ORC
ORGANIZED RETAIL CRIME

RESOURCE GUIDE

This guide is provided as a supplement to the interactive, online training course:
Recognizing ORC and Responding to Retail Theft

ORC is a Growing Concern

ORC is not just shoplifting. Organized Retail Crime is organized crime, and it is most often tied to other significant crimes like drug trafficking, money laundering, human trafficking and even terrorism. ORC affects everyone. This is not just a crime against a business, but a crime that results in higher costs for every consumer.

Like any criminal organization, it usually takes a concerted effort to investigate and identify all of the players involved and to identify the true reach and size of the criminal enterprise. Every investigation begins somewhere and so many times it is an alert patrol officer who identifies that first red flag—that first thread that leads to unraveling the extensive network of these organized groups.

Examples of Situations Where You Might Discover Elements of ORC

When responding to a retail theft, what may seem to be a simple $500 shoplifting case may in fact be part of a million, or even multi-million-dollar investigation. A walk through a warehouse or pawn shop business may uncover clues that indicate there is more going on behind the scenes. A traffic stop might include elements of ORC when you find stacks of merchandise in the back of a van or vehicle. Even responding to a domestic call might seem unusual when you realize the living room is full of merchandise and boxes are being prepared to ship goods overseas. While you may not be able to identify and react to make a case for any of these while in the moment, you can take notes and pictures and document what you see to share with detectives and other law enforcement agencies to investigate further and develop these ORC cases.

ORC - What to Look For

Whether responding to a shoplifting call or a traffic stop, you may identify quantities of merchandise that may indicate a connection to organized retail crime.

The following graphic highlights those merchandise categories which are most commonly stolen.

Grocery
Cigarettes, Energy Drinks
High-end Liquor, Infant Formula

Health & Beauty
Teeth Whitening Strips
Pregnancy Tests, Razors

Clothing
Denim Pants, Designer
Clothing / Handbags

Over-the-counter Medicine
Allergy Medicine, Pain Relevers
Weightloss Pills, Diabetic Testing

Home
High-end Vacuums, Electric Toys
Laundry Detergent, High-end Appliances

Electronics
GPS Devices, Laptops/Tablets
Cameras/ Recorders, Cellphones

DiY / Home Improvement
Power Tools, Cable / Wiring
Water Heaters

Questions You Should Ask / Points to Consider

The best way to develop leads for cases and to help identify when there might be more to the story that could lead to building a bigger and better case, is to ask questions. When responding to a call and you identify indicators of ORC, think about these questions to help uncover additional details that may support your investigation.

Let's start with some important questions you should ask yourself:

- **What am I really seeing here? Could this incident be related to organized retail crime?**
- **Is this a person who was acting alone—or were they working with others?**
  - **Was anyone acting as a lookout or distractor while another was stealing?**
- **Does this person or persons have a criminal history of theft, larceny, burglary, robbery, or substance abuse?**
- **Was this merchandise intended for personal use, or does this involve bulk merchandise likely to be sold for profit or exchanged for other value?**
- **Is this an individual stealing to support a personal drug habit? Have they been involved in multiple thefts that may indicate he or she could be part of an organized theft team?**
- **Did the suspect possess any type of merchandise shopping list?**
- **Did they admit they were stealing to sell the merchandise?**
- **Did the suspect take large quantities of the same merchandise?**
- **Did the suspect steal multiple items with small size and high value?**
- **Did the suspect take traditional high-theft/high-demand products such as razors, over-the-counter medications, health and beauty products, electronics, tools, clothing, baby formula, or other products commonly targeted by ORC teams?**
- **Were any burglary tools used, or any method of concealment like box stuffing, or Booster Bags?**
- **Does the merchandise fit the person or purpose?**
  - **Are the items taken consistent with the shoplifter's size or character?**
  - **Is the merchandise appropriate for the individual – and does one person really need 10 or 20 of the same items?**
- **Did the subject travel from another county or state of residence?**

- Does this merchandise belong here? For example, why would a pawn shop be buying or selling over-the-counter medication? Why is it in their stockroom?
    - Does the facility possess bulk quantities of the same products, or any signs that merchandise has tickets, labels, or tags indicating it's from a national retailer?

