-sharing, to include

intelligence as well as lessons learned and best practices regarding ORT. As you may already be aware, the result of that measure—the Law Enforcement Retail Partnership Network (LERPnet)—was subsequently launched in 2007.

The database, which is housed and run by the private sector, allows retail members to track and identify organized retail theft via a secure web portal. To date, nearly 100,000 retail locations are included in the data, which represents $1.17 trillion in retail sales or nearly 25% of all retail sales in one year.

With a recently signed Memorandum of Understanding (MOU), law enforcement will also be able to access LERPnet via the FBI's Law Enforcement Online to search reported incidents and track organized retail theft throughout the country. This partnership between law enforcement and private industry provides for greater efficiency in intelligence gathering and dissemination, enabling increased arrests, prosecutions, and recoveries of stolen merchandise.

Intelligence goes hand-in-hand with partnerships. One good piece of intelligence can be the breakthrough needed to make a vital connection or solve a case. By arming the retail industry with the infrastructure necessary to share such intelligence, it is our hope that they—along with their partners in law enforcement—are better able to thwart criminal efforts and reduce subsequent losses. Previously, individual retailers reported thefts to local law enforcement, but no uniform method of tracking these crimes across jurisdictions existed.

In addition to LERPnet and coordination with the retail industry, the FBI is identifying and targeting multi-jurisdictional ORT groups utilizing existing task force resources. Currently, there are seven FBI-led Major Theft Task Forces which are located in the Chicago, El Paso (2), Memphis, Miami (2) and New York Field Offices. Staffed by FBI Agents and other federal, state and local law enforcement officers, the task forces are responsible for conducting investigations in the major theft areas of ORT, cargo, vehicle, and jewelry theft crimes. Further, in cases where an organized retail theft enterprise can be tied to other criminal entities, additional FBI or law enforcement resources may be able to assist.

These task forces, which combine the resources of local, state and federal law enforcement, as well as retail loss prevention professionals, are applying investigative techniques and strategies which the FBI has successfully utilized to target traditional organized crime, including the development of a solid intelligence base and the use of undercover operations. Clearly, this approach increases the effectiveness and productivity of limited personnel and logistical resources, avoids the duplication of investigation resources, and expands the cooperation and communication among federal, state, and local law enforcement agencies as well as the retail industry.

SUCCESSES

The use of the task force approach to combating crime, coupled with successful partnerships within industry, is seen by the FBI as one of the most effective and efficient tools by which to identify, disrupt and dismantle any criminal enterprise. That strategy is working.

In February 2008, for example, seven individuals were indicted for participating in a scheme to shoplift merchandise and then sell it on the Internet auction site eBay. All seven defendants were charged with participating in a conspiracy to commit wire fraud and to engage in the interstate transportation of stolen property. That case was investigated by the FBI, Kansas City Police Department, and the Postal Inspection Service. It has since been prosecuted by the U.S. Attorney's Office, Western District of Missouri.

In May of that same year, 23 Organized Crime associates of the Gambino Crime Families—including a Gambino Crew Supervisor—were arrested based on a racketeering indictment charging them with operating an illegal enterprise involved in illegal gambling, extortion, fraud and labor racketeering. The fraud schemes pertained to eight or more associates involved in wire fraud because they created and used counterfeit UPC labels to obtain merchandise from numerous retail outlets. This six year investigation was conducted by the FBI as well as our partners at the U.S. Department of Labor, Office of Inspector General; the Internal Revenue Service; the New Jersey State Police; and, the Union County Prosecutors Office.

In August 2008, following months of investigation, the FBI and its law enforcement partners at the Internal Revenue Service, U.S. Immigration and Customs Enforcement, and the Broward County Sheriff's Department, participated in a raid of PharmaCare Health Services in Sunrise, Florida. The resulting indictments charged transportation of stolen goods, money laundering, conspiracy, and fraud. According to court documents, PharmaCare was actually a wholesaler that often purchased bulk quantities of mixed and damaged stolen products. Its employees were subsequently convicted of selling millions of dollars worth of over-the-counter medica-

tions, health and beauty aids that had been stolen from Walgreens, Target, CVS and Rite-Aid.

Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee, I appreciate the opportunity to come before you today and share the work that the FBI is doing to address the problem posed by organized retail theft syndicates in this country. I am happy to answer any questions.

Mr. SCOTT. Thank you very much.

I would like to recognize the—we have been joined by the Chairman of the full Committee, Mr. Conyers, and the gentleman from Illinois, Mr. Quigley.

Ms. Ayala?

TESTIMONY OF JANICE AYALA, DEPUTY ASSISTANT DIRECTOR, OFFICE OF INVESTIGATIONS, UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE), WASHINGTON, DC

Ms. AYALA. Chairman Scott, Ranking Member Gohmert, and distinguished Members of the Subcommittee, on behalf of Secretary Napolitano and Assistant Secretary Morton thank you for the opportunity to testify today about our efforts in the area of organized retail crime. ICE investigates individuals and organizations that exploit vulnerabilities in financial systems to launder their illicit proceeds domestically and internationally. This includes organized retail crime, or ORC.

ICE's financial investigative expertise coupled with its extensive customs and immigration authorities enables ICE special agents to identify, dismantle, and disrupt financial criminal interprises threatening our national economy and security. Additionally, ICE is well aware of the impact of ORC on the retail industry.

ICE recognizes that ORC groups engage in activities that cross over into one or more of ICE's ongoing initiatives or violate laws in which ICE has jurisdiction. ICE has been involved in a number of successful ORC investigations, but I would like to briefly discuss two.

In 2005 San Francisco Bay area retailers provided information to the Oakland Police Department regarding an ORC ring. They, in turn, forwarded the information to ICE agents who, with the assistance of the IRS, the Oakland Police Department, USDA, and FBI, uncovered a ring involving thieves who stole over-the-counter products from large retailers. The stolen products were then resold through Rosemont Wholesale, a company involved in selling products such as medicines, razor blades, baby formula over the Internet and to small local grocery stores.

Two fencing operations purchased the stolen merchandise on behalf of Rosemont and generated illicit profits by selling it to Rosemont at a premium. Rosemont then laundered the products through their online auction site, shipping them throughout the U.S. and Canada. They structured numerous banking transactions to avoid currency reporting requirements, and some of the illicit proceeds turned up in Yemen.

Following an extensive investigation, agencies—more than 12 tractor-trailer loads of stolen merchandise valued at approximately $4.4 million. Charges including interstate transportation of stolen

goods, fraudulent State tax stamps, money laundering, structuring, false statements, and conspiracy were brought against eight defendants.

After a 6-week jury trial Hassan Swaid, president, CEO, and owner of Rosemont, was sentenced to 78 months in prison. Five other members of this organization pled guilty to various crimes and are awaiting sentencing.

In 2001 ICE initiated the Mohammed Ghali investigation after receiving information that a criminal organization he headed was involved in the interstate transportation of stolen merchandise and laundering the proceeds of the sales internationally. Information uncovered during the investigations revealed several members of the organization may have had ties to terrorist organizations.

The Ghali organization recruited hundreds of shoplifters and drug addicts to steal over-the-counter medicinal products, prescription drugs, infant formula, glucose test strips, razors, and pregnancy test kits. Merchandise was repackaged and sold to wholesalers and retailers.

Numerous convenience stores owners operated by the organization in the Fort Worth, Texas area were used as fencing locations. They obtained product by committing various frauds, as well as through armed robbery and warehouse thefts. A shipment of Viagra valued at over $1 million was stolen from a legitimate drug wholesaler and purchased by the Ghali organization and then resold on the street.

ICE initiated a joint undercover operation between its Dallas SAC office and the Fort Worth Police Department and the FDA utilizing a number of investigative techniques to include wiretaps. The loss prevention community also participated throughout the course of the investigation.

As a result, 35 members of the organization were charged with State and Federal violations, including conspiracy; possession, receipt, or interstate transportation of stolen property; and money laundering. Ghali was convicted and sentenced to serve a 14-year Federal prison sentence.

ICE launched an ORC pilot program in July of 2009 in Houston, Los Angeles, Miami, and New York. The pilot focuses on the development of a threat assessment to determine how these groups are engaged in crimes over which ICE has jurisdiction, the tracking system and the database which places ICE agents in contact with members of the retail community and complements information contained in the National Retail Federation's LERPnet, and an enhanced effort to fully explore how these groups are exploiting systemic vulnerabilities in the banking system.

The ORC pilot program encompasses ORC-related criminal activities under the jurisdiction of ICE, including those committed over the Internet, and previous successful ICE investigations have yielded indicators of suspicious banking activity which have been shared with the financial sector. While the ORC initiative is only a pilot program at this time, based on our preliminary results ICE hopes to develop it into an ongoing initiative.

Thank you for your continued support of ICE, DHS, and our law enforcement mission. I would be happy to answer any questions that you may have at this time.

[The prepared statement of Ms. Ayala follows:]

PREPARED STATEMENT OF JANICE AYALA

STATEMENT

OF

JANICE AYALA

ASSISTANT DIRECTOR FOR INVESTIGATIVE PROGRAMS
OFFICE OF INVESTIGATIONS
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

"ORGANIZED RETAIL CRIME"

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

November 5, 2009 – 10:00 a.m.
2141 Rayburn House Office Building

INTRODUCTION

Chairman Scott, Ranking Member Gohmert, and distinguished Members of the Subcommittee:

On behalf of Secretary Napolitano and Assistant Secretary Morton, I would like to thank you for the opportunity to testify today on the efforts of U.S. Immigration and Customs Enforcement (ICE) in the area of Organized Retail Crime (ORC). As you know, ICE is the largest investigative agency within the Department of Homeland Security. We protect national security and uphold public safety by targeting transnational criminal networks and terrorist organizations that seek to exploit vulnerabilities at our borders.

ICE investigates individuals and organizations that exploit vulnerabilities in financial systems for the purpose of laundering illicit proceeds. ICE also addresses the financial component of every cross-border criminal investigation. Naturally, this includes investigations into organized retail crimes. ICE's financial investigative authorities and unique capabilities specifically enable it to identify, dismantle, and disrupt the financial criminal enterprises that threaten our nation's economy and security. One of the most effective methods utilized to identify, dismantle, and disrupt organizations engaged in retail crime is to target the unlawful proceeds gained through their efforts.

ICE's Role in Battling Organized Retail Crime

ICE's Office of Investigations is well aware of the impact of organized retail crime on more than just our retail industry and economy. ICE investigations have demonstrated that profits generated from organized retail crime represent a clear threat to the U.S. financial sector because these profits may be laundered through U.S. and international financial systems. Similar

to other criminal organizations, organized retail crime rings look for and exploit the vulnerabilities within these financial infrastructures to move and store their illicit proceeds.

ICE is involved in myriad investigations that target criminal activity including money laundering, narcotics trafficking, illegal importation and export, violation of intellectual property laws, human smuggling and trafficking, gang activity and human rights violations. ICE agents have broad investigative authorities under Titles 8, 18, and 31 of the United States Code, permitting them to pursue many different types of criminal violations, including complex banking and financial misconduct cases and seize assets of criminal enterprises engaged in immigration and customs violations. The melding of these authorities and unique capabilities given to, and used by, ICE enables it to identify, dismantle and disrupt the financial criminal enterprises that threaten our nation's economy and security.

From experience, ICE recognizes that organized retail crime groups engage in activities that cross over into one or more of ICE's ongoing initiatives or violate laws in which ICE has jurisdiction. ICE has been involved in a number of successful organized retail crime investigations over the past few years, but I would like to briefly discuss two of them.

Rosemont Wholesale, Inc.

ICE has been involved in the Rosemont Wholesale, Inc. investigation since 2005. At that time, ICE learned that individuals connected to Rosemont Wholesale, Inc. were possibly moving illicit proceeds abroad from the large-scale interstate sale of stolen retail products.

In 2005, retailers operating in the San Francisco Bay Area provided information to the Oakland Police Department regarding an ORC ring. Oakland Police Department subsequently forwarded that information to the ICE Special Agent in Charge (SAC) office in San Francisco.

ICE agents in San Francisco, with assistance from the Internal Revenue Service – Criminal Investigation (IRS-CI), the Oakland Police Department, the U.S. Department of Agriculture (USDA), and the Federal Bureau of Investigation (FBI), uncovered a ring involving thieves who stole over-the-counter products from large retailers throughout the San Francisco Bay Area. The stolen products were then resold through Rosemont Wholesale, Inc., a company involved in selling over-the-counter retail products such as medicines, razor blades, and baby formula, both over the Internet and throughout the San Francisco Bay Area to small, local grocery stores. Two fencing operations bought the stolen merchandise on behalf of Rosemont and generated illicit profits by selling it to Rosemont at a premium.

Rosemont then "laundered" the products, selling them through their online auction site and shipping them throughout the United States and Canada. Some of the proceeds from the criminal enterprise turned up in Yemen. In addition, Rosemont structured numerous banking transactions to avoid currency reporting requirements.

Following an extensive investigation, agents from ICE, IRS-CI, FBI, USDA, and officers from the Oakland Police Department executed search warrants at six locations in the San Francisco Bay Area. ICE seized more than 12 tractor-trailer loads of stolen merchandise valued at approximately $4.4 million. Charges were brought against eight defendants, including interstate transportation of stolen goods, securities, moneys, fraudulent state tax stamps or articles used in counterfeiting (18 U.S.C. § 2314), fraud and swindles (18 U.S.C. § 1341), laundering of monetary instruments (18 U.S.C. § 1956), structuring transactions to evade reporting requirements prohibited (31 U.S.C. § 5324), attempt to evade or defeat tax (26 U.S.C. § 7201), fraud and false statements (26 U.S.C. § 7206) and conspiracy to commit offense or to defraud the United States (18 U.S.C. § 371).

On October 16, 2009, Hassan Swaid, the President, Chief Executive Officer and owner of Rosemont Wholesale, Inc., was sentenced to 78 months in prison for his role in the conspiracy. Swaid was convicted on June 24, 2009, following a six-week jury trial. Five other members of this organization have pled guilty to various crimes, including structuring transactions to evade reporting requirements, conspiracy related to the interstate transportation of stolen goods, securities, moneys, fraudulent state tax stamps or articles used in counterfeiting, attempting to evade or defeat tax, and fraud and false statements. All remaining conspirators are currently awaiting sentencing.

Mohammed Ghali

ICE was involved in the Mohammed Ghali investigation after receiving information that a criminal organization he headed was involved in the interstate transportation of stolen merchandise and laundering the proceeds from the sale of this stolen merchandise internationally. According to sources ICE had developed, several members of the organization were also alleged to have direct ties to terrorist acts and/or organizations.

