ACAMS | U.S. Immigration and Customs Enforcement

Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

A Comprehensive Educational Guide for Law Enforcement and Financial Crime Investigators

Produced By: ACAMS and Homeland Security Investigations

Contents

Executive Summary 5

Part One: Defining, Analyzing, and Understanding Organized Retail Crime (ORC) 8

Section One: Understanding Organized Retail Crime and its Impact 8

Defining ORC 8
The Impact of ORC 10
Why is ORC Increasing? 12

Section Two: Organized Theft Group Business Hierarchy and Characteristics 13

OTG Organizational Structure 13
OTG Organizational Roles 15

Section Three: The Organized Retail Crime Cycle 17

ORC Steps and Potential Red Flags 18
Types of Retailer Targeted for ORC, by Ranking 19

Section Four: Understanding the Scope of ORC 20

Section Five: Expanding Beyond Retail Store Theft 21

Section Six: Organized Retail Crime Investigations 22

Section Seven: The Intersection of ORC and Financial Institutions 23

Part Two: Detecting and Investigating Organized Retail Crime 24

Section Eight: Law Enforcement Case Studies and Red Flag Takeaways 24

Homeland Security Investigations' (HSI's) Stored Value Initiative 24
Operation King of Thieves 25
Operation At the Card Wash 29

Section Nine: Additional Red Flag Indicators and Emerging Typologies 32

Red Flag Indicators Related to Transactions 33
Red Flag Indicators Related to a Customer or a Customer's Business 35
Red Flag Indicators on Customers' Bank Statements 35
Red Flag Indicators Related to Domestic and International Geographical Risks 36
Red Flag Indicators Tied to Open-Source Intelligence (OSINT) Research, Including Online Marketplaces 37
Common Indicators on the Surface Web Relating to Stolen Goods 38

Section Ten: Emerging Typologies 39

Front and Shell Companies 39

Exploiting E-Commerce 40

Trade-Based Money Laundering (TBML) Schemes Relating to Organized Retail Crime (ORC) 41

Part Three: Effective Reporting of ORC Activity and Other AFC Program Considerations for Financial Institutions 44

Section Eleven: Suspicious Activity Reporting Considerations 44

SAR Form Considerations 44

Targeted Suspicious Activity Terms (TSATs) 45

SAR Narrative and SAR Supporting Documentation Considerations 46

Section Twelve: Other AML Program Considerations and Enhancements 47

USA Patriot Act: Information Sharing 47

Training 47

Due Diligence for Businesses Typically Used as Front Companies for ORC 48

Transaction Monitoring and Red Flag Identification 50

Conclusion 51

Executive Summary

Organized retail crime (ORC) remains at the forefront of most major news channels across the United States. High profile "smash-n-grab" robberies, and nationwide cases involving major retailers in Chicago, Los Angeles, and San Francisco, garner the headlines. Recent hearings by the United States Congress, that discuss and debate proposed legislation, target the ability of criminal organizations to resell the stolen goods online with relative anonymity.[1] ORC is a low-risk, high-reward business line for transnational criminal organizations' portfolios that presents a significant financial and public safety risk. While retailers and law enforcement partner to investigate ORC cases and provide education on the misconceptions and misunderstandings, it is clear there is a missing link in these partnerships, and that link is financial institutions.

Criminal organizations need to launder the nearly 70 billion US dollars of illicit proceeds gained from ORC activities annually. These organizations are looking to launder their billions through the formal financial sector, unregulated payment processors, and online marketplaces.

To combat ORC and take down organized theft groups (OTGs) more effectively, first, financial institutions must be brought into the awareness and education triangle. Second, public-private partnerships and information sharing channels between retailers, law enforcement, and financial institutions need to be created. Third, as law enforcement and retailers prioritize investigations involving ORC, financial institutions should look to reasonably enhance their anti-money laundering (AML) and counter-terrorist financing (CTF) programs to detect and report illicit proceeds stemming from these crimes.

Financial institutions should ensure proper controls are in place to detect and report illicit activities tied to or involving ORC.

While not specifically addressed in the National AML/CFT Priorities issued by the Financial Crimes Enforcement Network (FinCEN) on June 20, 2021, it should be addressed that ORC has been tied to many of the priorities issued and other heinous crimes, as reflected in this guide.

1. The Brand Protection Professional, Professional Pointer: What Is ORC And Is It Related To IPRC?, https://bpp.msu.edu/magazine/professional-pointer-march2022/

Link between the US National Priorities and ORC

This guide defines ORC and its evolving threat landscape, introduces the illicit financial flows tied to ORC and larger organized theft groups (OTGs), and provides case studies, red flags, and typologies. It also includes guidance and reasonable steps to enhance your anti-financial crime (AFC) program, including your investigation effectiveness, suspicious activity reporting (SAR), and how to identify which information is highly useful to law enforcement.

ORC and OTG: key points

- ORC has vast economic costs to the global economy and exploits the formal financial system. OTGs are often linked to other heinous crimes like human trafficking, terrorism financing, and transnational organized crime including drug and weapons trafficking.

- Illicit proceeds stemming from ORC are laundered through the formal financial sector by both basic money laundering techniques – like structuring bulk cash and interstate funnel accounts, leveraging straw buyers, and account takeovers – and more multifaceted schemes, such as trade-based money laundering (TBML) and complex third-party money laundering (3PML) typologies involving straw buyers, stolen gift cards, front and shell companies, and transnational OTGs.