Next, let's look at some questions you may want to ask the suspect that may help identify if this activity is related to ORC.

- What were you going to do with the product?
- How did you get involved in boosting? Who trained you?
- Where or to whom do you sell it?
- When was the last time you sold stolen products?
- How much do you receive for the item(s)?
- How do you get paid?
- Why do you need the money?
- Are you given a shopping list? Who provides the list?
- Do you have a copy of this list? Is it on their phone?
- What do the buyers do with the products?
- Where else have you boosted product?
- What kind of car do you have? May I search it?
- How did you get to the store today?
- Specifically, why did you come to this store to steal today?
- Do you have a shopping list or list of items you intended to steal?
- Did someone tell you to steal this merchandise?
    - Who is that person? What is their location / phone number? How do you know them?
- Why were you stealing this specific product?
- What were you planning to do with the merchandise if you were not caught today?
- If the merchandise was going to be sold, how much would you have been paid for the items?
- What is the name of the person or place you were going to sell to today?
    - How often do you sell to this person/place?
    - Describe the place that you are referring to. What does it look like, how do I get there from here, what is the address?
    - How do you know this person?

- How do you contact the buyers?
- When was the last time you sold stolen merchandise to this person/place?
- Describe the person you sell to. What does he or she look like?
- Can anyone sell to this person, or do they have to be introduced?
- Do you know others selling to this person or place?

- Who else is involved with you? Other boosters.
- How did you learn to steal in the manner you tried today?
- Have you ever stolen from another retail store? If so, what types of product did you steal from them? Where do you sell that product?
- Do you have a drug, alcohol, or gambling problem?
- Would you be willing to cooperate with law enforcement and the retail victim to further this investigation?
- Do you sell any of this stolen merchandise online?
    - Do you have any sales history on any online marketplaces (Amazon, eBay, Facebook Marketplace)
    - What is your account name? Is this a personal or business account?
    - How long have you been selling online?
    - Does anyone else sell this merchandise with you? Or for you?

These are by no means all the questions you can ask, but hopefully offers some guidelines to get you started with your inquiry and provides ideas and avenues to explore when trying to determine the scope of your investigation and any connection to organized retail crime.

Other Methods of Retail Theft Often Related to ORC

You may discover other elements of theft and fraud that may also be prosecutable. To help identify this criminal activity, we are including some basic summary details below.

Refund Fraud Rings

Refund fraud is a common and widespread method of theft by deception. While refund fraud has been around for many years, incidents have continued to grow and gain momentum.

A simple approach that many ORC groups will employ is to simply gather items from the store and present them for return at the customer service desks. The refunder may use legitimate receipts that were discarded in the trash or otherwise recovered by the criminal group, or returned stolen merchandise accompanied by counterfeit receipts. Occasionally stolen items may be returned without accompanying receipts, with the refunder receiving merchandise credit, gift cards or similar tender that may then be sold for profit.

Another common method involves an individual legitimately purchasing a high-dollar item and leaving the store. The individual or an accomplice will then return to the store with the original receipt and attempt to steal another item identical to the one from the original purchase. Both items may then be returned to the store, one with a receipt for a cash refund, and the second for a gift card which can then be sold for cash by the perpetrator.

There are many variations to the types of refund fraud that can be conducted by organized retail crime groups, depending on the sophistication of the thief, the tools utilized, and the practices and policies of the stores victimized. The ability to convert merchandise to cash quickly makes this type of ORC incident very attractive to the professional thief, and one that will continue to be committed as long as such opportunities remain available.

Key Things To Look For:

- Multiple like items with only one originating purchase receipt
- Multiple receipts for the same item and or copies of the same original receipt
- Multiple return receipts, multiple gift cards for returned items and or multiple merchandise credit slips

Counterfeit Receipts

Counterfeit receipts have become an increasingly prevalent problem in retail and a common tool used by ORC groups. Advancements in computer technology and software have made it possible to create counterfeit/duplicate receipts using portable printers and scanners, laptop computers, and portable all-in-one technology, all of which have become more affordable and user-friendly in recent years. The quality of printers, scanners, and printing programs have evolved to the point that everything from receipts to prescriptions can be counterfeited and reproduced to a level where fraudulent copies are easily passed as legitimate.