Mohammed Ghali was the leader of a criminal organization involved in large scale organized retail theft and international money laundering. Proceeds from Ghali's criminal activity were deposited in foreign financial institutions with weak anti-money laundering programs.

Members of the Ghali organization recruited hundreds of shoplifters and drug addicts to steal over-the-counter medicinal products, prescription drugs, and other specific items such as infant formula, glucose test strips, razors, and pregnancy test kits. These items were then repackaged and sold to wholesalers and retailers.

The organization used numerous convenience stores owned and operated by members of the organization in the Fort Worth, Texas area as fencing locations. Shoplifters and thieves utilized elaborate schemes to obtain the products such as counterfeit coupons, price matching schemes, and manufacturing counterfeit uniform price code labels. They also committed fraud through the use of food stamps and Women, Infant and Children Programs. In some instances, large quantities of products were obtained through armed robbery and warehouse thefts. For example, a shipment of Viagra valued at over $1 million was stolen from a legitimate drug wholesaler, purchased by members of the Ghali organization, and then resold on the street.

To further expose the criminal organization, ICE initiated a joint undercover operation between its Dallas SAC office, the Fort Worth Police Department, and the Food and Drug Administration. The investigation utilized a number of investigative techniques, including the use of confidential informants, wiretaps, video and audio surveillance, undercover meetings and pen registers. Members of the loss prevention community also participated throughout the course of the investigation. Agents conducted approximately 93 undercover transactions in which property was specially marked, represented as stolen and sold to members of the organization. As a result of the investigation, approximately 35 members of the organization were charged with state and federal violations, including conspiracy, possession of stolen goods, interstate transportation of stolen property, receipt of stolen goods, and money laundering. Ghali, the leader of the organization, was convicted and sentenced to serve 14 years in federal prison. He also was ordered to forfeit two residences and $527,627 in cash that was seized during the investigation.

While I cannot discuss the specifics of ongoing organized retail crime investigations, ICE is currently working on active cases related to organized retail crime in Texas, Illinois, California and Florida.

Organized Retail Crime Pilot Program

ICE has become increasingly involved in investigations that target organized retail crime due to the interstate and international shipments of stolen goods and the corresponding movement of illicit proceeds from the sale of these stolen goods.

ICE has developed a pilot program to enhance the agency's ability to address the organized retail crime threat. The ORC Pilot Program was launched on July 6, 2009, in Houston, Los Angeles, Miami and New York, and is scheduled to last for an initial period of six months. The ORC Pilot Program focuses on four primary areas: 1) the development of a threat assessment to determine how these groups are engaged in crimes over which ICE has jurisdiction; 2) the development of a tracking system aimed at assessing ICE's involvement in ORC cases; 3) the development of a database that will be made available to the field with retail industry contacts for the affected ICE offices, which compliments the existing information contained in the National Retail Federation's LERPnet database by placing ICE agents in contact with members of the retail community throughout the country; and 4) an enhanced effort to explore fully how these groups are exploiting systemic vulnerabilities in the banking system to launder their profits.

The ORC Pilot Program, which is being funded with base investigative resources, encompasses all types of ORC-related criminal activities under the jurisdiction of ICE, including those committed over the Internet. Since the pilot program was launched just over four months ago, it is still too early to conduct an accurate analysis of its overall effectiveness. However,

based on previous successful ICE investigations into organized retail crime, we have been able to develop some indicators of suspicious banking activity related to ORC. These indicators include:

- Business checks written to individuals, as opposed to legitimate suppliers.
- Business checks cashed at the banks from which the checks originated, instead of being deposited into another business' bank account.
- Business checks written to cash on a regular basis in amounts that exceed a business's petty cash requirement.
- Multiple checks written on the same day to cash to ensure the amount of each check does not exceed $10,000.
- Multiple money orders in increments of $500 or less deposited into bank accounts in which the remitter of the money order is the same as the authorized signers on the bank accounts for which the checks are being deposited.
- Subjects of questionable financial transactions maintaining the same address.
- Occupations listed for the subjects of questionable financial activities that are not commensurate to the volume and type of the financial activities.
- Checks drawn from the questionable financial activities that are negotiated in foreign countries.
- Cash deposits related to the questionable financial activities involving currency in $100 denominations.

CONCLUSION

While the organized retail crime initiative is only a pilot program at this time, based on our preliminary results of the threat assessment, ICE hopes to develop it into an ongoing initiative.

I would like to thank the Subcommittee for this opportunity to testify and for your continued support of ICE, DHS and our law enforcement mission. I will be happy to answer any questions that you may have at this time.

8

Mr. SCOTT. Thank you.
Mr. Large?

TESTIMONY OF JOHN R. LARGE, SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIONS DIVISION, UNITED STATES SECRET SERVICE, WASHINGTON, DC

Mr. LARGE. Good morning, Chairman Scott, Ranking Member Gohmert, Committee Chairman Conyers, and distinguished Members of the Subcommittee. Thank you for today's opportunity to address the Secret Service's role in investigating financial crimes as they relate to organized retail crime.

United States Secret Service is responsible for two significant missions: protection and criminal investigations. While we are perhaps best known for protecting our Nation's leaders, I would like to point out that we were originally established in 1865 to investigate and prevent the counterfeiting of U.S. currency.

As the original guardian of the Nation's financial payment system, the Secret Service has established a long history of protecting American consumers, industries, and financial institutions from fraud. Over the last 144 years our investigative mission and statutory authority has expanded, and today we are recognized worldwide for our expertise and innovative approaches to detecting, investigating, and preventing financial fraud.

In recent years, the combination of the information revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve. On account of our work in the areas of financial and electronic crimes, we have developed particular expertise in the investigation of identity theft, false identification fraud, credit card fraud, debit card fraud, check fraud, bank fraud, cyber crime, and computer intrusions.

Globalization has made commerce easy and convenient for corporations and consumers. Financial institutions and systems are readily accessible worldwide. Today's financial fraud and cyber criminals have adapted to this new means of global trade and are subsequently seeking to exploit our dependence on information technology.

With the explosion of Internet accessibility worldwide, the criminal element has modified their fraudulent schemes to a new, more anonymous, and constantly evolving cyber arena. The Secret Service looks to outpace emerging threats posed by financial fraud and cyber criminals by adopting an innovative and multifaceted approach.

Through years of collaboration on our investigative and protective endeavors we have established unique and vital partnerships with State, local, and other Federal law enforcement agencies. These partnerships have enabled us to establish a national network of financial crimes task forces and electronic crimes task forces that combine the resources of the private sector, other law enforcement agencies, and academia in an organized effort to combat threats to our financial payment systems and credible infrastructures.

We currently maintain 37 financial crime task forces and 28 electronic crime task forces located in metropolitan regions across the country, including the first international electronic crimes task force, based in Rome, Italy.

Looking specifically at statistics for fiscal year 2009, agents assigned to Secret Service offices throughout the United States ar-

rested over 5,800 suspects for financial crime violation. These individuals are noted to be responsible for approximately $443 million in actual fraud loss to specific victims and/or financial institutions. With this globalization of ecommerce, online auction houses have found themselves the victims or even the unwitting participants in these organized schemes.

While investigating our core violations related to financial crimes, the Secret Service has also opened criminal investigations into these organized cyber groups. The Secret Service has found these cases primarily evolve from access device fraud investigations, wherein criminals fraudulently purchase merchandise from traditional and online retailers and then resell the merchandise through online auction houses.

In the recent past we have worked closely with online auction houses to successfully investigate and prosecute several of these groups. For example, in March 2008 we identified a complex fraud scheme in which an organized group of suspects were compromising credit cards at a local Washington, D.C. area restaurant, using the skimmed credit card numbers to purchase gift cards for nationally identified retail stores.

Upon obtaining gift cards, the subjects would purchase electronic merchandise and sell those items and other gift cards through various online auction houses. Through the collaborative effort of the Secret Service, the online auction houses, the victim retail stores, all suspects associated with this case were subsequently arrested on Federal charges of access device fraud, aggravated identity theft, and conspiracy.

In conclusion, as I have highlighted, Secret Service remains steadfastly committed to our mission of protecting the integrity of the U.S. currency and safeguarding the Nation's critical infrastructure and financial payment systems. Although our core violations remain the same, our methods of investigation have changed along with emerging technologies that drive crime today.

Through our successful partnerships with public and private task force members we continue to adapt to ever evolving cyber criminal environment and dedicate significant resources to aggressively investigate all offenses within our purview. Our efforts continue to fill our originating investigative mission and protect consumers and financial institutions.

Chairman Scott, Ranking Member Gohmert, Committee Chairman Conyers, and distinguished Members of the Subcommittee, I thank you again for this opportunity to testify on behalf of the U.S. Secret Service, and I will be pleased to answer any questions at this time.

[The prepared statement of Mr. Large follows:]

PREPARED STATEMENT OF JOHN R. LARGE

Statement of John R. Large
Special Agent in Charge
Criminal Investigative Division
Office of Investigations
U. S. Secret Service

Before the

House Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security
U.S. House of Representatives

Hearing on
"Combating Organized Retail Crime – The Role of Federal Law Enforcement"

November 5, 2009

Good morning, Chairman Scott, Ranking Member Gohmert and distinguished members of the Subcommittee. Thank you for the opportunity to testify today on the investigative responsibilities of the United States Secret Service (Secret Service).

While the Secret Service is perhaps best known for protecting our nation's leaders, we were established in 1865 to investigate and prevent the counterfeiting of United States currency. As the original guardian of the nation's financial payment system, the Secret Service has a long history of protecting American consumers, industries, and financial institutions from fraud. Congress continues to recognize the Secret Service's 144 years of investigative expertise in financial crimes and over the last two decades has expanded our statutory authorities to include access device fraud (18 USC §1029), which includes credit and debit card fraud. Congress has also given the Secret Service concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344). We take our mission to combat these crimes seriously and as a result, the Secret Service is recognized worldwide for its investigative expertise and innovative approaches to detecting, investigating, and preventing financial crimes.

To accomplish its investigative mission, the Secret Service operates 142 domestic offices (including domicile offices) and 22 foreign offices in 18 countries. The agency works closely with other federal, state, and local law enforcement, as well as other U.S. government agencies and foreign counterparts to maximize its efforts.

Financial Fraud and Electronic Crimes

In recent years, the combination of the information revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve. Through our work in the areas of financial and electronic crime, the Secret Service has developed particular expertise in the investigation of identity theft, false identification fraud, credit card fraud, debit card fraud, check fraud, bank fraud, and cyber crime, including computer intrusions. In Fiscal Year 2008, agents assigned to Secret Service offices across the United States arrested over 5,600 suspects for financial crimes violations. These suspects were responsible for approximately $442 million in actual fraud loss to individuals and financial institutions.

The Secret Service continues to observe a marked increase in the quality, quantity, and complexity of financial crimes, particularly offenses related to identity theft and access device fraud. Criminals often seek the personal identifiers generally required to obtain goods and services on credit, such as Social Security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers, and personal identification numbers (PINs).

In the 1980s and 1990s, criminals obtained stolen personal and financial information through traditional means, such as theft of mail, theft of trash from businesses or victims, home and vehicle burglaries, and theft of a victim's wallet or purse. While these low-tech methods of theft remain popular, criminal activity has also evolved so that criminals now employ newer, more high-tech methods for obtaining large quantities of stolen information.

Recent trends observed by law enforcement show that today's criminals continue to seek to compromise victims' personal and financial information through the use of computers and the Internet to launch cyber attacks targeting citizens and financial institutions. Cyber criminals have become adept at stealing victims' personal information through phishing emails, account takeovers, malicious software, hacking attacks, and network intrusions resulting in data breaches.

The Secret Service is particularly concerned about cases involving network intrusions of businesses that result in the compromise of credit and debit card numbers and all related personal information, and the subsequent exploitation of this data. A considerable portion of this type of electronic theft appears to be attributable to organized cyber groups, many of them based abroad, which pursue both the intrusions and the subsequent exploitation of the stolen data. Stolen credit card information is often trafficked in units that include more than just the card number and expiration date. These "full-info cards" include additional information, such as the card holder's full name and address, mother's maiden name, date of birth, Social Security number, a PIN, and other personal information that allows additional criminal exploitation of the affected individual.

Another rising trend is the increase in volume of trafficking "card track data" together with PINs. This data allows a criminal to manufacture a fully functional counterfeit credit or debit card and execute ATM withdrawals or other PIN-enabled transactions against an account.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals alike. Illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding websites," operate like online bazaars where criminals converge to trade in personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting memberships of approximately 8,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell, and trade malicious software, spamming services, credit, debit, and ATM card data, personal identification data, bank account information, hacking services and other contraband.

In addition to the exploitation of credit and debit card accounts, many of the more sophisticated online criminal networks are now actively exploiting compromised online financial accounts. Criminals who gain access to victim accounts using online systems then execute fraudulent electronic banking transfers or sell the information to other criminals. The desire to exploit online bank accounts has led to the explosive growth of phishing scams, as well as the recent wave of malicious software, also known as "malware" or "crimeware," which is specifically designed to harvest account login information from the computers of infected victims. The technical sophistication of the illicit services readily available continues to grow. For example, the online fraud networks are increasingly leveraging the technical capabilities of "botnets" (i.e. networks of thousands of infected computers which can be controlled by a criminal from a central location) for financial attacks ranging in nature from the hosting of phishing and other malicious websites to the launching of widespread attacks against the online authentication systems of U.S. financial institutions.

The information revolution of the 1990s has turned our personal and financial information into a valuable commodity, whether it is being collected and brokered by a legitimate company or stolen by an identity thief. This information is no longer only an instrument used to facilitate a financial crime; it is now the primary target of criminals. Today, many companies have access to or store customer's personal financial information. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals.

Globalization has made commerce easy and convenient for corporations and consumers – financial institutions and systems are readily accessible worldwide. Today's cyber-criminals have adapted to this new means of global trade and subsequently seek to exploit our dependence on information technology. With the explosion of Internet accessibility world-wide, criminals have modified their fraudulent schemes to a new, more anonymous and constantly evolving cyber arena. As a result, the Secret Service has modified its investigative techniques to keep pace with emerging technologies.

With this expansion of cyber crime, online auction houses have found themselves the victims or even the unwitting participants in organized criminal conspiracies. The Secret Service, while continuing to investigate financial crimes, has also opened criminal investigations into these organized cyber groups. The Secret Service has found these cases primarily evolve from access device fraud investigations, wherein, criminals who fraudulently purchase merchandise from traditional and online retailers and then resell the merchandise through online auction houses. In the recent past, the Secret Service, working closely with online auction houses, has successfully investigated and prosecuted several of these groups.