- Increasing awareness across the financial sector is imperative in strengthening investigations relating to ORC and transnational OTGs.

- Financial institutions, through effective detecting and reporting of suspicious activity, and aligning their reasonably designed AFC program to ORC risks, can play a critical role in providing highly useful information to law enforcement.

- Public-private partnership and information sharing involving retailers, financial institutions, law enforcement, and other interested industries will serve as the most effective mechanism to combat ORC and dismantle OTGs both domestically and internationally.

PART ONE: DEFINING, ANALYZING, AND UNDERSTANDING ORGANIZED RETAIL CRIME (ORC)

Section One: Understanding Organized Retail Crime and Its Impact

> **Organized retail crime is leading to more brazen and more violent attacks in retail stores throughout the country. Many of the criminal rings orchestrating these thefts are also involved in other serious criminal activity such as human trafficking, narcotics trafficking, weapon trafficking, and more. Tackling this growing threat is important to the safety of store employees, customers, and communities across the country.**

Steve Francis,
Acting Executive Associate Director, Homeland Security Investigations

Defining ORC

According to the Washington Organized Retail Crime Association (WAORCA), ORC is defined as "the theft/fraud activity conducted with the intent to convert illegally obtained merchandise, cargo, cash, or cash equivalent into financial gain when the following elements are present: occurs over multiple occurrences OR in multiple jurisdictions, conducted by two or more persons or an individual acting in dual roles (booster and fencer)". ORC syndicates plan attacks on highly sought-after goods and then look to sell them either through back-door and online marketplaces, or in many cases through apparently, legitimate business fronts, operating in plain sight. The thefts are detrimental to both businesses and the overall economy as they pose both societal and health risks to the community.

ORC misconception – it is not "just shoplifting"

Public perception of this billion-dollar criminal activity is to write it off as a bunch of shoplifters and view it as a problem for retailers to solve themselves.[2] However, a common misconception is that this problem is "just shoplifting". There is a difference between those individuals who have a need for merchandise they cannot afford, like a mother who cannot afford baby formula, or even a drug addict stealing to feed his or her habit. This problem even surpasses the "smash-and-grab" thefts that get sensationalized in the news, as these are often local gangs or even groups of opportunists taking advantage for a quick gain. Organized retail crime is organized crime that involve professional organized theft groups. These are transnational criminal networks of individuals working together to steal for profit that finances their on-going operation and other criminal activity.

While there are several surveys attempting to gauge the total impact of ORC, most estimate that the impact is around US$69 billion annually.

Another common misconception is that retailers are insured against retail crime. Most retailers are self-insured, and whether self-insured or insured through a broker, the base value of an individual theft that is required in order to file a claim far exceeds the amount of each theft on its own. This leaves retailers to absorb this loss as operating costs and/or to pass on the impact in increased prices, lower wages, and fewer staff.

Furthermore, as ORC is viewed as a property crime, it unfortunately tends to be towards the bottom of priorities when cases are investigated and prosecuted.

ORC syndicates

Organized retail crime can further be defined as the theft of merchandise with the intent to convert the illegally obtained goods to profit.

For a theft group to be considered organized, the criminal activity must occur multiple times or in multiple jurisdictions by two or more people or an individual acting as the thief and the seller.[3]

Organized retail crime differs from burglary and larceny (such as shoplifting) in that it is not the result of a single individual breaking the law, but rather part of an organized scheme to defraud retailers or to steal products for resale elsewhere. This is why ORC syndicates focus on high value branded items – like leather goods, over-the-counter medications, health and beauty products, designer clothing and power tools – which are in demand from consumers, most of whom are unaware that they are purchasing stolen goods.

2. The Brand Protection Professional, Op. Cit.
3. Washington Organized Retail Crime Organization, https://www.waorca.org/

In addition to defrauding retailers, threatening employees, reducing choice, and increasing costs to consumers, many of these organized retail crime syndicates use their ill-gotten gains to fund other criminal activities, such as labor, arms, and drug trafficking.

The Impact of ORC

Financial impact

ORC has been increasing globally; however, for this guide we will be focusing on the increasing threat in the United States. It is estimated that as much as US$68.9 billion worth of products were stolen from retailers in 2019. This represents about 1.5 percent of total retail sales.[4] Further estimates reveal retail theft costs federal and state governments nearly US$15 billion in personal and business tax revenues, not including the lost sales taxes.[5] In speaking with Ben Dugan, President of C.L.E.A.R, the Coalition of Law Enforcement and Retail, it is estimated that the average American family will pay more than US$500 annually in additional costs attributed to the impact of ORC.

ORC's victims

It should be noted that ORC is not a victimless crime.

In a survey prepared for the Retail Industry Leaders Association (RILA) and the Buy Safe America Coalition, nearly 76% of respondents said that a criminal has threatened the use of a weapon against an associate, and 40% of Asset Protection Managers (APMs) said that an organized retail criminal has used a weapon to harm an associate.[6]

Additionally, ORC can negatively impact consumer health and safety, especially when an unsuspecting consumer faces risks from legitimate products, such as stolen infant formula, pharmaceutics, and other consumable products which may have been mishandled or manipulated (e.g. expiration dates) by the OTG who stole them for resale to consumers.