Receipts can be scanned and edited with UPC and other relevant information (prices, descriptions, date stamps, store numbers, etc.) to create receipts to match stolen product. Receipt paper will be stolen from the stores, or similar paper that matches the store's original receipt paper color and touch can be purchased online or through other outlets to improve the appearance of authenticity of the document. The portable nature of this equipment allows the ORC network to create work stations in vehicles and other mobile sites that can be used to produce fraudulent documents almost anywhere in just minutes.

Key Things To Look For:

- Multiple receipts, copies of receipts
- Laptop, mobile device and or portable printers and printer accessories
- Multiple receipts for the same item and or copies of the same original receipt
- Multiple return receipts, multiple gift cards for returned items and or multiple merchandise credit slips

Gift Card Fraud

Gift Cards are offered by most retailers as a quick and convenient form of tender for the consumer. Gift cards can be purchased in specific denominations or can be loaded for a requested amount by the purchaser. Each card generally must be activated at a cash register before they are deemed active.

There are a variety of ways that gift card fraud can occur. For example:

- A card may be purchased with a stolen credit card and then used or sold to others
- A dishonest employee may keep a valued card that belonged to a customer
- A dishonest associate may keep and record the coded numbers from a card sold to a customer and use the number to make purchases
- A dishonest individual (employee or customer) may take cards, record valid card information, and then place the cards back in the store for display and purchase. The dishonest individual will then check the card numbers periodically to learn whether the card has been purchased and activated with a value assigned, in which case the balance on the cards is fraudulently used to make purchases

In an attempt to tighten security measures, many retailers that sell gift cards have responded by printing PIN numbers on the gift card that must be scratched off once the card is activated. Consumers are increasingly aware to ensure that the PIN code has not been revealed prior to purchasing a gift card. Retailers offering gift cards have also stopped allowing the consumer to check gift card balances online, and have stopped or restricted the use of live operators to check a gift card balance, making it more difficult for the dishonest individual to check several balances at one time.

Key Things To Look For:

- Multiple gift cards, receipts for gift cards and or multiple credit cards
- Lists of account numbers, expiration dates and or personal information on card holders, including name, address and any PIN number information
- Multiple receipts for gift card purchases
- Multiple receipts for items purchased with gift cards

Ticket Switching | UPC | Price Tag Altering

Ticket Switching refers to the removal and replacement of price tickets on merchandise to the benefit of the customer. The perpetrator will attempt to switch the UPC ticket from a lower-priced item, replacing the ticket on a higher valued item. The customer then presents the merchandise at the register in an attempt to purchase the more expensive item at a lower price.

This scenario may also be reversed during a return; when a customer may replace a price ticket with one indicating a higher value in an attempt to obtain more money when presenting the merchandise as part of a refund transaction.

Key Things To Look For:

- Higher value merchandise accompanied by receipts for lower amounts
- Loose price tickets, copies of price tickets, or lists of SKU information
- Ticket printing devices, ticket guns, or similar printing devices

Credit Card Fraud Rings

Credit Card Fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment method as a fraudulent source of funds. The purpose may be to obtain merchandise or as a means to obtain unauthorized funds from an account.

Credit card fraud is also a common form of identity theft. The fraud begins with either the theft of the physical card, or the compromise of information associated with the account, such as the card account number or other information that would routinely and necessarily be available to a retailer during a legitimate transaction. This type of incident can occur through different methods and the cardholder may not become aware until receiving a billing statement several weeks later. Incidents may include but are not limited to:

- **Stolen Cards** - This type of incident would involve larcenies from a person, vehicle, mailbox, home, or other means and using the card to purchase products.
- **Counterfeiting** - This involves fabricating cards and embossing lettering and fake or altered hologram identifiers. Often counterfeit cards will not be read when swiped through card readers, as the machines will not recognize the false magnetic stripe without the appropriate level of technology needed to code the stripes.