In May 2006, an internationally recognized telecommunications company contacted the Secret Service regarding the theft of approximately 20,000 cell phones from their plant in a major U.S. metropolitan area. The phones had left a warehouse in a shipment of five large pallets, and only two reached their final destination. The investigation led to employees of a nationally identified shipping company. The employees were interviewed regarding the missing shipments and eventually a manager of the shipping company confessed to running a stolen cell phone operation. The scheme involved cell phones that were sold to a re-seller at $75-$100 per phone, usually valued at $120-$150. Some of the phones were resold from a network of small collusive shops and some were sold at other venues, such as online auction houses. As a result of the investigation, the Secret Service recovered $1,549,000 of merchandise from a suspect's residence and all suspects in this case were arrested on federal charges for Aiding and Abetting, Conspiracy, and Access Device Fraud.

In October 2007, members of a Secret Service Electronic Crimes Task Force (ECTF), in cooperation with a District Attorney's Office, began an investigation into the criminal activities of an identified international currency transmittal service. The investigation revealed that suspects associated with this currency transmittal service recruited numerous individuals to sell fraudulently obtained merchandise over online auction houses. These proxy sellers advertised and took orders and/or bids for electronic merchandise at a significantly reduced price. Using stolen credit card information, the suspects purchased the ordered merchandise and then shipped it directly to the purchaser, or through another remailer. To date, the known fraud loss attributed to the group exceeds $4 million. Since the launch of the investigation, fourteen defendants have

been arrested and are now in the United States and one defendant is currently in custody overseas awaiting extradition to the United States.

In March 2008, the Secret Service was contacted by a credit card issuing bank regarding credit cards that were compromised at a local restaurant. Subsequent investigation revealed four suspects were using "skimmed" credit card numbers to purchase gift cards from nationally identified retail stores. Upon obtaining the gift cards, the subjects would purchase electronic merchandise and sell those items and other gift cards through various online auction houses. All suspects associated with this case were subsequently arrested on federal charges for Access Device Fraud, Aggravated Identity Theft, and Conspiracy.

Fostering Partnerships and Combining Resources

Criminal groups involved in financial crimes routinely operate in a multi-jurisdictional environment. By working closely with other federal, state, and local law enforcement representatives, as well as foreign law enforcement, the Secret Service is able to provide a comprehensive network of information sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries.

The Secret Service has established unique and vital partnerships with state, local, and other federal law enforcement agencies through years of collaboration on our investigative and protective endeavors. These partnerships enabled the Secret Service to establish a national network of Financial Crimes Task Forces (FCTFs) to combine the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to our financial payment systems and critical infrastructures. The Secret Service currently maintains 37 FCTFs located in metropolitan regions across the country.

Further, in 1996, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress has since directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

To date, the Secret Service has established 28 ECTFs, including the first international ECTF based in Rome, Italy. Membership in our ECTFs include: 299 academic partners; over 2,100 international, federal, state and local law enforcement partners; and over 3,100 private sector partners. The Secret Service ECTF model is unique in that it is an international network with the capabilities to focus on regional issues. For example, the New York ECTF, based in the nation's largest banking center, focuses heavily on protecting our financial institutions and infrastructure, while the Houston ECTF works closely with partners such as ExxonMobil, Chevron, Shell, and Marathon Oil to protect the vital energy sector. By joining our ECTFs, all of our partners enjoy the resources, information, expertise, and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Partnerships between law enforcement and the private sector are critical to the success of the ECTF's preventive approach. Our ECTFs collaborate with private sector technical experts in an effort to protect their system networks and critical information by encouraging the development of business continuity plans and routine risk management assessments of their electronic infrastructure. Greater ECTF liaison with the business community provides rapid access to law enforcement and vital technical expertise during incidents of malicious cyber crime. The ECTFs also focus on partnerships with academia to ensure that law enforcement is on the cutting edge of technology by leveraging the research and development capabilities of teaching institutions and technical colleges.

Another key element of success within the ECTF model is the Secret Service's Electronic Crimes Special Agent Program (ECSAP). This program is comprised of 1,148 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received extensive training in forensic identification, preservation and retrieval of electronically stored evidence. ECSAP agents are computer investigative specialists and among the most highly-trained experts in law enforcement, qualified to conduct examinations on all types of electronic evidence. This core cadre of special agents is equipped to investigate the continually evolving arena of electronic crime and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud, and various other electronic crimes targeting our financial institutions and private sector.

These resources allow ECTFs the potential to identify and address possible cyber vulnerabilities before criminals find and exploit them. This proactive approach has successfully prevented cyber attacks that otherwise would have resulted in large-scale financial losses to U.S. based companies or disruptions of critical infrastructures. The Secret Service task force model opens the lines of communication and encourages the exchange of information between all academic, private sector, and law enforcement partners.

Additionally, the National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, the Department of Homeland Security (DHS), and the State of Alabama. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct basic electronic crimes investigations.

Since opening on May 19, 2008, the Secret Service has provided critical training to 564 state and local law enforcement officials representing over 300 agencies from 49 states and two U.S. territories.

Community Outreach and Public Awareness

The Secret Service raises awareness of issues related to counterfeit, financial fraud, and electronic crimes, both in the law enforcement community and among the general public. The Secret Service has worked to educate consumers and provide training to law enforcement personnel through a variety of programs and initiatives. Agents from local field offices routinely

provide community outreach seminars and public awareness training on the subjects of counterfeit currency, financial fraud, identity theft, and cyber crime. Agents often address these topics when speaking to school groups, civic organizations, and staff meetings involving businesses or financial institutions. In addition, the Secret Service provides training in the form of continuing education to state and local law enforcement. This training includes formal and informal classes which occur at field office sponsored seminars, police academies, and other various settings.

The Secret Service currently participates in a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission (FTC), the International Association of Chiefs of Police (IACP), and the American Association of Motor Vehicle Administrators to host identity crime training for law enforcement officers. In the last four years, Identity Crime Training Seminars have been held in over 18 cities nationwide, with two more expected by the end of the year. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their identity crime investigations.

In addition, the Secret Service is committed to providing our law enforcement partners with publications and guides to assist them in combating counterfeit activity, financial fraud and cyber crime. The Secret Service continues to collaborate with the Department of Treasury and the Bureau of Engraving and Printing to produce and distribute various pamphlets, guides, posters, and visual aides pertaining to counterfeit currency detection.

Specific instructions pertaining to the seizure and analysis of electronic evidence should be provided to officers to ensure proper investigation and successful prosecution of cyber crime offenses. To provide this essential knowledge, the Secret Service published the "*Best Practices Guide for Seizing Electronic Evidence*." This pocket guide was designed for police officers and detectives acting as first responders and helps guide law enforcement officers in recognizing, protecting, seizing, and searching electronic devices in accordance with applicable statutes and policies. The guide continues to be updated, and it is currently issued in its third edition.

The Secret Service also has collaborated with several of our law enforcement and corporate partners to produce the interactive, computer-based training programs known as "*Forward Edge*" and "*Forward Edge II*." The *Forward Edge* series is a CD-ROM that provides law enforcement and corporate investigators with practical training in order to recognize and seize electronic storage items.

Finally, the Secret Service produced an Identity Crime Video/CD-ROM, which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to law enforcement which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the FTC and the IACP.

Conclusion

As I have highlighted in my statement, the Secret Service is committed to our mission of protecting the integrity of U.S. currency and safeguarding the nation's critical financial infrastructure and financial payment systems. Although the Service's core responsibilities remain the same, our methods of investigation have changed to keep pace with emerging technologies. Through successful partnership with public and private task force members, the Secret Service continues to adapt to the ever evolving cyber criminal environment. The Secret Service dedicates significant resources to aggressively investigate all offenses within our purview to protect consumers and financial institutions.

This concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Mr. SCOTT. Thank you.
Mr. Hill?

TESTIMONY OF ZANE M. HILL, DEPUTY CHIEF POSTAL INSPECTOR, UNITED STATES POSTAL INSPECTION SERVICE, WASHINGTON, DC

Mr. HILL. Mr. Chairman, Members of the Committee, thank you for holding this hearing on organized retail crime. The U.S. Postal Inspection Service is committed to protect the American public from criminals who use the United States Postal Service in furtherance for fraud and theft schemes, including organized retail crime.

The Postal Inspection Service has a long, proud, and successful history of securing the Nation's mail system and maintaining the public's trust in the mail. Postal inspectors are charged with ensuring the mail is safe and free from fraudulent schemes, illegal drugs, various forms of contraband, child pornography, as well as other dangerous products. Additionally, we work with other law enforcement and government agencies at the local, State, and Federal level to ensure the postal service is not used to facilitate the commission of other crimes or as a conduit for the transportation of proceeds from illegal activities.

It is this commitment that makes the Postal Service the most trusted government agency and one of the most trusted organizations in the United States. The use of the mails in organized retail theft has not historically been one of the major types of criminal activities we have encountered. That being said, we are now aware of its potential impact and a number of these types of cases have been referred to us from other law enforcement agencies as well as the retail industry.

Our colleagues in Federal, State, and local law enforcement, as well as corporate security professionals, are the principal investigators in the area of organized retail crime. When these crimes or aspects of these crimes cross into the postal system we have the jurisdiction and statutory authority to investigate and ssist other law enforcement agencies and retailers in combating these illegal activities.

We generally see two types of schemes, which I will discuss briefly: Internet auction fraud and reshipper fraud. Both of these crimes take advantage of increasing use of the online marketplace in order to sell the stolen or fraudulently obtained goods.

The Internet has become a critical component of the world's commerce. More and more businesses are increasing their use of this commerce channel. Likewise, consumers have the convenience and ease of shopping in this expanded marketplace with a simple click of the mouse without having to leave home.

This convenience, though, has a downside. Criminals now have a larger market in which to sell and distribute their stolen products and can made substantial profits with fewer risks than the physical fencing operations that these criminals have historically used.

By far, there is a greater reach for advertising of the stolen products and the risk of detection is somewhat limited, making this online marketplace option so attractive to the organized retail crime groups. Like all law enforcement agencies, we have had to adapt our investigative strategies and tactics in order to investigate and prevent cyber crime of all types.

Our jurisdiction in organized retail crime lies in the use of the mails to ship the stolen products or as a means to remit payments to the online seller. In these investigations we have seen the criminal groups attempt to utilize the full spectrum of postal service products and services in their fraudulent schemes.

One example of a recent Post Inspection Service case began early 2008. Postal inspectors received a tip that owners of two Toledo, Ohio convenience stores were buying stolen merchandise, selling it on eBay, and then shipping the items both domestically and internationally via the Postal Service. Postal inspectors determined that proceeds from the fraudulent sales were then being laundered by the operators' relatives in Jordan.

We alerted special agents of ICE in July when it was determined one of their operators was—one of the operators was leaving for Jordan on a flight from the Detroit Metro Airport and was believe to be smuggling an unknown amount of cash. ICE agents stopped the owner, his wife, and their two children at the airport and seized $75,000 in undeclared funds which were hidden in the children's clothing. The husband and wife each pled guilty to illegally smuggling cash and were sentenced to time in prison.

Postal inspectors continued their investigation of the other suspect operator with excellent cooperation from eBay and PayPal and obtained records from the owner which identified over 7,500 items valued at $650,000 that had been sold online. Postal inspectors working with loss prevention specialists from the victim companies identified most of the items as coming from their stores.

Throughout 2008 postal inspectors and corporate security investigators continued their work undercover, purchasing stolen items from online sites operated by the suspect. In February 2009 postal inspectors, ICE agents, and Toledo, Ohio police executed a search warrant at the suspect's home and recovered boxes of stolen merchandise as well as maps of pharmacies he apparently planned to target in Cleveland, Columbus, and Toledo. He was arrested and charged with mail fraud, pled guilty in August, and is being detained until sentencing.

Second area of retail crime we have become involved in is in reshipper fraud. In these types of cases criminal organizations enlist individuals to receive and then reship products to other segments of the criminal enterprise, generally to locations outside of the United States.

In the majority of these cases the products are obtained by the retail crime groups through credit card theft and fraud. Reshippers are oftentimes unwitting accomplices to the scheme, receiving and mailing the products based on instructions provided by the fraudsters. The reshippers do not know the source of the products they receive and then reship.

Many of these groups recruit the reshippers in an attempt to further insulate themselves from detection using a variety of ploys to trick individuals looking for easy work-at-home jobs. Ultimately these reshippers become part of the fraudulent activity.

Retailers, shipping companies, and financial institutions have all seen an increase in this type of crime. Again, the ability to move the stolen product with the least amount of exposure to those per-

petrating the crimes is the reason for the use of the reshipper approach.

The Postal Inspection Service continues to educate consumers about these fraudulent schemes through an aggressive consumer awareness and education program. These are distributed through the Postal Service, our Web site, videos, and newspaper, as well as online publications.

In closing, be assured the Postal Inspection Service remains committed to working with law enforcement and retailers to deal with the criminal distribution of illicit goods. Thanks for the opportunity to testify at this hearing. I am ready to answer any questions you might have.

[The prepared statement of Mr. Hill follows:]

PREPARED STATEMENT OF ZANE M. HILL

Mr. Chairman and members of the Committee: thank you for holding this hearing on organized retail crime. The Postal Inspection Service appreciates the opportunity to be here with our colleagues from the U.S. Secret Service, Federal Bureau of Investigation and Immigration and Customs Enforcement to talk about our efforts to thwart organized retail crime. The Postal Inspection Service is committed to protect the American public from criminals who use the United States Postal Service in furtherance of fraudulent schemes, including organized retail crime.

The Postal Inspection Service has a long, proud, and successful history of securing the nation's mail system and ensuring the public's trust in the mail. Postal Inspectors have been fighting consumer fraud since the mail fraud statute was enacted in 1872. The company name, address and "product" may change, but con artists take advantage of economic trends and current events to plan their schemes and illegal activities. With modern technology, the potential for the American public to be defrauded through the mail is much greater and potentially impacts more people than ever before.

Because it is essential the public have full trust and confidence in the mail, Postal Inspectors are intent on preserving the integrity of the U.S. Mail through vigorous law enforcement, public education, and crime prevention efforts.

Postal Inspectors are charged with ensuring the mails are safe and free from fraudulent schemes, illegal drugs, various forms of contraband, child pornography, as well as other dangerous products. Additionally, we work with other law enforcement and government agencies at the local, state, and federal level to ensure the Postal Service is not used to facilitate the commission of other crimes or as a conduit for the transportation of proceeds from illicit activities.

It is this commitment that makes the Postal Service the most trusted government agency and one of the most trusted organizations in the United States. It is the ongoing vigilance of the Postal Service and Postal Inspectors in identifying criminals who attempt to use the mails in furtherance of their illegal activities. The use of the mails in organized retail theft has not historically been one of the major types of criminal activities we have encountered. That being said, we are now aware of its potential impact and a number of these types of cases have been referred to us from other law enforcement agencies as well as the retail industry.