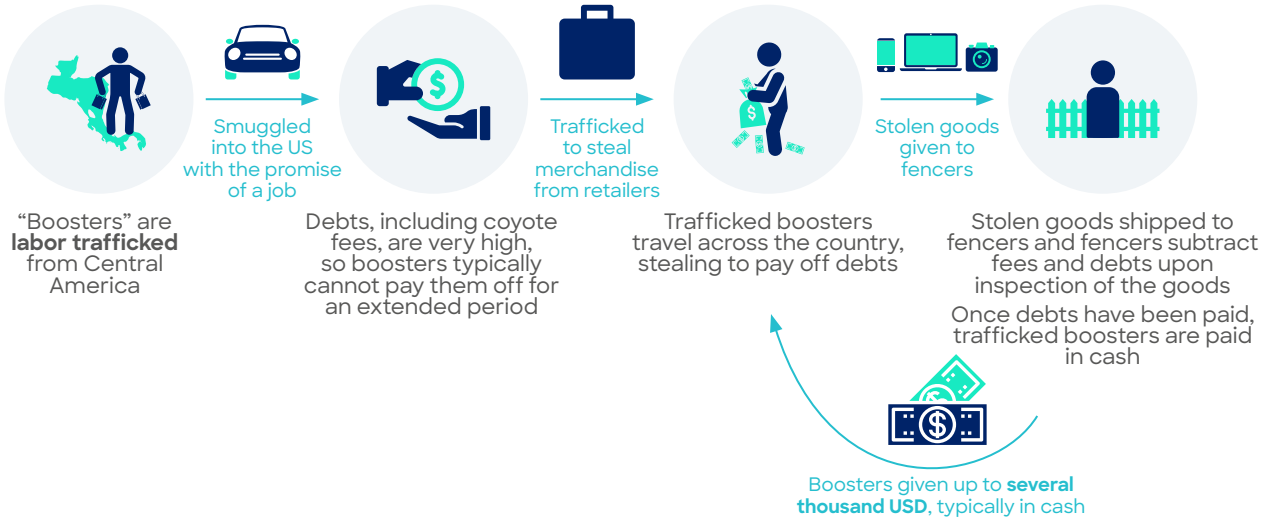
4. Retail Industry Leader's Association and Buy Safe America, The Impact of Organized Crime and Theft in the United States, https://www.buysafeamerica.org/impact-of-organized-retail-crime-and-product-theft
5. Ibid
6. Ibid

Example: public health threat

Stolen infant formula requires certain storage conditions. It poses a significant health risk to the child if infant formula is re-introduced into the retail market and has not been stored properly or it has been tampered with, such as manipulating the federally mandated expiration dates. The infant formula is repackaged and resold to unknowing wholesalers and retailers, who may sell the product to government food programs, retailers, and discount stores.

In addition to the violent acts made to retail employees, and the unsuspecting consumers of tampered and mishandled products, recent cases revealed victims from Central and South America are labor trafficked into the US to be the boosters in large OTGs. The trafficked individuals will boost until their "coyote fees" and other debts have been paid. Once the debts have been paid, the labor trafficked boosters from Central America will continue to boost across the country. The fencers will pay these individuals in cash. Boosters can and do have bank accounts. They can be under their name, a fake or stolen identity, or they could use the bank account of a trusted friend or family member.

Example: Central America labor trafficking threat



The cost to retailers

Retailers must now hire extra security for their storefronts and during transportation, and add additional expenses and labor costs for locking up products typically stolen, while also making up for lost profit from the thefts. This then drives higher prices for consumers and lower sales for retailers. Organized retail crime now costs retailers an average of US$700,000 per US$1 billion in sales, and three-fourths of retailers saw an increase in ORC in 2020.[7]

7. National Retail Federation, December 15, 2020, 2020 Organized Retail Crime Survey, https://nrf.com/research/2020-organized-retail-crime-survey

Why is ORC Increasing?

> **The sale of stolen and counterfeit goods on third party marketplaces is a multifaceted problem in need of a multifaceted solution. There is an undeniable connection between the growth of ORC and the ease with which criminals can sell stolen goods through unregulated online marketplaces.**
>
> **RILA Blog**

> **Organized retail crime is more than petty shoplifting, and the economic impact has become alarming. Professional thieves and organized criminal rings are building a business model by stealing and reselling products, increasingly online through marketplace platforms like Amazon or Facebook.**
>
> **Michael Hanson,**
>
> Senior Executive Vice President of Public Affairs for the Retail Industry Leaders Association

Online marketplaces have made it even easier for criminals to sell stolen goods anonymously, from any location. The chart below shows common goods that are typically targeted for theft and then sold via online marketplaces.

Products generally subject to shoplifting and those sought after through online marketplaces

Category	Marketplaces	Visits/Month (Million)	Sales (US$)	Theft (US$)	Percentage of Sales Stolen	Rank
General Merchandise	93	13,500	912,390,087,484	32,600,003,846	3.57%	1
Fashion	31	644	452,244,692,405	16,348,002,633	3.61%	2
Arts, Crafts, Gifts	3	402.5	N/A	N/A		
Homewares	7	281.2	235,302,033,513	8,313,002,402	3.53%	3
Electronics	6	80.8	206,584,642,838	7,801,817,813	3.78%	4
Music	2	80.3	N/A	N/A		
Books	5	42.8	29,292,502,626	1,003,693,094	3.43%	6
Sports	3	22.9	26,464,433,086	932,564,028	3.52%	7
Musical Instruments	1	16.8	N/A	N/A		
Collectibles & Antiques	2	6.4	N/A	N/A		
Toys & Baby	2	6	53,252,180,712	1,892,391,555	3.55%	5