- **Altered (Re-encoded) Mag-Stripes –** The magnetic stripe on the card is re-encoded with a different account number, which is often difficult to identify. This re-encoding technology is relatively inexpensive and readily available for purchase. The technology is similar to that used for encoding hotel room keys, which simply reads the track, erases the information, and re-writes new information. These devices can be mounted to a laptop, and may be used by ORC groups in a vehicle as they travel from store to store.

- **Account Takeover** - A common method used in credit card fraud. The involved victim has a legitimate credit card account, but the card is "taken over" by a 3rd-party perpetrator. The perpetrator(s) will portray the legitimate card holder, and will add on "authorized users." In other instances, the perpetrator may be the actual account holder, adding and later denying that they added other "authorized users" to the account. In some cases, perpetrators may change the address and phone number on the account to prolong detection.

- **True Name Fraud -** This is classic identity theft. The victim never had a legitimate account. The perpetrator uses information associated with the victim to create a fraudulent account. Typically, the involved party doesn't discover that they're a victim until after they receive a bill.

Chip & PIN Technology

Chip and PIN is a technology that embeds a microchip into a credit or debit card. The word "chip" refers to a computer chip embedded in the smartcard; while the word PIN refers to a personal identification number that must be supplied by the customer. The technology is also known as EMV, which stands for Europay, MasterCard, and Visa, the developers of the technology's standards.

Banks and retailers are replacing traditional magnetic stripe equipment with smartcard technology, where credit and debit cards contain an embedded microchip and are authenticated automatically using the personal identification number (PIN). When a customer wishes to pay for goods using this system, the card is placed into the Point of Sale (POS) terminal or a modified swipe-card reader, which accesses the chip on the card. Once the card has been verified as authentic, the customer enters a 4-digit PIN, which is submitted to the chip on the smartcard; if the two match, the chip tells the terminal the PIN was correct. Otherwise, it informs it the PIN was incorrect. The chip generates a unique, one-time code that changes with each transaction. As a result, even if thieves manage to get data from a merchant it's like stealing an expired password—useless.

EMV cards and the use of chip technology thwart some of the most common ways thieves clone cards and steal data. It has significantly reduced fraud at point-of-sale terminals, and according to reports could reduce credit card fraud by 40% or more.

Skimmers

Card "Skimmers" are devices used to read and record a card owner's account information from the magnetic stripe found on the back of a credit or debit card. "Track Data" is the information encoded within the magnetic stripe on the back of the card which is read by an electronic reader within the terminal or point-of-sale (POS) system. Each credit and debit card has a unique pattern of magnetic particles embedded on the magnetic stripe which contains exclusive customer account information—not only the name, card number, and expiration date that appear on the card's face, but also an invisible, encrypted verification code that is transmitted electronically from merchant to card issuer to confirm a card's validity at the point of sale.

Skimming often involves dishonest employees working with ORC networks. After a customer's card is read through the legitimate card reader at the point of sale, the dishonest employee will then skim the card through a portable skimming device, copying the coded information found on the card without the customer's knowledge. The skimmer device records the pattern contained on the magnetic stripe, and a counterfeiter has all of the information they need to create a perfect clone of the card. A single skimmer can hold card data from hundreds of different credit/debit cards. Once this information has been stored on the skimmer, it can be downloaded onto a computer and emailed anywhere in the world.

Other skimming operations can involve equipment placed around or over legitimate card readers in different venues, designed to capture the information for fraudulent purposes. They may be placed over a legitimate card reader in a retail store, over the card reader at an ATM machine, or inside a gasoline pump device, for example.

Card skimming has become an increasing problem in recent years as technology has improved the function and design of the equipment. Skimmer devices that were once too bulky to carry around can now easily fit into a pocket or purse. They are affordable, easy to carry, easy to hide, and easy to buy. They can be used almost anywhere that credit/debit cards are put into point of sale systems.