Our colleagues in federal, state, and local law enforcement, as well as corporate security professionals, are the principal investigators in the area of organized retail crime. When these crimes or aspects of these crimes cross or enter into the postal system, we have the jurisdiction and statutory authority to investigate and assist other law enforcement agencies and retailers in combating these illegal activities.

We generally see two types of schemes which I will discuss briefly: Internet auction fraud and Re-shipper fraud. Both of these crimes take advantage of the increasing use of the on-line marketplace in order to sell the stolen or fraudulently obtained goods.

The Internet has become a critical component of the world's commerce. More and more businesses are increasing their use of this commerce channel. Likewise consumers have the convenience and ease of shopping in this expanded marketplace with a simple click of the mouse without having to leave home. This convenience though has a downside—criminals as well as others who seek to take advantage of consumers, now have a larger market in which to sell and distribute their stolen products while making substantial profits with fewer risks than the physical fencing operations that these criminals have historically used. By far, there is a greater

reach for advertising of the ill-gotten products and the risk of detection is somewhat limited, making this online marketplace option so attractive to the organized retail crime groups.

As noted our jurisdiction in organized retail crime lies in the use of the mail in order to ship the stolen products or as a means to remit payment to the online seller. In these investigations, we have seen criminal groups utilize the full spectrum of postal products, including Priority Mail, Express Mail, postal money orders as well as Post Office boxes from which they run their fraudulent schemes.

One example of a recent Postal Inspection Service case began in early 2008. Postal Inspectors received a tip that owners of two Toledo, OH convienence stores were buying stolen merchandise, selling it on eBay and then shipping the items, both domestically and internationally via the Postal Service. Postal Inspectors determined that proceeds from the fraudulent sales were being laundered by the operators' relatives in Jordan. We alerted special agents of Immigration and Customs Enforcement (ICE) in July when it was determined one of the operators was leaving for Jordan on a flight from the Detroit Metro Airport, and was believed to be smuggling an unknown amount of cash. ICE special agents stopped the owner, his wife, and their two children at the airport and seized $75,000 in undeclared funds which were hidden in the children's clothing. The husband and wife each pled guilty to illegally smuggling cash and were sentenced to time in prison.

Postal Inspectors continued their investigation of the other suspect operator with excellent cooperation from eBay and PayPal and obtained records of the owner which identifed over 7,500 items valued at $650,000 that he had sold online. Postal Inspectors worked with loss-prevention specialists from the victim companies and identified most of the items as coming from their stores.

Throughout 2008, Postal Inspectors and corporate security investigators worked undercover, purchasing stolen items from online sites operated by the suspect. In February 2009, Postal Inspectors, ICE special agents, and Toledo, OH police executed a search warrant at the suspect's home and recovered boxes of stolen merchandise as well as maps of pharmacies he apparently planned to target in Cleveland, Columbus, and Toledo. He was arrested and charged with mail fraud. He pled guilty in August and is being detained until he is sentenced.

The second area of retail based crime we have become involved in is re-shipper fraud. In these types of cases, criminal organizations enlist individuals to receive and then reship products to other segments of the criminal enterprise generally to locations outside of the United States. In the majority of these cases, the products are obtained by retail crime groups through credit card theft as well as fraud. The re-shippers are oftentimes unwitting accomplices to the scheme, receiving and mailing the products based on instructions provided by the fraudsters. The re-shippers are then paid for their services. Many of these groups recruit the "re-shippers" in an attempt to further insulate themselves from detection, using a variety of ploys to trick individuals looking for easy work-at-home jobs. Ultimately, these re-shippers become part of the fraudulent activity. Retailers, legitimate shippers and financial institutions have all seen in increase in this type of crime. Again, the ability to move the stolen product with the least amount of exposure to those perpetrating the crimes is the reason for the use of the re-shipper approach.

As part of their operation recruiters for the groups post bogus job listings on the various Internet career sites purporting to employ "merchandising managers" and "package processing assistants." The employment is described as, "receiving packages in the mail and resending them to foreign addresses." This certainly sounds attractive as well as easy to the prospective participants. The groups further the scheme often providing bogus and fraudulently obtained postage-paid mailing labels to their re-shipper recruits. The Postal Service can also suffer significant losses as well as damage to its brand integrity when postal products or services are targeted by criminal schemes.

Re-shippers are also recruited by a variety of other fraudulent solicitations, such as on-line dating Web dating sites. In the typical "sweetheart scammer", the fraudster sends e-mails to the potential recruit in order get to know them. Once they have aroused their attention, the fraudster asks them to help the business or family by shipping packages to Europe or Africa.

Other scammers oftentimes claim to be working with a charity or mission which needs help getting "donated" merchandise delivered to third-world countries as well as other parts of the world.

In reality, both the "sweetheart" and the "charity worker" need assistance with smuggling goods out of the United States which were purchased with stolen and other fraudulently obtained credit cards. In the end there's no sweetheart or legitimate charity—even the mailing labels are either fraudulent or obtained using stolen credit cards.

The U.S. Postal Inspection Service continues to educate consumers about these fraudulent schemes using, for example, prevention-oriented messages delivered through online videos, newspaper and ad awareness campaigns (such as fakechecks.org), as well as via online publications, and our Web site at: www.usps.com/postalinspectors.

In closing, be assured the Postal Inspection Service remains committed to collaborating with our law enforcement and corporate partners to deal with the problem of distribution of illicit goods through on-line market places and ultimately the U.S. mail.

Mr. SCOTT. Thank you very much.

I want to thank all of our witnesses for their testimony, and now we will recognize ourselves for 5 minutes each for questions.

And my first question, probably to Mr. Johnson: If somebody notices that their goods are being sold on an Internet auction site who should they call?

Mr. JOHNSON. Well, I think they have a couple of options. One, they can call their local police department or they can call their local FBI office and report the activity which they believe may be criminal. And, although I can only speak for the FBI, to the extent possible we would follow up that information and determine whether or not enough facts exist to open an investigation or not.

Mr. SCOTT. And do you have enough authority under present criminal law procedure to open an investigation and proceed? Do you need any new laws on the books, from a procedural perspective, to investigate?

Mr. JOHNSON. Although I can't comment specifically on legislation here—we typically do it through DOJ—my personal opinion is that the existing laws on the books, whether it is Title 18, U.S. Code 2314 or 2315, or the conspiracy statutes, or the money laundering statutes, or even the RICO statute, do provide adequate criminal remedies to address these matters——

Mr. SCOTT. Okay. Those are criminal remedies. What about procedure? Do you have enough in terms of probable cause to get information from the auction site?

Mr. JOHNSON. Although I have not personally been involved in any of those types of investigations, what I can tell you is that based on my limited interaction with some of those auction sites the answer is yes, they have been cooperative with the FBI and provided us with the assistance that we have requested, yes.

Mr. SCOTT. Are there any problems with jurisdiction, or which agency ought to be involved? Do you have problems in coordination to make sure that the Federal Government is doing what it can in an investigation without people tripping over themselves and not cooperating?

Mr. JOHNSON. Yes. No, I have had no experience—let me rephrase that—the level of cooperation between local, State, and Federal law enforcement with regard to this particular effort, as well as private industry, has been outstanding. We haven't had any issues that I am aware of where we haven't been able to work effectively together to address the problem.

Mr. SCOTT. Now, the investigation of the—Ranking Member of the full Committee has mentioned the investigation of these cases can be resource-intensive. What do you need—or, have you had to

prioritize and not investigate cases that you thought you could investigate and solve because of lack of resources?

Mr. JOHNSON. The answer to that question is yes, we have to prioritize on a daily basis, in terms of what cases we will investigate and dedicate resources to. One of the difficult things that we have to do is we have to select our target based on the intelligence that we have, that is one of the—one of the criteria that we have is making sure that we are on the right target, and those that don't meet certain criteria we will refer to local or State law enforcement.

Mr. SCOTT. Have you requested additional resources so that you could chase after more of the organized retail thieves?

Mr. JOHNSON. Can I ask somebody a question real quick?

The answer is yes, we have requested additional resources. Typically, or at least to my knowledge, they have not been successful to date.

Mr. SCOTT. If you could provide us with that information we—hopefully we can be helpful in that because it is my belief that the responses to your questions were criminal law is enough, the procedures are enough, and the problem in chasing down the thieves is lack of resources. So if we want to do something we have to give you the appropriate resources and that is our challenge.

Mr. JOHNSON. We will get that information for you.

Mr. SCOTT. Thank you.

Gentleman from Virginia?

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. Johnson, when we talk to retailers the most common complaint they have about the difficulty in dealing with organized retail crime is that the Federal law enforcement organizations just don't give them the time of day when it comes to dealing with these. They view it as just another shoplifting case or maybe a shoplifting case of a little greater magnitude, but they don't get enough effort in terms of digging beyond the person that may be apprehended in the store, or at a swap meet, or at a flea market, or whatever the case might be.

And these are national organized rings that really do require the Federal Government to step in. What do you say in response to that?

Mr. JOHNSON. What I will say is that yes, typically, as we have talked about today, typically these cases can be very resource-intensive. Generally speaking the FBI will approach these types of cases from a criminal enterprise theory, so what we are trying to do, as opposed to selecting one or two low-level boosters or fencers to try and develop a case on we try and look at the entire enterprise, which may be 10, 15, 20 or more individuals. And as a result of that, the investigative techniques that we typically utilize generally tend to be very expensive and require a lot of personnel to, you know, to utilize those particular techniques.

So what I can say is that as always, we can do a better job in terms of investigating these cases. We do the best we can with the resources that we have and we try and target the most sophisticated enterprises that are engaged in this conduct.

Mr. GOODLATTE. Now, last year how many of these types of investigations were conducted by the FBI?

Mr. JOHNSON. I can get you exact numbers, but my understanding is somewhere between 70 and 80 investigations were pending last fiscal year.

Mr. GOODLATTE. And how many of them were opened last year?

Mr. JOHNSON. I don't have that information right now.

Mr. GOODLATTE. If you could get us information about how many were opened and how many were closed so we would get a gauge for exactly how many investigations you are initiating per year that would be helpful to us, maybe going back over the last 3 or 4 years.

Mr. JOHNSON. Sure.

Mr. GOODLATTE. Would prosecutions of organized retail criminals increase if State and Federal felony thresholds were lowered?

Mr. JOHNSON. Could you repeat the question? I am sorry.

Mr. GOODLATTE. Yes. The question was, would prosecutions of organized retail criminals increase if State and Federal felony thresholds were lowered?

Mr. JOHNSON. Again, that is a difficult question to answer. What I can say is that, again, as the FBI has resource issues to deal with the United States Attorneys Offices have resources issues to deal with. So it is a question of whether or not there are available investigative and prosecutive resources to investigate and prosecute those cases.

Mr. GOODLATTE. In my opening statement I referred to the Law Enforcement Retail Partnership Network, and I am wondering what you can tell us about how that has improved your ability to investigate.

Mr. JOHNSON. As I mentioned in my statement, there is a lot of data in LERPnet currently. Law enforcement will have access through LEO Online very shortly—we are working through some technical issues right now—but what that will do is it will make that data available to a variety of local, State, and Federal law enforcement officers to go in and conduct some analysis in terms of trends or to try and connect the dots, if you will, between particular events that are happening in various locations throughout the United States.

Mr. GOODLATTE. Let me ask everyone on the panel, how do you typically become aware of ORC violations? It seems like once they are brought to your attention Federal law enforcement agencies can effectively prosecute these criminals.

What is the best way for Congress to help facilitate bringing these crimes to your attention, number one? And number two, is it a problem of not being aware of these things? Are the big box stores and other retailers who are suffering some serious problems from organized retail crime not bringing enough information to you or is it a problem of having the resources to investigate them further?

Well start with you, Mr. Hill.

Mr. HILL. Over the last 3 years we have only received information—we have investigated 21 of these types of cases. Last year we did eight that we attribute to organized retail crime groups, and those were referrals from either other law enforcement agencies, including my colleagues here, or the retailers themselves. So we are not getting a lot of information that, at least from the perspec-

tive of the Postal Service, is being used to facilitate these types of crimes that——

Mr. GOODLATTE. Well, that is interesting because I would assume that if you bought something on the Internet that it would be shipped to you using the mail in many instances, would it not? And therefore, that would entail your involvement. You could investigate those.

Mr. HILL. In many instances the mail jurisdiction is limited to the U.S. Mail, not to FedEx, not to UPS——

Mr. GOODLATTE. Right. So do you think criminals avoid using the U.S. Mail to avoid your investigative powers and focus on FedEx and UPS?

Mr. HILL. Well, we would like to think that they stay out of the mail because of our——

Mr. GOODLATTE. That would be an interesting question to have answered, because if they are evading your organization's involvement that would shift the focus down the table here, but it also would say maybe we need to be looking at some changes in the law to address that.

Mr. Large?

Mr. LARGE. Yes, sir. Typically we become aware of these cases through our access device investigations, and primarily that is through our task force model. We have over 100 retail fraud investigators that either participate on a full-or a part-time basis with either a financial crime task force or an electronic crime task force that are spread out throughout the country. They will bring cases to us typically——

Mr. GOODLATTE. Do you have much direct interaction with major retailers bringing matters to your attention?

Mr. LARGE. With their investigators, sir. Their investigators that participate with our task forces will bring cases directly to our agents. We get cases from State and local law enforcement——

Mr. GOODLATTE. Are you able to investigate all of the cases that are brought to your attention, or do you have limited resources and have to select amongst those?

Mr. LARGE. Well again, like my comrade said from the FBI, that is a tough question to answer. We will look into it and see if there is a nexus to organized criminal groups that are operating in multiple different States and see if we can build a bigger case from the small case, but we cannot investigate everything that is brought to our attention.

Mr. GOODLATTE. And Ms. Ayala?

Ms. AYALA. Well, we work closely with the National Retail Federation and RILA in order to determine what the large threat cities are, and they have polled their membership and due to our pilot program have been able to identify the top 10 cities, of which we selected four where we think ICE resources could best be able to investigate these cases. The industry provides leads to us at the headquarters level, and then we funnel the leads out to the field.

Mr. GOODLATTE. Thank you.

Mr. Chairman, my time is well expired, so thank you for your forbearance.

Mr. SCOTT. Thank you.

Gentleman from Michigan, Chairman of the full Committee, Mr. Conyers?

Mr. CONYERS. Thank you, Mr. Chairman. This is a good hearing.

I am preparing a memo along with our Chairwoman that is trying to get out of the room right now, and what we are going to recommend is that we meet with the head of the FBI, with the Secret Service, with the Postal—the same witnesses you have here—and try to get in front of—this is a crime, a new crime aspect that is going to grow, and if we just keep measuring how it grows every year it will keep on growing. It is probably out of hand now in a proportion that we are probably not aware of.