Source: The Impact of Organized Crime and Theft in the United States

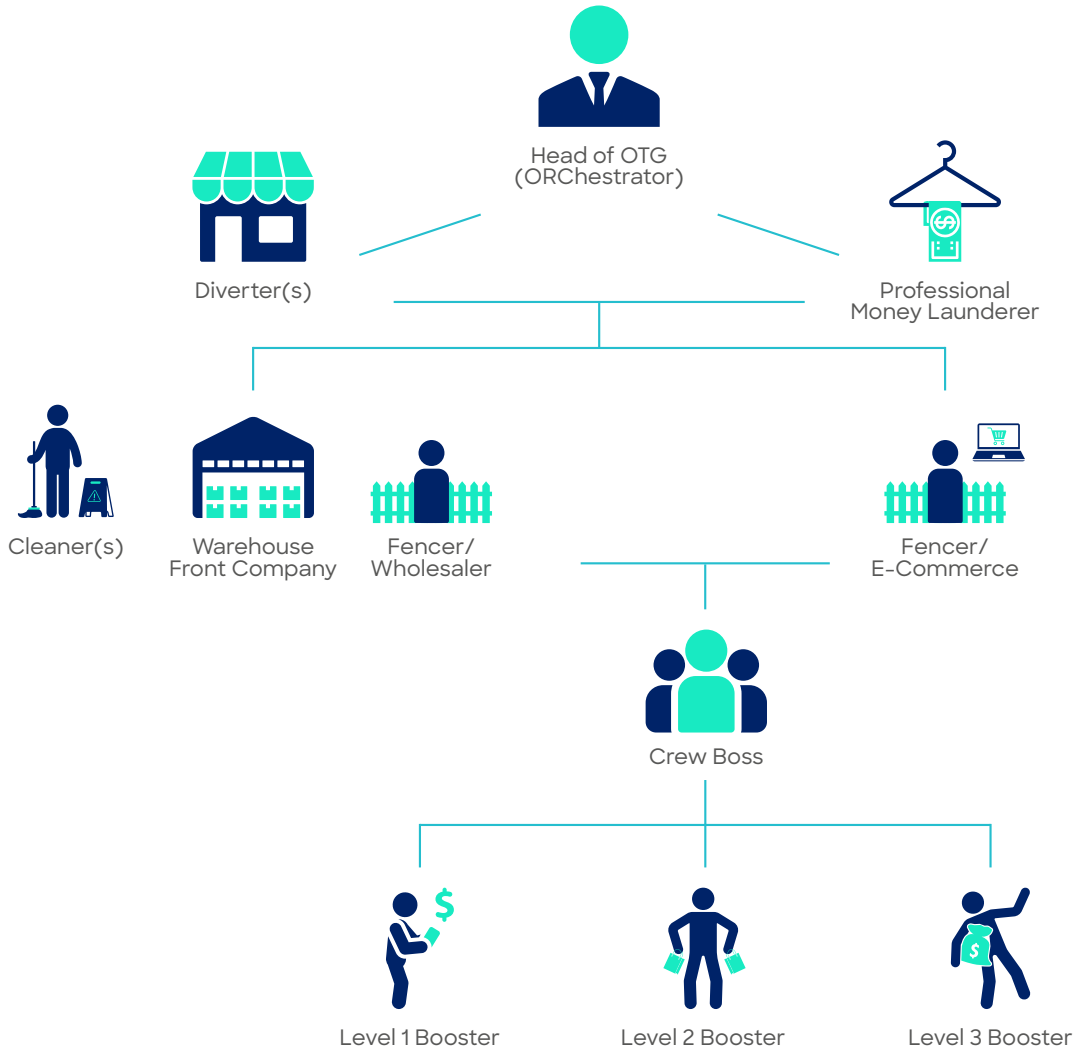
In addition to the increased ease of selling, the United States has begun raising felony thresholds for theft, essentially decriminalizing the act as jails are becoming overpopulated.[8] Therefore, organized theft may be an attractive criminal activity for organized crime groups for funding with little risk. Further, ORC is becoming increasingly globalized due to the widespread use of digital currencies, which make investigations difficult due to jurisdictional differences for law enforcement and retailers.[9]

8. Axis, April 26, 2021, The growing issue of organized retail crime, https://www.axis.com/blog/secure-insights/organized-retail-crime/
9. Ibid

Section Two: Organized Theft Group Business Hierarchy and Characteristics

Understanding the hierarchy and complexities of the OTG organizational chart assists financial crime investigators in analyzing transactions and flagging suspicious activity. Comprehending financial touchpoints and the money movement between the hierarchy will be key for financial crime investigations.

OTG Organizational Structure



OTGs can vary in size, complexity, roles, and hierarchy. The previous figure is a basic model. Supplemental considerations are reflected below.

In less complex organizations, the fencer may be the top individual in the OTG network.

More complex networks involve a head of the OTG theft group, known as the ORChestrator.

The fencers, diverters, and ORChestrator may all appear to be running legitimate businesses and funneling illicit money through front-companies. This will be discussed more below.

There are three levels of boosters:

Level one: local thefts

Level two: thefts within the same state or close neighboring states

Level three: national thefts, travels often and always sells to wholesalers

Large complex OTG networks may have multiple fencer wholesalers working under a diverter. The wholesale fencers sell to the diverters in bulk and may co-mingle goods with legitimate retailers for sale.