Key Things To Look For:

- Multiple credit cards or other cards with magnetic strips
- Laptops or mobile devices with attached card-swipe or encoding devices
- Lists of account numbers, expiration dates and or personal information on card holders, including name, address and any PIN number information
- Multiple receipts for items purchased on multiple account numbers
- Handheld card swipe devices, devices that attach to a computer, a point of sale device or other devices or micro-cameras that are attached over ATM, gas pump or other such areas where a person would insert their credit card

Cargo Theft Rings

Cargo theft rings are highly organized criminal groups that work together to identify, steal, and sell merchandise that has been stolen from companies at some point along the supply chain.

Often highly sophisticated in their methods, these groups may target individual shipments or multiple endeavors involving trucks, distribution centers, trains, shipping lines, and/or 3rd-party logistic companies. Incidents can range from the theft of specific items to entire shipments.

Cargo theft rings may simply be opportunistic, looking for prospects when the cargo is at rest. Perpetrators may attempt to steal entire trucks, or simply break into a truck or a warehouse and steal large quantities of product. However, as groups grow more experienced and organized, methods can become much more complex and have greater yields. Specific products may be targeted, with intricate plans and multifaceted operations. Some operations may enlist the help of company employees or recruit individuals to infiltrate the organization, providing cargo and transportation information, creating opportunities, or implementing theft operations themselves.

Some common forms of cargo theft may involve but are not limited to:

- **Burglaries** – Burglaries may occur at distribution facilities, transportation truck yards, commercial parks, railroad yards, or even when a full trailer is dropped at a store. These crimes typically occur during the hours when the least traffic or supervision is present, or other times when the risk of detection is minimized such as under the cover of darkness and/or during the weekend. Such incidents may involve employee co-conspirators.
- **Driver Giveaways** - These incidents involve a driver that actually participates in a conspiracy to steal a loaded rig, or merchandise off of the loaded rig. Drivers generally agree to turn over their rig or loaded merchandise to a theft group for a substantial cash payment.
- **Grab and Runs** - This method is often used by theft groups targeting trucks loaded with high-value goods or high-tech equipment. Individuals will follow a targeted truck and once the rig stops, suspects force open the trailer doors and off-load as much property as they can before the rig proceeds.
- **Counterfeit Paperwork** – This method generally is more common when companies use independent drivers to transport product. False drivers present counterfeit paperwork to the security team and/or other responsible parties, ultimately making off with valuable loads.
- **Terminal Robberies** – Organized theft groups may simply enter a distribution center or other facility, hold employees hostage, and proceed to steal one or several loaded vehicles.
- **Hijackings** – These incidents generally occur when a truck driver comes to a stop, be it at a signal light, truck stop, or dinner break. Theft groups will actually surveil the targeted commercial rig after receiving inside information regarding the transported load. Once the driver stops the rig, perpetrators (often armed) will enter the cab, detain the driver, and transport the load to a pre-determined destination. Typically, the driver is set free some distance from the theft location. Note: Some hijackings are staged and involve the drivers.
- **Leakage Incidents** – A “leakage” operation involves seizing part of a load while making it appear that no theft has occurred. This may involve seal tampering, counterfeit seals, removing the doors while the seals are intact, or other methods designed to conceal load compromise. This allows theft rings to operate with greater gains and less risk, and can prove extremely lucrative over time.

Often stolen cargos of merchandise are transported to a pre-designated warehousing or storage facility for off-loading and storage of stolen commodities. Such facilities may include but are not limited to industrial storage facilities, public storage facilities, restaurants, pallet yards, single-family houses, apartments, and condemned buildings. Product is also frequently loaded into another trailer for transport to overcome GPS equipment and other security measures.

Cargo theft incidents are continuing to grow in frequency and sophistication with thieves stealing every type of product from electronics and pharmaceuticals to food products and toilet paper. Events can involve vast amounts of products, immense losses, and substantial threats to the safety of drivers and other employees.