And I think meeting to try to get the resources that are going to be needed—just informally, we don't—our memo will not recommend another hearing, but that we just meet in your office and get down with it, and we didn't even include ICE. Ayala is probably the nicest person over there.

I mean, we only hear bad things about ICE in the Judiciary Committee, so we recognize that you have been deliberately selected to come over here and put a nice face on that outfit.

But I think this is good, and, Mr. Large, while you were arresting so many people did you get anybody on Wall Street while you were at it?

Mr. LARGE. None that I am aware of, sir.

Mr. CONYERS. Yes, well this is probably petty stuff. They don't deal in multimillion dollar crime—retail crime things. Why do you have to? You have got some many derivatives and new designs, many of which are not even regulated. So I just wanted to—any of those guys that might have fallen on hard times that just do this on the side.

Well, thank you, Mr. Chairman.

Mr. SCOTT. Thank you.

And I would point out that we have been working on this. LERPnet has helped coordinate, and the FBI has already testified on the record that criminal law and criminal procedures are sufficient to deal with it, but the thing we have not provided are appropriate resources.

These cases take a lot of people, a lot of investigation, a lot of stakeouts, and it is resource-intensive, and I think the meeting that you have suggested would be helpful that we could bring in and see exactly—the FBI has indicated that they will be providing us with some ideas about what kind of resources would be helpful. So that would be very helpful.

Mr. GOODLATTE. If the Chairman would yield, we would certainly like to participate in that on our side of the aisle, too.

Mr. SCOTT. The expectation would be that you would participate.

Mr. GOODLATTE. Thank you.

Mr. SCOTT. Thank you.

Gentleman from Illinois, Mr. Quigley?

Mr. QUIGLEY. Thank you, Mr. Chairman.

For any of the panelists—apologize if I——

Mr. SCOTT. Excuse me, Mr. Quigley. I thought the gentleman from Michigan had yielded back. He did. Okay, I am sorry. Proceed.

Mr. QUIGLEY. Okay.

The online marketplace companies, people resell stolen items—part of me thinks it is sort a needle in the haystack. I am not sure how they are possibly going to be able to police themselves. But in a perfect world, how do they police this sort of thing? And the question for all of you is, how well are they doing it?

I guess we will start with Mr. Johnson.

Mr. JOHNSON. I don't know how they would police themselves, to be perfectly honest with you. I would have to think about that question a little bit more before——

Mr. QUIGLEY. Not so much policing themselves but policing the marketplace that they provide.

Mr. JOHNSON. Yes, I believe that they are—I say they—online marketplaces are—some of them are looking at the postings on a daily basis and are attempting to identify those that just look suspicious. And based on those postings—again, this is just my understanding having talked to a couple of them—then they have investigators or somebody internally taking a look at what those postings are or what the items are, and then if they develop enough information to refer it to law enforcement they will. That is just based on my limited knowledge.

I am sorry, could you repeat the second half of that question?

Mr. QUIGLEY. Well I guess you sort of answered the question. How well are they doing what they can?

Mr. JOHNSON. Yes, and again, based on my experience working with a limited number of them, in my opinion I believe they realize that they have an issue, and they are actively trying to address it.

Mr. QUIGLEY. Thank you.

Ms. AYALA. Yes, I recently attended a RILA conference where I saw a presentation from eBay and some of the other online services where they do have mechanisms in place to look at the Internet as far as the volume of activity in a given timeframe, also multiple addresses or sites tied back to one or two individuals, so they are attempting to look at that. I know they are working closely with the federation on these issues.

Mr. QUIGLEY. Thank you.

Mr. LARGE. Yes, sir. While the Secret Service is not in a position really to evaluate their internal controls and the methods they use to detect this type of fraud, we do say—we can say that they do cooperate with us, they participate in our task forces, on occasion they have noted fraudulent activity and brought cases to us to investigate. So that we can give you an opinion on.

Mr. HILL. The legitimacy of the auction house is the start. That is probably the beginning because you have a lot of very legitimate, well-established businesses that are in this sector, and then you have other ones that aren't. Those legitimate businesses that we have worked with have protective measures in place to police the use of the Internet for purposes of their operation.

The problem with this is obviously that they don't control the inventory. It is not like a pawn shop or fencing operation where you have the product there. They are basing it on the assurance that the seller is that I have this product, and I am going to sell it on your site.

In terms of what they can do for policing, I think all they can do is establish a good business relationship, the legitimacy of the

seller, and if they have a bad seller, or picked a bad seller, they take them down off the system and deny them access.

Mr. QUIGLEY. Do you also understand that I guess some sites would be too good to be true, right? Blue jeans for $10 or something like that, and they are all new. Some of that must be obvious.

I guess in the end what I would like is, if it is possible in the future for us to advise us on what else they might be able to do, again, in a perfect world. Are there computerized systems or is it a random check, or as you suggested, multiple sites for one person or a deal that is too good to be true—what else can they be doing to help monitor this and send information of suspected sites to all of us? Thank you.

Mr. SCOTT. Does the gentleman yield back?

Mr. QUIGLEY. Yes, I yield back.

Mr. SCOTT. Thank you.

We have talked about meetings with law enforcement. I think it would also be helpful if we—and we have in the room representatives of the retail industry and the Internet industry—if they could be in the room and discuss what some of the problems are at the same time.

But I would like to thank all of our witnesses for their testimony today. Members——

Ms. LOFGREN. Mr. Chairman?

Mr. SCOTT. [Off mike.]

Ms. LOFGREN. I don't have a lot of questions, Mr. Chairman——

Mr. SCOTT. I am sorry. I looked, and I didn't see you, and you——

Ms. LOFGREN. That is all right. I was getting a cup of coffee.

I just wanted to make a quick——

Mr. SCOTT. Gentlelady is recognized for 5 minutes.

Ms. LOFGREN [continuing]. A quick comment because eBay actually is headquartered in my congressional district, and as a consequence I am in touch with them often. I have, you know, thousands of constituents who work there, and I think they take this very, very seriously, and certainly with local law enforcement as well as federal, if there is an issue they are all over it because, you know, they value the law.

And I would just like to note that hundreds of thousands of Americans have their entire business and livelihoods are because of eBay. And so there is that aspect to it as well. There are just many Americans who earn a living by selling things through eBay and we need to value that as well. It is a great source of income for Americans.

I just wanted to leap to the defense of my constituents, Mr. Chairman, and thank you for holding this hearing.

Mr. SCOTT. Thank you.

We have to leave in just a moment. I understand the Ranking Member pro temp has another question.

Mr. GOODLATTE. Thank you, Mr. Chairman, and this will be quick, and it pertains to the gentlewoman from California's constituents.

One of the issues that comes up is that a lot of this activity may take place on the Internet. And the problem is that the bricks and mortar retailers have a problem with getting information about

whether particular Web sites have information about a product that they suspect is being fenced on the Internet, but they don't have any real proof of it unless they can gather information.

Well, that draws a response from the online businesses that they don't want other competitors being able to ask them literally thousands of questions regarding their customers that are doing business on their Web sites and so on without the involvement of law enforcement.

So we have been trying to find some common ground here to work out this situation and move it forward. And my question to you, Mr. Johnson, is would you be willing to participate in a program to allow expedited requests for information from online marketplaces when probably cause is found that goods being sold online are stolen?

Mr. JOHNSON. I think the answer to that question is yes.

Mr. GOODLATTE. And if we gave you the resources to have some people dedicated to that information—gathering that information that might help the bricks and mortar folks and allow the online folks to have greater cooperation, greater results without having to interface with private citizens demanding information from them that they don't think it is appropriate for them to be asking.

Mr. JOHNSON. Correct.

Mr. GOODLATTE. Thank you very much.

Mr. SCOTT. Thank you.

And I would like to thank our witnesses for their testimony today. Members may have additional written questions which we will forward to you and ask you to answer as promptly as possible so that the answers may be made part of the hearing record.

Without objection the case summary and chart describing Target's double deal investigation and additional statements that have been submitted to the Subcommittee from the Coalition Against Retail Crime, the Food Marketing Institute, the National Association of Chain Drug Stores, the National Insurance Crime Bureau will all be entered into the record. The record will remain open for 1 week for the submission of additional material.

And without objection, the Subcommittee stands adjourned.

[Whereupon, at 10:47 a.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Target Double Deal Investigation

Target's Double Deal case involved a business in a criminal enterprise with over 150 boosters selling brand new merchandise stolen from retailers in Minnesota, Wisconsin, Iowa, California, New York, North Dakota, and Missouri. Boosters obtained stolen merchandise through thefts, check and credit fraud schemes. The business then sold the merchandise on eBay and other online sites, representing itself as a legitimate wholesaler of media products.

Professional Booster Crews delivering merchandise to the business after multi-state shoplifting trip

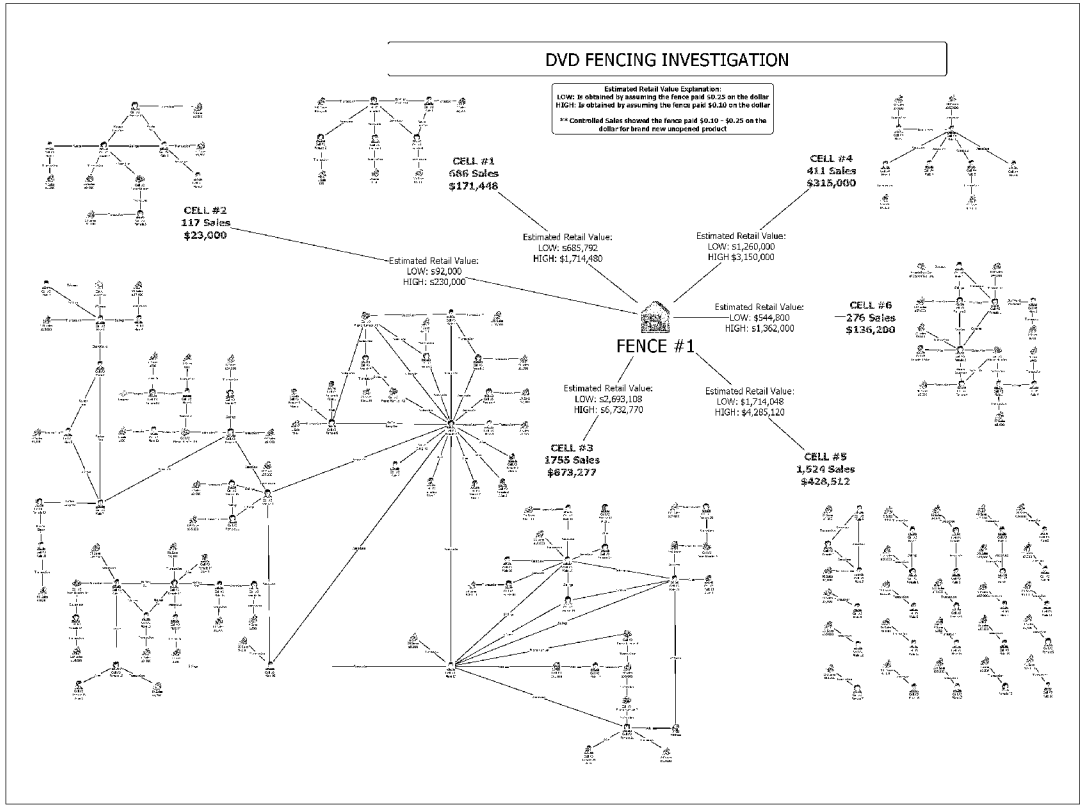
Target investigators were notified of the business' practices through interviews of shoplifters apprehended at Target stores throughout 2002 – 2005. Target investigators approached local law enforcement regarding the business on multiple occasions. During that timeframe, local law enforcement met with the business owners several times explaining they should stop buying new product from these individuals.

In May, 2006, local law enforcement contacted Target investigators. Their agency had obtained intelligence that the business was continuing to buy new product from boosters. Target investigators conducted mobile surveillance of professional booster crews that were selling to the business in order to establish the product was stolen and develop informants who conducted controlled sales to the business using merchandise provided by Target. During these sales the business requested specific merchandise, paying boosters roughly 15% of the retail value for merchandise they later sold at wholesale and near retail prices.

Over $14000 in stolen merchandise recovered during a booster car search after they crossed into Minnesota.

The US Postal Inspection Service in Minnesota was notified in January 2007. Inspectors worked steadily to coordinate the investigations with multiple retailers and agencies. Target investigators provided GPS tracking equipment to LE to establish multi-state boosting trips of booster crews, ultimately returning to the business where they sold the product. Inspectors and Target investigators conducted covert purchases through eBay of stolen merchandise.

In September, 2007 search warrants produced over $250,000 in stolen merchandise seized from the business. Target's Forensic lab in Minneapolis was used to examine seized computers. Target's known losses due to boosters selling to the business was $56,000. Retail industry losses are estimated at $11 million over 4 years. US Attorney's office in Minnesota prosecuted multiple subjects for conspiracy to commit mail fraud and wire fraud who have pled guilty. Additional charges are pending.


DVD FENCING INVESTIGATION
Estimated Retail Value Explanation:
LOW: Is obtained by assuming the fence paid $0.25 on the dollar
HIGH: Is obtained by assuming the fence paid $0.30 on the dollar
** Controlled Sales showed the fence paid $0.10 - $0.25 on the dollar for brand new unopened product
CELL #1
686 Sales
$171,448
CELL #2
117 Sales
$23,000
CELL #3
1755 Sales
$873,277
CELL #4
411 Sales
$315,000
CELL #5
1,524 Sales
$428,512
CELL #6
276 Sales
$136,200
Estimated Retail Value:
LOW: $685,792
HIGH: $1,714,480
Estimated Retail Value:
LOW: $92,000
HIGH: $230,000
Estimated Retail Value:
LOW: $1,260,000
HIGH $3,150,000
Estimated Retail Value:
LOW: $544,800
HIGH: $1,362,000
Estimated Retail Value:
LOW: $2,693,108
HIGH: $6,732,770
Estimated Retail Value:
LOW: $1,714,048
HIGH: $4,285,120
FENCE #1

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism and
Homeland Security

Hearing on
"Combating Organized Retail Crime – The Role of Federal Law Enforcement"

on Behalf of
The Coalition Against Organized Retail Crime
Arlington, VA

November 5, 2009

Today before a hearing of the House Judiciary Committee, Subcommittee of Crime, Terrorism and Homeland Security, representatives from the retail industry and law enforcement would like to present their case for strong federal legislation to combat organized retail crime (ORC). The Coalition Against Organized Retail Crime (CAORC) thanks Subcommittee Chairman Bobby Scott for his steadfast dedication and support for tackling this growing crime and commends the Chairman for his thoughtful leadership in holding a hearing to address this important issue.