OTG Organizational Roles

Booster

Boosters are often undocumented immigrants, labor trafficked into the United States and working off a debt, or individuals suffering from some form of addiction. The boosters are the thieves on the ground that steal (boost) the products. They typically have a list of merchandise to steal from their crew boss and may hit numerous stores in one day. The boosters will likely be paid in cash or through anonymous/encrypted peer-to-peer payment apps. Boosters often work in pairs, with individuals tasked with other roles such as a lookout (keeping an eye out for salespeople), or distractor (distracting salespeople while the boosters take merchandise). Boosters often use modified clothing or modified shopping bags lined with aluminum foil, to conceal merchandise and defeat electronic article surveillance, or security tag, technology. They may also be so brazen as to simply fill up a shopping cart and push it out the door without making payment.

Crew boss

The crew boss leads a group of boosters on the ground. Crew bosses communicate with the fencers on logistics and pricing. The crew boss is given a list of items to steal from the fencer, which they then communicate to the boosters.

Fencer

Fencers are the next tier in the hierarchy and are typically the middleman between the thieves on the ground (crew boss) and other individuals involved in the organization such as the diverter, cleaner, professional money launderer, and ORChestrator. Fencers will typically own a wholesale front company or a warehouse that employs cleaners, and may sell the merchandise either through a store front, at a flea market, or through an online marketplace. In more complex organizations, they may provide the first round of cleaning, package merchandise, and ship it in bulk to a wholesale retailer. The wholesale retailer will then sell the items to diverters.

Cleaner

Cleaners typically work for a fencer or a diverter, and they are responsible for cleaning the product. The cleaners ensure the stolen goods have no indications of theft by removing retail anti-theft stickers with lighter fluid and heat guns. This often occurs at repackaging facilities, which are illicit operations often in small warehouses or businesses. Repackaging facilities convert the stolen goods into looking like their own product by counterfeiting lot numbers, packaging, and shipping labels. Often cleaners may issue new labels to increase the selling price and confirm the stolen merchandise cannot be traced. The cleaner will ship the product to the diverter. Typically, small local shipping locations are leveraged for selling stolen products.

Diverter

Diverters are the higher-level illicit wholesalers, salespeople, or coordinators for secondary sales. You will typically find diverters in more complex OTGs. Diverters often set up shell companies with opaque names to place and layer the illicit proceeds of the stolen goods. Diverters typically own warehouses where the boosters or fencers ship the stolen merchandise. They often have prominent interaction with the formal banking industry through e-commerce, shell companies, and transaction laundering, as they will own the shell company bank accounts and initiate wire transfers. Whether at the diverter level or the ORChestrator level, these may appear to be legitimate businesses, operating openly, and in many cases, these businesses act as suppliers for small to mid-size (and sometimes even large, national) retail chains, selling merchandise to these companies that in turn is used to stock their shelves for sale to consumers.

Professional money launderer

In some complex organizations, professional money launderers are employed to disguise any suspicious financial activity and co-mingle illicit funds. Professional money launderers may set up multiple shell companies to further layer illicit funds from ORC proceeds. The shell companies are only used to process the financial aspects of ORC. They communicate with diverters and ORChestrators.

ORChestrator

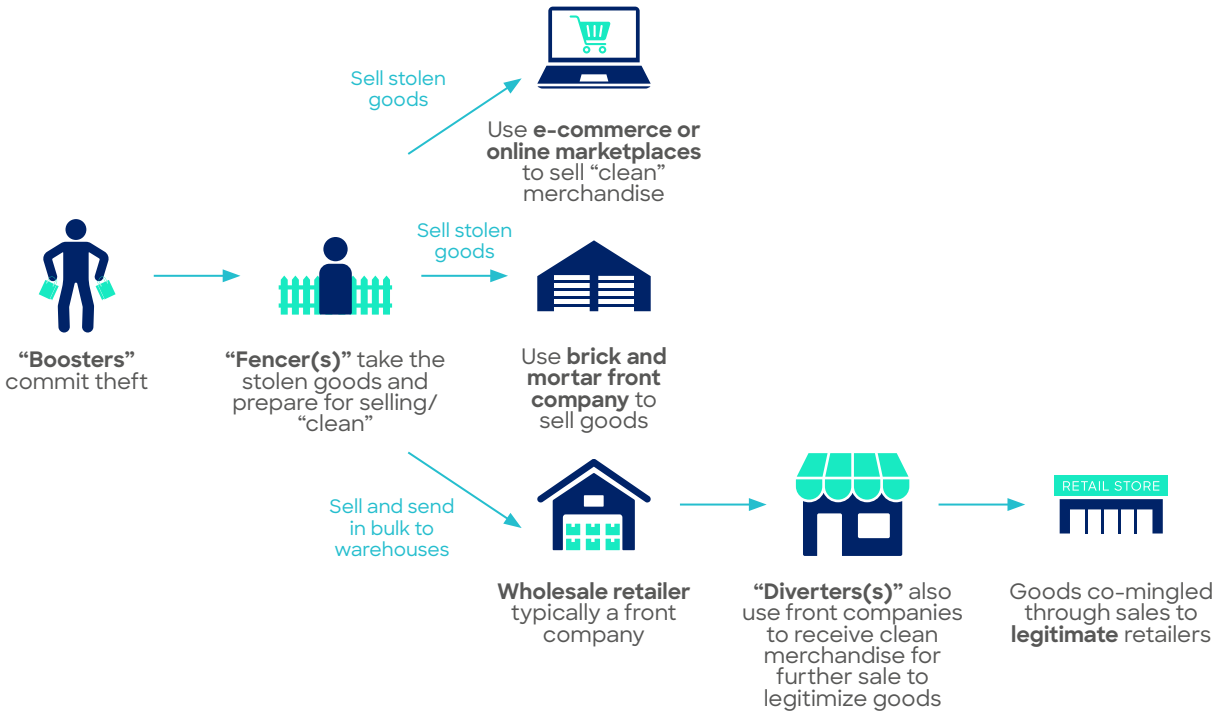
While it is possible that a fencer or a diverter could be considered the leader of a less complex theft group, the leader of the OTG is usually the ORChestrator. The ORChestrator may supervise multiple organized OTGs. The ORChestrator may further own brick and mortar stores that sell stolen merchandise, like over-the-counter medication, at discounted prices. In recent cases, ORChestrators have been noted to be foreign nationals from the Middle East, shipping their goods transnationally through free trade zones like Dubai. They have also been linked to labor trafficking boosters from Central and South America. Complex syndicates like these may be involved in large counterfeit schemes or other criminal activity, like drug or weapons trafficking, and use the illicit proceeds from ORC to fund their other criminal activities, or in some cases, terrorism.