Key Things To Look For:

- Individuals or vehicles loitering in or around truck yards or warehouse / distribution centers
- Individuals or vehicles following specific trucks or truck routes, especially near areas where trucks may be at rest in transit or overnight
- Trucks with broken seals or locks
- Copies of various or similar cargo information or bill of lading details.
- Truck trailers left abandoned

Re-packing Operations

"Repacking" is the process of changing the wrapper, container, or labeling of stolen goods to conceal the origin of the stolen product. A repacking operation typically operates as a wholesale distribution operation. Stolen goods are obtained from fences or directly from professional thieves. Repackers sort, clean, shrink-wrap, remove tags and tickets, and otherwise repack the product, also adding their own tags and labels to make the goods appear to have been legitimately purchased from manufacturers and other legitimate sources.

Repackers often have counterfeit manufacturer shipping cartons and have the ability to produce counterfeit UPC codes. Products are then typically sold to an illegitimate wholesaler, who will mix stolen merchandise with legitimately obtained merchandise for resale to retail businesses. Products may be sold directly to small businesses for resale as well.

Key Things To Look For:

- Quantities of merchandise being prepared for shipment with labels being removed or replaced.
- Quantities of merchandise that do not fit the business, for example, over-the-counter pharmaceuticals found in the back of a pawn shop.
- Quantities of merchandise with price tags or other identifying information from other businesses or multiple businesses (for example, similar merchandise such as beauty supplies with price or product information indicating they would be sold by Walgreens, CVS, and Target).

ORC Resources Dedicated to Supporting Your ORC Investigation

Obviously, your local supervisor and investigations teams are your first stop, but if you or your department need additional contacts or support, there are many available to you:

National Associations

There are a number of national associations that are actively involved in the fight against Organized Retail Crime. These organizations are well connected to retail leadership and retail investigation resources and can absolutely help connect you with contacts at a specific retailer and or other investigation resources in any area of the country. Leading these efforts are the following associations:

- **CLEAR – The Coalition of Law Enforcement and Retail**

  Website: www.clearusa.org

  Contact: 954-410-8760

- **RILA – The Retail Industry Leaders Association**

  Website: www.RILA.org

  Contact: 202-869-0200

- **LPF – The Loss Prevention Foundation**

  Website: www.losspreventionfoundation.org

  Contact: info@losspreventionfoundation.org

Organized Retail Crime Associations

There are currently more than 30 regional organizations dedicated to the battle against ORC. These Organized Retail Crime Associations, or ORCAs, can be found across the United States and are comprised of members of law enforcement at local, state, and federal levels, as well as retailers, prosecutors, and legislators, all working together to fight ORC. These groups are extremely well-connected in their various areas of operation and can be a tremendous resource to help support your investigation.

The number of organized retail crime associations (ORCAs) has grown steadily in recent years, with a primary emphasis on assisting law enforcement, retail investigators, and prosecutors with the identification, investigation, and prosecution of those involved in organized retail crime.

In response to the scope and severity of organized retail crime concerns across the country, there has been an increased effort on the part of retailers and law enforcement agencies to share information regarding organized retail crime at the local, state, and regional levels.

Organized retail crime associations have helped provide that vehicle, opening doors to improve legislation, enhance investigations, and build cooperative relationships in the battle against organized retail crime.

Alaska Organized Retail Crime Alliance (AKORCA)	**www.akorca.org**
Alert Mid-South Tennessee-Alabama-Mississippi Organized Retail Crime Alliance	**alertmidsouth.org**
Arizona Organized Retail Crime Association (AZORCA)	**www.arizonaorca.org**
Arkansas Organized Retail Crime Association (AORCA)	**www.aorca.org**
California Organized Retail Crimes Association (CAL-ORCA)	**www.cal-orca.org**
Carolinas Organized Retail Crime Alliance (CORCA)	**www.corca.org**
Central New York Organized Retail Crime Alliance (CNYORCA)	**www.romepd.com/department-programs**
Collier County Organized Retail Theft Association (Florida)	**www.ccorta.org**
Colorado Organized Retail Crime Alliance (COORCA)	**www.coorca.org**
Cook County (Illinois) Regional Organized Crime Task Force (CCROC)	**www.ccroc.org**
Florida Organized Retail Crime Exchange (T-Force)	**www.frf.org**
Florida Law Enforcement Property Recovery Unit (FLEPRU)	**www.flepru.org**
Georgia Retailers Organized Crime Alliance (GROC)	**www.georgiaroc.org**