By way of background, The CAORC, formed in 2001, is composed of 37 national manufacturing and retail organizations as well as individual companies that have come together to fight this growing crime. The Coalition's web site can be accessed at www.stopretailcrime.com. The CAORC has previously provided testimony to Congress on this issue in March of 2005 and October of 2007. The Coalition strongly supports enactment of pending federal legislation to combat ORC in the House of Representatives. Those bills include: The E-Fencing Enforcement Act of 2009, H.R. 1166, introduced by Chairman Scott, and the Organized Retail Crime Act of 2009, H.R. 1173, introduced by Reps. Brad Ellsworth and Jim Jordan.

Organized Retail Crime:

ORC involves sophisticated crime rings that steal and stockpile huge quantities of merchandise that they then sell, often to unwitting buyers. ORC gangs target high value consumer goods such as power tools, gift cards, razors and disposable blades, over the counter medicine, and other items that are in high demand and often easily concealable. The stolen merchandise is then sold through flea markets, swap meets, pawn shops and, increasingly, through Internet auction sites.ORC gang members use other fraudulent means to acquire merchandise from retail stores, such as writing bad checks and using stolen credit cards numbers. In many instances an ORC gang will switch the UPC label or bar code on an item to obtain the item at a lesser cost. In addition, these criminals will produce fraudulent receipts to obtain cash or a gift card; often, the gift card will then be sold online for cash.

This criminal activity puts consumers and communities at risk, strips states of needed sales tax revenue and costs retailers billions of dollars each year. Merchandise, such as baby formula and diabetic test strips, which can be damaged if not stored at proper temperatures, is often mishandled after being stolen. It is not uncommon for retail investigators recovering the stolen merchandise to find their products stored in extremely hot conditions or in the trunk of a vehicle. ORC gangs will often switch labels or remove expiration dates to take advantage of unsuspecting consumers who are placed at risk when a diabetic test strips fail or baby formula spoils.

Consumers and retailers are not the only victims in instances of ORC. The losses in state sales taxes are staggering. The CAORC conservatively estimates that the 46 states that have a state sales tax are deprived of approximately $1.6 billion each year in lost sales tax revenue. States incurring the largest losses include California at $228.5

million, Texas at $153 million and Florida with $132 million. Additionally, the proceeds derived from ORC are used to fund other criminal activity, putting communities at risk.

E-Fencing and Online Market Places:

The popularity of Internet auction sites for fencing stolen merchandise is increasingly evident over the past several years. ORC gangs have migrated many of their activities to the Internet and unfortunately laws and law enforcement have had a difficult time keeping pace with this migration. E-fencing is a user-friendly, instantaneous and anonymous means to facilitate ORC behavior. While flea markets, swap meets and pawn shops have become increasingly regulated over the years, the online marketplaces have yet to adopt proactive measures to stop the stolen merchandise from being sold on their sites.

It is not uncommon for retailers to find proprietary items, new in the box, listed on online marketplaces for significantly less than the retailer can buy the product directly from the manufacturer. Often times merchandise is sold in multiple quantities, boxes, or pallets. However, retailers have encountered resistance when they have sought help from online auction sites in pursuing ORC investigations. In one recent example, a large retailer found sixty boxes of over the counter medication listed on eBay for 20% of the product's cost. The retailer has extensively tracked the theft of this medication from its stores. When the retailer approached eBay with evidence of a theft ring likely connected to this particular eBay account, eBay refused to provide information about the account holder. This information was vital to the retailer's investigative efforts in gaining information about the theft ring. Unfortunately, these experiences are typical and affect all retailers.

Recently, there have been a number of positive changes in eBay's Partnering with Retailers Offensively Against Crime and Theft (PROACT) program. These modest changes reflect eBay's acceptance that significant amounts of stolen product continues to be trafficked through their sites. Although many retailers see these changes as constructive, the program still falls far short of what would be reasonably expected of a re-sale business with a long record of facilitating the sale of stolen goods. The eBay program maintains its passive approach by requiring retailers to make elaborate cases that are subjected to an internal eBay self policing process lacking in any reasonable level of transparency. Moreover, there is no external consequence to eBay for failing to assist, and retailers have no independent ability to hold the company accountable for continuing to traffic in stolen goods. The cursory changes to a program such as PROACT are not enough to deter this type of crime and, instead, these ORC rings continue to hide behind the anonymity of the Internet.

Currently, when a retailer reaches out to the eBay for case information, eBay will ask for case information and then make the independent analysis of whether there is enough evidence to warrant any sharing of information. Since eBay makes a percentage of profit with every sale made through the company's site, they are inherently conflicted from policing themselves absent any external, independent, and consequential influence.

In a similar example, a large hardware chain had significant evidence of an ORC ring in Connecticut. Extensive witness testimony, controlled sales, and video surveillance indicated that a pawn shop chain was coordinating the theft of power tools and fencing the tools on eBay. The investigation was able to identify specific online accounts where stolen goods were being fenced. When the retailer requested information from eBay regarding the accounts, eBay declined the request. A month later, local law enforcement raided the pawn shops and discovered a massive eBay centered operation. Rows of computers were set up to post items online and to manage auctions. Products were organized in storage for quick order fulfillment. The pawn shops were owned by an Austrian national. The lack of information from eBay prevented the investigators from uncovering the true depths of the operation. Although four pawnshops were raided and over $160,000.00 in stolen property was recovered, the investigators were forced to pursue lesser charges of possession of stolen property, instead of the more serious offenses worthy of such a large enterprise.

Many ORC case investigations have been stymied by an uncooperative response from online marketplaces that delay providing helpful information to law enforcement and retailers. The incremental technical changes that are being asked of online market providers in the pending federal legislation are not difficult to incorporate to existing point of sale systems. In fact, many retailers use similar models with internal controls to monitor suspicious behavior and activity within their own stores. A good example of this is a retailer who buys and sells pre-owned products, such as gaming products. Internal triggers alert retail associates if someone has returned more than one of the same item as well as if that person has tried to return items at more than one location. These flags generate higher scrutiny and enable the retailer to deploy reasonable efforts to guard against the acceptance of stolen merchandise.

We estimate that millions of dollars worth of stolen items have been fenced through eBay and other online marketplaces. Any good corporate citizen does not want to aid in the sale and profit of stolen merchandise. Federal legislation is needed to increase the civil and criminal liabilities for facilitating this type of criminal behavior.

Relationship with Federal Law Enforcement:

Retailer relationships with federal law enforcement vary widely depending on a number of factors. These factors include location, office resources, office familiarity and/or experience with ORC cases, and threshold guidelines. Most commonly, retail loss prevention executives do not interact directly with the U.S. Attorneys' offices at the initial investigation stages. Typically, the loss prevention professional will present information to an agent with the FBI, Secret Service, Postal Inspectors, the Department of Agriculture, Immigrations and Customs Enforcement or other federal agency. The choice of agency varies depending on location. While some federal offices are extremely effective in responding to an investigative request, many unfortunately are not. The lack of a national strategy to address ORC produces a sporadic and weak federal response that is constantly being exploited by ORC rings.

The information presented to federal law enforcement typically includes surveillance video, link charts, witness statements, and controlled sales. Extensive investigative

work is conducted prior to seeking the assistance of the federal investigator. The federal investigator will then present the case to the appropriate U.S. Attorney's office and provide the loss prevention executive with the U.S. Attorney's response. If the U.S. Attorney's office takes a case, often times the retail loss prevention executive will provide supplemental information to aid in the prosecution process.

In most instances, the decision to take a case related to ORC lies within the discretion of U.S. Attorney's office and depends upon what they believe meets their thresholds. Failure to meet case amount thresholds is often the reason given for a decline. Thresholds are defined differently depending on the office. Some offices require a per incident threshold (ex. $5,000.00 per theft) which is extremely difficult to meet in cases of ORC because the criminals often know the felony thresholds within a given area and will steal beneath those thresholds at any given retailer. The aggregate amount of these thefts add up to millions of dollars in losses, but the incident thresholds would prevent federal law enforcement offices from getting involved in the case.

Aggregate thresholds are also used to govern whether the federal government will become involved in a case. Aggregate thresholds vary by location. Without police powers or subpoena authority, retailers are forced to provide evidence that a case has a value in the hundreds of thousands of dollars prior to the engagement of federal law enforcement. As a result, retailers take months and even years monitoring theft rings they know are stealing significant amounts of their products. They have no choice but to allow the crime rings to be amply successful in order that the retailer receives the federal assistance they so desperately need. The proof requirements for these valuations are extremely arduous. Without investigative powers, retailers are limited in their ability to determine the true magnitude of a criminal enterprise. A case that looks like a hundred thousand dollar case can easily be a hundred million dollar case once a federal investigation is commenced. Other factors, such as qualitative information on the enterprise, interstate presence, and levels of sophistication, should carry equal weight in intake case evaluation.

In addition to threshold matters, cases have been declined due to lacking "organized crime" involvement. The aforementioned Connecticut case was apparently rejected by the New Haven FBI office due to the lack of "organized crime involvement". A large retailer had reasonable suspicion that a pawn shop was receiving stolen items and fencing the merchandise through various pawn shop locations across the state of Connecticut and through multiple eBay accounts. A task force was set up to investigate the fencing operation. In the preliminary meetings, New Haven FBI investigators were invited to participate in the sharing of information and apprehension of the ORC ring. After attending early meetings, these investigators found there to be no evidence of organized crime and no longer participated.

Once the bust occurred, multiple large retailers and local law enforcement seized an aggregated $160,000 dollars worth of merchandise from the pawn shop locations. There were multiple eBay account transaction records and proprietary marked merchandise from various retail outlets. The owner of the pawn shop was an Austrian national and received much of the profits overseas. The tracking of those profits was never investigated because of the lack of attention by the appropriate federal

investigative body. The case would have been investigated more efficiently and thoroughly had federal law enforcement provided support when invited to do so.

Retailers need law enforcement partners to perform many essential aspects of the investigation. Delays in decisions to take cases mean many more financial losses from merchandise that continues to be stolen. The quantifiable amount of such delays in the investigation and prosecution of the cases is significant.

Education and training continues to be a large factor that contributes to the successful investigation and prosecution of ORC cases. With regard to training, our retailers find that many cases are much more successful when the federal agent and U.S. Attorney's office is more familiar with ORC. In some instances our loss prevention executives find it harder to engage an agent if there is no familiarity with these types of cases and ORC's broad impact in interstate commerce and other types of crimes. The retail loss prevention investigator will often have to start the process with educating that person in hopes that the agent will look globally beyond the isolated retail theft to the magnitude and impact of ORC.

Many state retail associations are working with retailers to develop programs that will train local and state law enforcement to address ORC. We believe a similar federal approach would be of extreme value in providing investigators with the tools and resources they need to identify ORC crimes and gather relevant physical evidence to file applicable federal criminal charges. We urge the various federal agencies present at the hearing to consider such proposals as they develop their responses to ORC.

Conclusion:

The focus of today's hearing is on the current steps federal law enforcement is taking to combat this issue and the CAORC applauds their current efforts. Retailers depend on their law enforcement partners to perform many essential aspects of investigations and we look forward to working with federal agencies on a coordinated federal strategy to address this growing crime. We also encourage federal law enforcement to consider education and training programs within their various agencies to better equip their investigators with the knowledge and tools to proactively and effectively identify ORC activity.

The losses to our communities, consumers, and retailers are significant. We urge members of Congress to support the proposals (H.R. 1166/H.R. 1173) introduced in this Congress, which would strengthen the tools that law enforcement needs to effectively prosecute and deter this criminal behavior.

Lastly, the CAORC calls upon online marketplaces to better police their sites and work with retailers and law enforcement on preventative measures to deter and prevent the sale of stolen goods on their sites.

Once again, we look forward to working with members of Congress and federal law enforcement agencies to ensure the safety of our consumers and provide the tools necessary to combat ORC.

About the Coalition Against Organized Retail Crime

Coalition Members: Abbott Laboratories, Ahold USA, Inc., Consumer Healthcare Products Association, Cosmetic, Toiletry, and Fragrance Association, CVS/pharmacy, Duane Reade, Eastman Kodak Company, Food Lion, LLC, Food Marketing Institute, Giant Food LLC, Giant Food Stores LLC, GlaxoSmithKline, Grocery Manufacturers/Food Products Association, The Home Depot, International Formula Council, The Kroger Co., Macy's, National Association of Chain Drug Stores, National Association of Convenience Stores, National Community Pharmacists Association, National Insurance Crime Bureau, National Retail Federation, Nestle, Publix Super Markets, Inc., Retail Industry Leaders Association, Rite Aid Corporation, Safeway Inc., Security Industry Association, SUPERVALU, The Stop & Shop Supermarket Company, Target Corporation, Tops Markets, LLC, Inc., Universal Surveillance Systems, Virginia Retail Federation, Wal-Mart Stores, Walgreen Co.

Written Testimony of
Food Marketing Institute

"Combating Organized Retail Crime – The Role of Federal Law Enforcement"

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

Thursday, November 5, 2009

ORGANIZED RETAIL CRIME

THE FOOD MARKETING INSTITUTE

EXECUTIVE SUMMARY - TESTIMONY

Organized Retail Crime or ORC is a large nationwide problem that needs a federal solution. According to federal law enforcement officials and loss prevention experts, losses attributed to ORC activity are as much as $30 billion annually.

Every segment of the retail community is being victimized by these sophisticated theft rings including supermarkets, pharmacies, specialty shops, and department stores among others.

ORC is not petty shoplifting. Rather ORC involves sophisticated criminal enterprises that move quickly from community to community and across state lines stealing large quantities of merchandise from retail stores.

The health and safety of consumers is at risk because ORC rings are engaged in the theft and resale of products that are regulated by FDA including infant formula, over-the-counter medicines and diabetic supplies. ORC rings often times will tamper with these types of products and modify or change their labels and expiration dates.

ORC gangs once relied exclusively on the black market and locations like flea markets and pawn shops to sell their ill-gotten goods. Now these criminal enterprises have embraced technology and are selling stolen merchandise on Internet auction sites.

Federal legislation needs to be enacted to combat ORC and deter the sale of stolen merchandise over the Internet. For this very reason, **FMI strongly supports legislation (H. R. 1166 – H. R. 1173) to address ORC more extensively from a federal perspective.**

H. R. 1166 and H. R. 1173 will not impose unreasonable burdens on the Internet. These initiatives simply call for a few modest transparency and recordkeeping requirements for Internet auction sites and high volume sellers. High volume sellers are individuals who conduct at least $12,000 in sales over an internet auction site in a 12-month period.