Section Three: The Organized Retail Crime Cycle

By increasing their awareness of the organized retail crime cycle, key stakeholders in investigations can more effectively analyze financial transactions tied to ORC. Following the money is an effective tactic for prosecution and further investigations tied to complex organized criminal groups.

Furthermore, public-private partnership between financial institutions, law enforcement, and retailers, that includes information sharing, is vital to combating organized crime.

The organized retail crime cycle



ORC Steps and Potential Red Flags

Step	Description
Boosting the Stolen Goods	Typically, boosters are given a list from the crew boss of the goods to steal and their quantities. They typically target stores with a small number of employees for a quick get-away. Boosters use aluminum-lined bags to bypass store alarm systems during the theft.
Handling the Stolen Goods	Boosters or a crew boss will send the stolen goods via FedEx, UPS, and similar shipping companies to alias names previously provided by the fencer. The packages containing the stolen merchandise are sent to local mail centers and/or storage units. The mailboxes and storage units utilized will likely be rented under an alias name. Fencers typically buy the goods from the boosters and pay them in cash, though they may wire money directly to accounts in some instances or leverage peer-to-peer networks like Zelle and Venmo. The fencers lead a wholesale organization that may employ cleaners. Cleaning consists of removing any tags or sensors that would suggest the goods are stolen. Potential red flags include purchasing large amounts of lighter fluid or heat guns, which can be used to remove anti-theft stickers.
Preparing the Stolen Merchandise for Sale	After being cleaned of retailer anti-theft stickers and organized by like-type, the stolen goods are stored in a warehouse owned by the fencer or ORChestrator. In larger schemes stolen goods are sent to a diverter via FedEx, UPS, or similar shipping companies, or via trucking companies for larger, palletized shipments. Typically, the goods will not be shipped in the name of the diverter and the shipping label may indicate a shell company. The storage unit will likely be owned under a different name or under a shell company also. In addition to shipping companies and mailrooms, small businesses like pawn shops, thrift stores, or neighborhood convenience stores may employ transportation companies (common carriers) to ship pallets or truckloads of product every week.

Step	Description
Sales Through E-Commerce, Brick and Mortar Stores, and Bulk to Diverters	The most common mechanism of illicit sales is using e-commerce on online marketplaces. Many online marketplaces do not require customer or merchant identification or vetting, making them easy to exploit by criminals. The fencers will take stock pictures of the clean goods and then post those pictures on marketplaces like Amazon, Facebook, eBay, or Alibaba. This would be a similar process for large scale diverters. Fencers may also sell directly to brick and mortar stores or to a wholesale retailer. The wholesale retailer is part of the ORC scheme and sells to the diverter or ORChestrator. The goods will then be co-mingled with legitimate businesses. The goods can be listed by the front or shell company owned by the diverter, fencer, or the ORChestrator, then shipped directly to the customer or wholesale customer. Third party payment processors may be used to further disguise the identity of the criminals through the online marketplace directly to shell bank accounts. Diverters will often receive goods using a shell company name. Professional money launderers may also be employed to assist in disguising illicit funds.

Types of Retailer Targeted for ORC, by Ranking

Source: chart provided by Ben Dugan, President of C.L.E.A.R, the Coalition of Law Enforcement and Retail, a national public-private partnership of law enforcement professionals and retailers, working together to combat ORC.

Section Four: Understanding the Scope of ORC

National criminal organizations and high-level e-commerce ORC activities continue to be rated the highest severity in terms of financial impact. The levels of violence associated with these national-level organizations are generally low to moderate, purposely, to minimize the risk of being caught boosting the targeted products. The financial impact per case varies greatly, from US$500,000 to US$200 million.

The chart below summarizes different types of retail theft, including the levels of, and their impact on, numerous sectors.