Hawaii Organized Retail Crime Alliance (HIORCA)	**www.hiorca.org**
Indiana Regional Organized Crime Coalition (INDIANAROC)	**www.indianaroc.org**
Kentucky Organized Retail Crime Association (KYORCA)	**www.kyorca.org**
Loss Prevention Organization of the Caribbean	**www.linkedin.com/groups/6951593**
METRORCA – NY, NJ, PA Metro Area Organized Retail Crime Alliance	**www.metrorca.org**
Michigan Regional Organized Retail Crime Association (MIORCA)	**www.mi-orca.org**
Mid-Atlantic Organized Retail Crime Alliance (MAORCA)	**www.maorca.org**
Minnesota Organized Retail Crime Association (MNORCA)	**www.mnorca.com**
Montana Organized Retail Crime Alliance (MTORCA)	**www.mtorca.org**
National Anti-Organized Retail Crime Association (NAORCA)	**www.naorca.org**
Nevada Organized Retail Crime Alliance	**www.nvorca.org**
New England Organized Retail Crime Alliance (NEORCA)	**retailersma.org/neorca**
New Mexico Organized Retail Crime Association (NMORCA)	**nmchamber.org/nmorca**
Ohio Regional Organized Crime Coalition (OROCC)	**www.orocc.org**
Oklahoma Organized Retail Crime Association (OKORCA)	**www.okorca.com**
Organized Retail Crime Association of Idaho (ORCAID)	**www.orcaid.org**
Organized Retail Crime Association of Oregon (ORCAOR)	**www.orcaor.org**
San Diego Organized Retail Crime Alliance (SDORCA)	**www.sdorca.org**
Texas Organized Retail Crime Association (TEXASORCA)	**www.txorca.org**
Upstate New York Organized Retail Crime Association	**www.nyorca.org**
Utah Organized Retail Crime Association (UTORCA)	**www.utorca.org**
Washington Organized Retail Crime Association (WAORCA)	**www.waorca.org**
Wisconsin Organized Retail Crime Association	**www.wiorca.org**

For the most up-to-date list of the Organized Retail Crime Associations available, you can always visit "Organized Retail Crime Associations: Complete List" at **losspreventionmedia.com/orcas-list**. This list is updated on a regular and consistent basis with the most recent ORCA information.

Federal Agencies

Homeland Security Investigations (HSI)

HSI has a national lead development center located in Vermont that is available 24/7 to support any suspected ORC investigation.

For additional DHS inquiries and to reach the HSI National Leads Development Center email **CombatOTGs@hsi.dhs.gov** or email **OTGcasesupportnldc@hsi.dhs.gov.**

Federal Bureau of Investigation (FBI)

The FBI has resources available to help support you with ORC investigations and can be reached at:

Federal Bureau of Investigation (**FBI**)
https://www.fbi.gov/

US Secret Service

The Secret Service has particular interest in those investigations relating to credit card theft and fraud. They can be reached at:

United States Secret Service
https://www.secretservice.gov/

Other Federal Agencies can be contacted via the following websites:

United States Immigration & Customs Enforcement (**ICE**)
https://www.ice.gov/about

United States Drug Enforcement Administration (**DEA**)
https://www.dea.gov/index.shtml

United States Postal Inspection Service
https://postalinspectors.uspis.gov/

Thank you for participating in the Recognizing ORC and Responding to Retail Theft training course. We appreciate your initiative to learn more about organized retail crime and supporting the effort to identify and dismantle these criminal networks. For more information about the training courses available or for any other ORC related questions, please feel free to email LPM Media Group at: **CustomerSupport@LPMmg.com.**

If we do not have the answers, we will help you find them!

customersupport@lpmmg.com
www.lpmmediagroup.com

This ORC Resource Guide is a supplement to the online interactive training course: Recognizing ORC and Responding to Retail Theft, available at www.LPpro.com