H. R. 1166 and H. R. 1173 will not require more resources from federal law enforcement agencies if these initiatives are enacted into law. In fact, because the ORC legislation will discourage the sale of stolen merchandise on the Internet, federal law enforcement will be able to devote their limited resources on other priorities.

INTRODUCTION

The Food Marketing Institute (FMI) on behalf of our supermarket retail and wholesaler members submits the following testimony to the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security in response to this oversight hearing relating to Organized Retail Crime (ORC). FMI commends Chairman Bobby Scott (D-VA) for his leadership on ORC and the supermarket industry also wishes to express appreciation and acknowledge the ongoing efforts of state and federal law enforcement to combat this serious criminal activity.

ORGANIZED RETAIL CRIME - A $30 BILLION PROBLEM

Organized Retail Crime or ORC is a large nationwide problem that needs a federal solution. According to federal law enforcement officials and loss prevention experts, retail losses attributed to ORC activity are as much as $30 billion annually.

Every segment of the retail community is being victimized by these sophisticated theft rings including supermarkets, pharmacies, specialty shops, and department stores among others.

ORC is not petty shoplifting. Rather ORC involves sophisticated criminal enterprises that move quickly from community to community and across state lines stealing large quantities of merchandise from retail stores.

ORC – HEALTH & SAFETY RISK TO CONSUMERS

The health and safety of consumers is at risk because ORC rings are engaged in the theft and resale of products that are regulated by FDA including infant formula, over-the-counter medicines and diabetic supplies. ORC rings will often tamper with these types of products and modify or change their labels and expiration dates endangering the health and safety of unknowing consumers.

STATE BUDGETS ARE IMPACTED

State budgets are also impacted by these criminal enterprises. FMI estimates that of the 46 states that have a state sales tax, these jurisdictions are foregoing about **$1.6 billion each year in lost sales tax revenue as a result of ORC activity.**

ORC gangs once relied exclusively on the black market and locations like flea markets and pawn shops to sell stolen goods. Now these criminal enterprises have embraced technology and are selling stolen merchandise over the Internet.

More than a dozen states have enacted laws that provide for more stringent penalties and fines to combat ORC, but these new laws cannot address the emerging trend of the sale of stolen merchandise over the Internet. Clearly, Federal legislation is needed to thwart and deter the posting and the sale of stolen products on Internet auction sites. **And that is**

why FMI strongly supports legislation (H. R. 1166 and H. R. 1173) to address ORC more extensively from a federal perspective. These initiatives go after both the off-line and on-line sale of stolen merchandise by ORC theft rings.

FMI firmly believes H. R. 1166 and H. R. 1173 will not impose unreasonable burdens on the Internet. These initiatives simply call for a few modest transparency and recordkeeping requirements for Internet auction sites and "high volume" sellers. High volume sellers are defined as individuals who conduct at least $12,000 in sales over an Internet auction site in a 12-month period. The legislation's minimal transparency provisions call for the posting or record retention of each high volume seller's name, address and phone number similar to what is already required in Great Britain by the EC Directive Regulations of 2002.

H. R. 1166 and H. R. 1173 will not require more resources from federal law enforcement agencies if these initiatives are enacted into law. In fact, because the ORC legislation will discourage the sale of stolen merchandise on the Internet, federal law enforcement agencies will be able to devote their limited resources on other priorities.

STOLEN GOODS SOLD OVER THE INTERNET

To illustrate the magnitude of the problem regarding stolen products being sold over Internet, FMI wishes to bring the following cases to the Subcommittee's attention:

In 2008, an enormous organized retail crime ring was broken up in **Polk County, Florida**. What began as a single shoplifting investigation turned up a sophisticated enterprise that stole up to $100 million in medicine, health and beauty aids. Operating for at least five years, the ORC ring operated out of two warehouses, three flea markets and **two websites.**

In June of 2008, state and federal law enforcement broke up two ORC rings in the **San Jose / San Francisco Bay area**. Seventeen individuals were arrested and over $5.5 million worth of stolen merchandise was recovered including razor blades, infant formula, teeth whitening strips and otc medicines that were being resold through storefronts, flea markets and **the Internet.**

Sensitive stolen military technology including expensive night vision equipment and F-14 components was being illegally sold on **E-Bay and Craig's List according to a recent Government Accounting Office Report (GAO-08-6447) released in the Spring of 2008.**

In 2008, the Federal Trade Commission received a record number of complaints, some 160,000, related to Internet fraud linked to losses of $200 million. Half of the complaints involved **online auctions.**

An **Atlanta, Georgia** couple was prosecuted recently for selling at least $150,000 worth of fraudulently obtained gift cards on **an Internet auction site.**

A couple in **Chicago, Illinois**, sold about $3 million worth of stolen merchandise on an **Internet auction site** before being stopped by the Federal Bureau of Investigation (FBI) and local police.

In February of 2008, seven individuals were indicted in **Kansas City, Missouri** for selling $1.2 million worth of stolen merchandise on an **Internet auction site.**

In November of 2005, eleven individuals were indicted in **Chicago, Illinois** by a federal grand jury for selling more than $2 million worth of stolen merchandise through an **Internet auction site.**

In August of 2009, more than a dozen individuals who were pawn shop employees were arrested in Connecticut by local law enforcement for selling stolen merchandise through **an online auctioneer**.

Two individuals were arrested for selling more than $6 million in pirated software **over the Internet** between late 2002 through October 2005.

In September of 2008, the head of an ORC ring was arrested in **Queens, New York**, for selling $80,000 worth of stolen Victoria Secret lingerie on an **Internet auction site.**

Forty nine individuals operating a multistate ORC network were federally prosecuted. The investigation led to the seizure of more than $3 million in stolen merchandise and $950,000 in cash. The suspects told federal investigators they resold much of the stolen product on an **Internet auction site because of the anonymity assured by the site.**

A U. S. Postal Service employee in March of 2009 was charged with stealing more than $600,000 in postage stamps. The individual sold the stolen stamps for less than their face value on an **Internet auction site** starting back in 2000.

CONCLUSION

Clearly, Internet auction sites need to be held more accountable for what is being posted and sold on their platforms. Allowing Internet auction sites to sit idly by while making a profit on the posting and sale of stolen merchandise is simply wrong and should not be tolerated. For this very reason, **FMI and our supermarket members support and urge the enactment of H. R. 1166 and H. R. 1173**.

To conclude, FMI appreciates the opportunity to provide testimony for the record and we urge the Subcommittee to act expeditiously in favor of the pending legislation that provides for long overdue federal solutions to the problems relating to Organized Retail Crime.

NICB - Online Marketplace Issues

- NICB investigations reveal that online marketplaces are often used as a source to fence stolen goods.
- In the course of our property/casualty investigations, we find large dollar losses to the national retail community.
- The types of stolen goods most often seen by NICB range from autos, motorcycles, vehicle component parts such as catalytic converters, high intensity headlights, air bags to electronic equipment such as televisions, video recorders and MP3 players.
- No area of the country is immune as the mounting dollar losses are reflected nationwide.
- Online marketplaces can often become the fraud victims as organized rings will conspire to defraud the sites that provide or offer financial assistance to the buyer/seller transaction.
- Tightening the requirements to sell items through online marketplaces would dramatically reduce the stolen goods issues.

STATEMENT OF:
THE NATIONAL ASSOCIATION OF CHAIN DRUG STORES
ALEXANDRIA, VIRGINIA

TO:
THE UNITED STATES HOUSE OF REPRESENTATIVES
HOUSE JUDICIARY COMMITTEE
SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY

ON

COMBATING ORGANIZED RETAIL CRIME
THE ROLE OF FEDERAL LAW ENFORCEMENT

NOVEMBER 5, 2009

INTRODUCTION

Chairman Scott, Ranking Member Gohmert and Members of the Crime, Terrorism, and Homeland Security Subcommittee: the National Association of Chain Drug Stores (NACDS) is pleased to submit a statement for the record on the growing problem of organized retail crime (ORC). Our member companies appreciate your commitment to ending ORC and its harmful impact to consumers, businesses and federal and state governments. We also appreciate that Chairman Scott has scheduled this hearing to bring much needed attention to this serious issue. As a member of the Coalition Against Organized Retail Crime, NACDS is actively engaged in efforts to address the large-quantity theft and re-sale of consumer products through flea markets, pawn shops, retail establishments as well as on-line auction sites. We offer our views to help this Subcommittee and Congress adequately address the problem of ORC through effective federal legislation.

NACDS represents 154 traditional drug stores, supermarkets, and mass merchants with pharmacies – from regional chains with four stores to national companies. NACDS members also include more than 900 pharmacy and front-end suppliers, and over 70 international members from 24 countries. Chains operate 37,000 pharmacies, and employ more than 2.5 million employees, including 118,000 full-time pharmacists. They fill more than 2.5 billion prescriptions annually, which is more than 72 percent of annual prescriptions in the United States. The total economic impact of all retail stores with pharmacies transcends their $815 billion in annual sales. Every $1 spent in these stores creates a ripple effect of $3.82 in other industries, for a total economic impact of $3.11 trillion, equal to 26 percent of GDP. They are the largest sellers of non-prescription products and other routine healthcare consumer goods. For more information about NACDS, visit www.NACDS.org.

Unlike trivial theft or shoplifting, ORC involves complex schemes undertaken by highly dangerous and coordinated criminals, who steal large quantities of goods from multiple retail stores as they move through different towns and states and divert the stolen goods back into the stream of commerce. All too often, these products are resold through on-line auction houses and similar websites, which are hard to monitor by the authorities given the volume of products involved and are not always within reach of the law enforcement.

ORC reduces consumer access to goods and services, increases the cost of doing business for retailers, eliminates an important source of revenue for state governments and, more importantly, places public health at grave danger. Despite the best efforts of state police and prosecutors, the problem of ORC continues to grow at an alarming rate, which necessitates the federal government to take action. Therefore, NACDS strongly urges Congress to pass legislation to deter and punish ORC at the federal level.

ORC PUTS FINANCIAL STRAIN ON RETAILERS AND THE GOVERNMENT

ORC results in significant economic losses and inefficiencies in the marketplace – to the tune of $30 billion annually. Retailers sustain losses from the theft of their goods, unrealized profits, and expenditures related to security, additional personnel and training, and equipment to combat ORC. These losses amount to billions of dollars that could otherwise have been spent on business

expansion and development, additional job creation or improvement of product selection. In addition, some retailers unknowingly repurchase these products when the stolen goods are diverted back into to the legitimate stream of commerce, placing consumers at risk.

The government is also greatly impacted by ORC. State and local governments lose vital tax revenue as a result of lost sales. Stolen items that are re-sold at Internet auction sites or flea markets are not subject to sales tax, thereby adding to the problem of lost revenue. Further, law enforcement resources are perpetually engaged in apprehending repeat offenders who engage in ORC because of weak and ineffective laws. These losses and additional expenses to fight ORC put significant stress on state government budgets and resources, which are already strained.

ORC INCREASES CONSUMER PRICES AND REDUCES ACCESS TO GOODS AND SERVICES

ORC also impacts consumers since losses sustained by retailers are passed on to consumers in the form of higher prices. Retailers have no choice but to increase prices of all goods to mitigate the overall losses they sustain due to ORC. However, the impact on consumers is not limited to increased prices. As retailers shift their financial resources to technologies and measures to control ORC, their ability to expand the scope and range of their products becomes severely limited. Retailers are also forced to restrict access to certain products by locking them in cases or placing them behind the counter, making it more difficult for a consumer to purchase such products. Thus, consumers may be denied access to the important products they expect in the retail marketplace.

ORC JEOPARDIZES THE PUBLIC'S HEALTH

ORC creates enormous public health risks. ORC gangs focus on high demand goods such as infant formulas, baby foods, over-the-counter (OTC) medicines and medical devices, and other consumer healthcare products. These goods come in small packages, are easy to conceal and steal and even easier to re-sell due to their high demand, which makes them very appealing to ORC gangs.

OTC medicines, baby formulas and other healthcare products can become dangerous if the standards related to their storage, handling and distribution are not closely followed. Traditional retailers follow the storage, handling and distribution standards of these products as required. ORC gangs and "fences" who sell stolen products through flea-markets, on-line auction sites and other non-traditional sellers do not abide by these standards, placing consumer safety at peril. ORC gangs also alter the labeling -- particularly the expiration date -- of OTC medicines, infant formula, and other consumer healthcare products. Tampering with OTC medicines and other healthcare products is a threat to consumer safety; nonetheless, these acts are commonplace in these criminal enterprises.

In addition, ORC gangs routinely engage in violent activities that threaten the safety of consumers and retail employees. Moreover, income from ORC is believed to benefit individuals and organizations involved in drug trafficking, terrorism and gangs, such as MS-13, who use the money to support their activities, including using illegal aliens as thieves to "reimburse" the gang

for their relocation to the US. These criminal activities will continue as long as ORC remains a profitable and low-risk crime.

ENACT H.R. 1173 AND H.R. 1166 TO DETER AND PUNISH ORC

Currently, state laws do not provide an effective deterrent against ORC. In most states, thefts that do not exceed $500 in a single location or instance are still classified as misdemeanors, allowing ORC gangs to steal thousands of dollars worth of merchandise from different stores in a single day and risk nothing greater than a misdemeanor charge and a small fine in each case.

Given the costs of ORC to the national economy and consumers, Congress has attempted to address the problem at the national level. Congress recently passed legislation that established an FBI taskforce to combat organized retail theft; however, the taskforce has not received adequate funding or manpower to combat ORC effectively. Stronger federal legislation is therefore needed to effectively deter and punish ORC.

Congress must provide law enforcement with the necessary tools to combat ORC as a federal crime. In addition, unregulated venues such as flea markets and online auction houses and similar websites that sell the fruits of ORC must also be accountable for encouraging or allowing these activities to flourish in these settings. NACDS especially encourages Congress to prohibit the sale of infant formulas, baby foods, OTC medicines and medical devices, and other consumer healthcare products at such non-retail related outlets. Consumer safety can only be guaranteed by limiting the sale of such products through legitimate retailers.

Two key pieces of legislation were introduced earlier this year to help curb the incidence and impact of ORC. The Organized Retail Crime Act of 2009 (H.R. 1173), by Rep. Brad Ellsworth (D-IN), would amend the federal criminal code to make it illegal to engage in ORC activities and imposes obligations on on-line marketplaces and those who are considered high-volume sellers at such venues. In addition, the E-Fencing Enforcement Act of 2009 (H.R. 1166), by Chairman Scott, requires on-line entities to halt sales of stolen goods and imposes a duty to collect data law enforcement can use to prosecute those that sell these goods on their websites.