Severity

ORC Activity	Targeted Product	Retail Victims	Level of Violence	Scope	Financial Impact (per case)	Collateral Crimes
National Criminal Organizations (Control Pricing and Disrupt Infrastructure)	OTC medicines Razor blades Health and beauty aids	Pharmacies, big box, and grocery stores	**Low** Purposely non-violent	Transnational, national interstate theft across large geographic areas (includes e-commerce)	US$10 - 200 Million	Interstate stolen goods, ML/wire fraud, international crimes/ counterfeiting, large scale financial fraud (gov), drug trafficking, human (labor) trafficking, terrorism financing
E-Commerce High Level Sell Nationally	Tools, electronics, health and beauty aids	Home improvement, electronic stores, grocers, pharmacies, big box	**Moderate**	Product stolen regionally; same state or neighboring states	US$500k- 2 Million	Interstate stolen goods, narcotics trafficking, ML/wire fraud
E-Commerce Local Level Sell Nationally	Tools, cosmetics, clothing and accessories	Home improvement, electronic stores, grocers, pharmacies, and big box	**Moderate**	Product stolen and listed locally	US$25K- 500K	Interstate stolen goods, narcotics trafficking, ML/wire fraud
Local ORC Flea Markets, Small Illicit Businesses	Laundry detergent, hand and body lotions; personal hygiene and some clothing	Dollar stores, big box, soft lines, pharmacies	**High probability for violence**	Product stolen and sold locally in public forum	US$10k- 200K	Interstate stolen goods, robbery/assault, narcotics trafficking, ML/wire fraud
Smash and Grabs	High dollar designer goods, jewelry, clothing	High end, soft lines, jewelry, small businesses	**Very violent**	Local gangs	US$5K- 100K	Robbery/assault, burglary, narcotics trafficking
Retail Theft Personal Use	All retailers	All retailers	**High potential for violence**	Local homeless or drug addicted	Low dollar	Narcotics, robbery/assault

Source: chart provided by Ben Dugan, President of C.L.E.A.R.

In this chart, while the basic act of shoplifting and even the smash-and-grabs represent common retail theft, the evolution to organized crime is noted past the level of local ORC, up to the national level.

Section Five: Expanding Beyond Retail Store Theft

Beyond retail store theft, OTGs target multiple industries in the United States and worldwide, as summarized below.

Cargo/rail theft

There are varied methods related to cargo theft. Due to the size of the load and type of merchandise being transported, these incidents can range from thousands of dollars to tens of millions of dollars with a single theft. Cargo thieves and ORC thieves often utilize the same fencers. It is estimated that there is US$15-30,000,000,000 in annual losses due to cargo theft alone.

Standard cargo theft

An OTG steals the tractor and/or trailer transporting high value/desirable cargo, or may target the cargo during vulnerable times, e.g. overnight storage, railroad stops, etc. The stolen cargo usually passes through a middleman/fencer before being introduced into the supply chain. The stolen cargo will be sold as-is or co-mingled with legitimate merchandise to be sold by a wholesale company or similar business. Financial transactions related to these thefts are usually business to business transactions by check, wire transfer, and/or cryptocurrency.

ID theft/cargo theft

OTGs assume the name and identifiers of an actual business through freight-related business websites. The OTGs target high value/desired cargo, forge documentation and pick-up the cargo. However, it is then sold for profit and/or traded for other contraband.

Double broker scams

Double broker scams usually target fuel advances paid by trucking companies or freight brokers. The OTGs obtain actual documentation from freight-related business websites and request a fuel advance. The OTG then brokers the load to another carrier with no intention of providing payment. Normally, since payment is within 30-60 days, multiple cargo loads will be transported before the brokered carrier realizes they've been victimized. The fuel advances can be sent via wire transfer to a person at a money service business or a business at a bank.

Section Six: Organized Retail Crime Investigations

Investigating these crimes takes a combined effort, typically initiating from activity discovered by a retailer, or a group of retailers, and further investigated in partnership between various local, state, and federal law enforcement agencies. Many retailers have asset protection teams dedicated to the investigation and surveillance of these ORC groups.

National organizations such as CLEAR, the Coalition of Law Enforcement and Retail, as well as regional Organized Retail Crime Associations (ORCAs) exist specifically to combat the efforts of ORCs and OTGs. There are currently more than 25 ORCAs across the United States. The membership of these organizations is comprised of retailer and law enforcement professionals working together to identify and dismantle these organized groups.

Key to furthering the success of these groups is the inclusion of the financial community as an additional partner.

The illicit funds derived from this criminal activity exploit the integrity of our financial system and intersect directly with many of the critical US National Priorities that both the public and private sectors are collectively committed to combat.

Identification of assets that are proceeds of, or are used to facilitate, ORC

Law enforcement utilizes asset forfeiture as a means to disrupt and dismantle criminal organizations by seizing and forfeiting the proceeds of their crimes, and property that has been used to facilitate those crimes, including ORC. Investigating agents facilitate the seizure and forfeiture of criminally derived assets, including currency, real property, and complex assets such as cryptocurrency, operating businesses, warehouses, planes, and vessels.

Asset forfeiture is an integral part of law enforcement's investigative efforts against OTGs as it helps to dismantle their criminal organizations and financial networks, hence impeding their enterprises.

It also helps to: punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities; promote and support future law enforcement efforts; and recover assets that may be used to compensate victims when authorized under federal law. In investigations against OTGs, asset forfeiture may be the only chance that retail companies have to recover some of their losses as victims of ORC.

Section Seven: The Intersection of ORC and Financial Institutions

Organized retail crime (ORC) is believed to cost retailers US$68,900,000,000.00 per year in losses[10] or more. It is undeniable that the corresponding profits from the re-sale of those products are flowing through the formal, and in some cases informal, banking sectors.

Therefore, financial institutions will play a key role in combatting ORC and dissolving OTG rings.