We urge all members of Congress, including members of this subcommittee to support and work for swift enactment of H.R. 1173 and H.R. 1166. NACDS is also working at the state level to have the states adjust their monetary value threshold to classify ORC as a felony under state law to appropriately target transient ORC gangs. Finally, adequate funding must also be provided at the federal and state levels to allow law enforcement agencies to effectively combat ORC.

CONCLUSION

NACDS stands with Chairman Scott, Ranking Member Gohmert and other Members of the Crime, Terrorism, and Homeland Security Subcommittee to help eliminate ORC. ORC's impact on consumers is too great to delay action. As Congress considers legislation to combat ORC, NACDS is prepared to provide further assistance from a retail perspective. Thank you for your consideration of our views.

HOUSE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY
HEARING ON COMBATING ORGANIZED RETAIL CRIME – THE ROLE OF FEDERAL LAW ENFORCEMENT
2141 RAYBURN HOUSE OFFICE BUILDING
STATEMENT OF SENATOR RICHARD J. DURBIN ON
THE COMBATING ORGANIZED RETAIL CRIME ACT OF 2009 (S.470)
November 5, 2009

Chairman Scott and Ranking Member Gohmert, thank you for holding this hearing and thank you for the opportunity to address the issue of organized retail crime and to discuss S.470, the Combating Organized Retail Crime Act of 2009, which I introduced in the Senate along with Senator Klobuchar earlier this year.

The Combating Organized Retail Crime Act takes important steps to confront the growing problem of organized criminal activity involving stolen and resold retail goods. Organized retail crime costs retailers billions of dollars per year and creates significant health and safety risks for consumers. Our legislation will toughen criminal laws and put in place effective regulatory and information-sharing measures to help retailers, secondary marketplaces, and law enforcement agencies work together to stop this crime.

Organized retail crime rings currently operate across the nation and internationally. Their criminal activity begins with the coordinated theft of large amounts of items from retail stores with the intent to resell those items. The foot soldiers in these organized retail crime rings are professional shoplifters, called "boosters," who steal from retail stores such items as over-the-counter drugs, baby formula, medical diagnostic tests, health and beauty aids, clothing, razor blades, and electronic devices. These boosters often use sophisticated means for evading retailer anti-theft safeguards, and occasionally dishonest retail employees are complicit in the theft. Each booster routinely steals thousands of dollars worth of items from multiple stores, and delivers the items to a "fence," a person who buys stolen products from boosters for a fee that is frequently paid in cash or drugs.

Today, organized retail crime rings often enlist numerous fences to deliver stolen retail goods to processing and storage warehouses operated by the rings. At these warehouse locations, teams of workers sort the stolen items, disable anti-theft tracking devices, and remove labels that identify the items with a particular retailer. In some instances, they alter items' expiration dates, replace labels with those of more expensive products, or dilute products and repackage the modified contents in seemingly-authentic packaging. Often, the conditions in which these stolen goods are transported, handled and stored are substandard, leading to the deterioration or contamination of the goods.

Organized retail crime rings typically resell their stolen merchandise in physical marketplaces, such as flea markets and swap-meets, or on Internet auction sites. Internet sites are particularly tempting avenues for these sales, since the Internet reaches a worldwide market and allows sellers to operate anonymously and maximize return.

Organized retail crime has a variety of harmful effects. Retailers and the FBI have estimated that this crime costs retailers approximately $30 billion per year and deprives states of hundreds of millions of dollars in lost sales tax revenues. The proceeds of organized retail crime can be used to finance other forms of criminal behavior, including gang activity, drug trafficking and international terrorism. Further, organized retail crime often involves the resale of consumable goods like baby formula or medical diagnostic tests like diabetic strips, which can cause significant harm to consumers when stored improperly or sold past their expiration date.

Organized retail crime has taken a large and growing toll on retailers' balance sheets. A December 2008 survey by the Retail Industry Leaders Association found that 80 percent of the retailers surveyed reported experiencing an increase in organized retail crime since the start of the current economic downturn. In a 2008 survey of loss prevention executives performed by the National Retail Federation, 85% of the 114 retailers surveyed indicated that their company had been a victim of organized retail crime in the past 12 months. Many law enforcement officials predict that organized retail crime will continue to increase during these troubled economic times.

After I introduced legislation on this subject last Congress, I listened to the views of stakeholders from law enforcement, the retail community, and the Internet marketplace community, and have made several revisions to my legislation in response to their suggestions. My current bill would do several things.

First, it would toughen the criminal code's treatment of organized retail crime. It would refine certain offenses, such as the crimes of interstate transport and sale of stolen goods, to capture conduct that is being committed by individuals engaged in organized retail crime. It would also require the U.S. Sentencing Commission to consider relevant sentencing guideline enhancements.

Second, the bill would establish a reporting system through which evidence of organized retail crime can be effectively shared between the victimized retailers; the marketplaces where items are being resold, very often without the knowledge of the marketplace operator; and the Justice Department. The bill would create a form that retailers could use to describe suspected illegal sales activity involving goods that were stolen from that retailer. The retailer would sign and submit this form to both the Justice Department and to the operator of a physical or online marketplace where the stolen goods are suspected of being offered for resale. Upon receiving the form, the marketplace operator would be required to conduct an account review of the suspected sellers and provide the results of that account review to the Justice Department. This reporting system would ensure that the Justice Department receives information from both retailers and marketplaces in order to piece together organized retail crime investigations and prosecutions.

Third, the bill would require that when a marketplace operator is presented with clear and convincing evidence that a seller on that marketplace is selling stolen goods, the operator must terminate that seller's activities unless the seller can produce exculpatory evidence. The bill would also require that when a marketplace operator is presented with documentary evidence that consumable goods or medical diagnostic tests offered for sale on that marketplace may have

been stolen, the operator must immediately suspend the ability of that seller to sell such goods because of the potentially imminent danger to public safety.

Additionally, the bill would require high-volume sellers on Internet marketplace sites to provide a physical address to the marketplace operator. This address would be shared with the Justice Department and with a retailer when the retailer attests and provides evidence that the high-volume seller is suspected of reselling goods stolen from that retailer. This address-sharing regime will permit appropriate inquiries to determine whether high-volume Internet sellers are legitimate operations, and is similar to address-sharing regimes that permit inquiries into possible copyright violations by online sellers.

In sum, the Combating Organized Retail Crime Act of 2009 is targeted legislation that aims to deter organized retail crime and facilitate the identification and prosecution of those who participate in it. The bill would heighten the penalties for organized retail crime, stop criminals who are selling stolen goods, and place valuable information about illegal activity into the hands of law enforcement. This legislation has broad support in the retail industry in my home state of Illinois and nationwide. It is supported by the Illinois Retail Merchants Association, the National Retail Federation, the Retail Industry Leaders Association, the Food Marketing Institute, the National Association of Chain Drug Stores, and the Coalition to Stop Organized Retail Crime, whose members include such retail chains as Walgreens, Home Depot, Target, Wal-Mart, Safeway, and Macy's.

Thank you again for holding this hearing and for the opportunity to submit this testimony. I look forward to working with you to enact legislation to crack down on the growing problem of organized retail crime.

November 5, 2009
For Immediate Release

Contact: Liz Jennings (703) 600-2063

House Judiciary Committee Hears from Federal Law Enforcement on Retail Crime

Washington, DC – Representatives of three federal law enforcement agencies told a House Judiciary Subcommittee today that more needs to be done to combat organized retail crime (ORC) in the U.S.

In testimony before the House Judiciary, Subcommittee on Crime, Terrorism and Homeland Security, officials from the FBI, U.S. Secret Service, U.S. Postal Inspection Service, and Immigration and Customs Enforcement testified to the challenges they face combating this growing crime.

"The Coalition Against Organized Retail Crime (CAORC) thanks Subcommittee Chairman Robert C. "Bobby" Scott (D-VA) for holding this hearing and for his commitment to providing federal law enforcement with the tools they need to address this growing criminal activity," said the coalition.

Coalition testimony provided to the committee for the record can be viewed **here.**

Organized Retail Crime involves sophisticated criminal networks made up of many individuals who steal large quantities of goods from retailers and in turn sell the goods for profit though pawn shops, flea markets and increasingly on the Internet. Experts estimate organize retail crime losses in the tens of billions of dollars annually.

Consumers are endangered when stolen goods are mishandled or altered before being sold to unsuspecting consumers. This is of particular concern when sensitive items such as baby formula, diabetic test strips and over the counter medicine is involved. Recent investigations have uncovered these sensitive health and beauty items stored at dangerous temperatures damaging the safety and reliability of the product. In most cases, consumers are unaware of the unlawful source of the products purchased from anonymous sellers.

Retailers work closely with law enforcement to identify and investigate local trends and to develop cases against these criminal networks. However, ORC criminal networks often operate across state borders, exploiting legal gaps arising from the existing patchwork of state and local laws. Consequently, law enforcement is often unable to fully investigate and prosecute ORC criminal networks. As a result, despite the close coordination between retailers and law enforcement, according to the University of Florida, 2008 National Retail Security Survey, instances of ORC activity and losses attributable to the crime continue to rise.

Federal legislation is necessary to bring the criminal code into the 21st century by closing the legal gaps that have benefited ORC criminals for too long.

Federal Legislation Currently Under Consideration:

The E-fencing Enforcement Act of 2009 (HR 1166), introduced by Chairman Robert C. "Bobby" Scott (D-VA), would impose reasonable duties on online marketplaces when there is good reason to believe that items listed for sale were acquired unlawfully.

The Organized Retail Crime Act of 2009 (HR 1173), introduced by Rep. Brad Ellsworth (D-IN), which modifies the federal criminal code to include ORC activities, and makes the facilitation of ORC a crime. The legislation also imposes practical reporting requirements on the operators of online marketplaces and sellers when goods are suspected of having been acquired through ORC.

The Combating Organized Retail Crime Act of 2009 (S 470), introduced by Sen. Dick Durbin (D-IL) would clarify existing law to give law enforcement the tools to fight ORC, require on-line and off-line market places to investigate suspicious sales, and place basic disclosure requirements on on-line marketplaces.

About the Coalition Against Organized Retail Crime

The CAORC, formed in 2001, is composed of 37 national manufacturing and retail organizations as well as individual companies that have come together to fight this growing crime. The Coalition's web site can be accessed at www.stopretailcrime.com. The CAORC has provided testimony to Congress on this issue in March of 2005 and October of 2007. The Coalition strongly supports enactment of pending federal legislation to combat ORC in the House of Representatives. Those bills include: The E-Fencing Enforcement Act of 2009, H.R. 1166, introduced by Chairman Scott, and the Organized Retail Crime Act of 2009, H.R. 1173, introduced by Reps. Brad Ellsworth and Jim Jordan.

###

Quotes from Members and Supporters of the Coalition Against Organized Retail Crime

"The FBI estimates that organized retail crime costs retailers billions of dollars annually, with proceeds from ORC often used to finance other criminal enterprises such as drug trafficking and gang activity, including those associated with terrorist factions. As a national retailer, Walgreens is impacted by ORC throughout the country. That's why we're advocating for ORC legislation in all states and support making ORC a federal criminal offense, including criminalizing those activities that clearly promote and expand ORC," **said Frank Muscato, Organized Retail Crime Investigations Supervisor, Walgreen, Co.**

"Organized retail crime impacts consumers as well as retailers, who must cover losses and invest in additional security measures. Consumers are placed at risk when package tampering occurs on consumer health care products, such as infant formula and over-the-counter medications. These stolen products are often repackaged and relabeled to falsely extend a product's expiration date or to hide the fact that the item has been stolen. NACDS will continue to work with lawmakers to pass strong legislation that will assist retailers and law enforcement to combat the serious problem of organized retail crime," said **NACDS President and CEO Stephen C. Anderson, IOM, CAE."**

"Organized retail crime (ORC) is a serious crime with real health and consumer safety implications that endangers our neighborhoods and citizens. Consumers are put in harm's way when stolen goods are mishandled or altered before being sold to unsuspecting buyers and communities are endangered when illicit proceeds from ORC are used to fund more dangerous and violent criminal activity. Federal legislation is essential to give law enforcement the necessary tools to combat these growing crimes and close the legal gaps exploited by criminals for too long," said **John Emling, Senior Vice President of Government Affairs for the Retail Industry Leaders Association.**

"Organized retail crime is a serious and ever-growing crime that poses serious risks to the safety and well being of our communities. The growth of the online marketplace has given criminals an unfettered avenue to fence their goods to innocent consumers, including here in Cook County. Federal criminal statutes are needed

to provide law enforcement with the tools necessary to deter and prosecute this complex criminal activity. I commend Senator Durbin's leadership in introducing the Combating Organized Retail Crime Act (S 470) as a means to combat organized conspiracies; including tightening regulations for online auction sites that could serve as conduits for stolen goods," **said Thomas J. Dart Cook County Sheriff.**

"The National Insurance Crime Bureau's (NICB) data and investigations show that organized retail crime is a growing problem from coast to coast. Online marketplaces often times become fraud victims as organized criminal rings defraud Web sites and offer financial assistance to buyers and sellers in transactions. Unfettered access to these online auctions negatively impacts businesses and innocent consumers as a source to fence stolen goods. NICB supports the Organized Retail Crime Act of 2009 as an effective means to combat this problem. By tightening the requirements to sell items online and beefing up federal criminal statutes, we can reduce the market for stolen goods, making retail theft less attractive to the criminal rings," **said the National Insurance Crime Bureau.**

"Organized retail crime is more sophisticated and more dangerous than petty shoplifting as organized rings of criminals move from store to store stealing large quantities of goods. They jeopardize the health and safety of consumers by fencing goods to buyers unaware of their origins and increasingly use internet auction sites, which conceal their identity. We support legislation that gives law enforcement the tools they need to fight these criminals and makes organized retail crime a federal felony for all the perpetrators involved," **said Leslie G. Sarasin, president and chief executive officer of the Food Marketing Institute.**

"The business of organized retail crime continues to proliferate throughout the U.S. Winning the battle against organized retail crime begins with the support of law enforcement, loss prevention teams and industry partners. Winning the war requires specific legislation that will make criminals think twice before participating in these illegal, often dangerous activities," **said Joe LaRocca, Senior Asset Protection Advisor, National Retail Federation.**

"RAM strongly supports federal legislation to combat organized retail crime. While we are backing legislation in our own state and feel that it is necessary to update our criminal code in MA, we firmly believe that federal legislation is needed to address this growing issue which has no state boundaries," **stated Jon Hurst, President of Retailers Association of Massachusetts (RAM).**

The Coalition Against Organized Retail Crime, hosted a briefing in advance of today's hearing. A recording of the press conference is available by dialing (800) 642-1687 and entering code 39367794.

○