In addition to the illicit proceeds touching the global financial system, investigations have proven that in many cases, ORC is related to, and is funding, other criminal activity that financial institutions already monitor for. The proceeds from the low cost, high reward ORC crimes have been used to fund further criminal activity, such as:

- Drug and arms trafficking across the southern border
- Third-party money laundering for the benefit of Asian OTGs
- Possible terrorist financing through Middle Eastern OTGs and the ORChestrators
- Labor trafficking of Central and South Americans forced to act as boosters and steal goods for transnational criminal organizations
- Counterfeit goods and cross-border fraud schemes

Significant ORC cases, several of which will be described further in this guide, have been tied to other illicit criminal activity. Regardless of whether the activity is tied to a larger criminal portfolio, a financial institution has government reporting obligations, including ORC activity, as the funds derived from ORC activity are illegal.

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including sanctions evasion.[11]

10. US Immigration and Customs Enforcement, January 2021, Cornerstone: Collaborating with the Financial Industry to Prevent Crime, www.ice.gov/cornerstone
11. See 31 CFR § 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320 https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-C/section-1020.320

Section Eight: Law Enforcement Case Studies and Red Flag Takeaways

Homeland Security Investigations' (HSI's) Stored Value Initiative

HSI's National Bulk Cash Smuggling Center (BCSC), in conjunction with the HSI Financial Crimes Unit (FCU), established the Stored Value Initiative (SVI). This initiative utilizes the Electronic Recovery and Access to Data (ERAD) Solution, to combat transnational criminal organizations' (TCO) use of stored value and prepaid cards to launder illicit proceeds.

Increased banking restrictions and enforcement efforts regarding bulk cash smuggling have forced TCOs to seek alternate means of moving illicit proceeds. These means include converting bulk currency to prepaid and stored value cards (SVC). The use of SVCs by TCOs creates obstacles for law enforcement due to the ease of concealment, fluidity of funds, and the obstacles faced in determining their worth during cursory observations. TCOs are heavily involved in exploiting credit card processing centers and consumers' use of SVCs at traditional point of sale locations. They often target unwitting card users at retail stores, convenience stores, and ATM locations, defrauding consumers by surreptitiously obtaining their personally identifiable information. This information may be sold on the internet or dark web, or re-encoded onto other cards to perpetuate the fraud schemes.

Scheme one: an OTG steals credit/debit cards through a residential burglary, vehicle theft, etc. The OTG then goes to a retail store to purchase numerous gift cards, usually via self-checkout. The transactions range from US$1,500 - US$50,000 per incident. Some of the coveted gift cards are Apple, Home Depot, and/or cash cards, e.g. Vanilla Visa, etc.

Scheme two: Vanilla Visa gift cards, for example, are stolen from retail stores by an OTG. The OTG will create a bar code that they will place over the Visa barcode. The OTG then covertly brings the altered Visa cards back into the store and returns them to where they were stolen from. Upon purchase, the OTG barcode will add the funds, up to US$500 per card, to a separate, non-Visa gift card.

Scheme three: transnational triangular fraud involves illicit online sellers that operate across all of the online marketplaces.

The illicit seller will list products that they do not actually have and, when they get an order, purchase the product from a retailer using a credit card number from an account take over scheme. Typically, an elderly individual is exploited as part of the account takeover scheme to obtain the credit card number.

The retailer then fulfills the order and ships the product to the unsuspecting customer. The retailer gets hit for loss of product and chargeback from credit card company. They also use drop shipment orders at "work from home" private residences in the US, that reship the stolen product internationally.

Red flags:

- Subject(s) in possession of numerous SVCs
- Subject(s) purchasing large amounts of SVCs, physically or electronically
- SVCs loaded with funds in the United States, withdrawn overseas
- Unusual level and frequency of ATM usage
- Unusually high value/volume card activity
- Card usage in unexpected or high-risk countries (Mexico, China, Russia, India, Middle East, etc.)

Operation King of Thieves

Case study provided by Homeland Security Investigations, Houston, Texas

In 2015, HSI targeted a TCO profiting from ORC and other criminal activities. The TCO was comprised of individuals with familial and business ties to Palestine and Egypt who operated wholesale, trading, and/or distribution companies. The owners of these businesses employed professional thieves, known as boosters, to steal specific merchandise from retailers throughout the United States. The OTG leaders were involved in human smuggling by financing the "coyote fees" of deported individuals to return to the United States.

Anti-theft stickers removed from stolen OTC medications

After being provided a list of items to steal and front money, by cash or wire transfer, the boosters, mainly from Honduras, would travel throughout the United States targeting retailers such as CVS, Walgreens, and Rite-Aid, among others.

The TCO leaders would also wire money to the boosters while they were traveling to continue their stealing cycles. This TCO centered on stolen health and beauty goods, e.g. over-the-counter medications, diabetic test strips, shaving razors, etc. These items are high value and easy to conceal.

The main method utilized by the boosters to steal was to covertly remove the aforementioned items from the shelf, and place them into a large bag or purse lined with heavy duty aluminum foil to defeat the store security sensors. Once stolen, the boosters would utilize shipping centers to send the stolen items to alias names specified by the TCO. When the boosters returned to meet with the TCO leaders, they would be paid in cash or by check. Utilizing a former booster as a confidential source (CS), HSI was able to insert this individual into the organization by making multiple sales of purportedly stolen merchandise to the TCO leaders. Additionally, it was later revealed that the TCO began a large-scale healthcare fraud conspiracy involving various pharmacies throughout the United States, and millions of dollars in criminal proceeds were being utilized at casinos and wired to individuals and businesses overseas.

From 2018 through 2021, HSI led enforcement operations against the TCO with assistance from the U.S. Food and Drug Administration – Office of Criminal Investigations (FDA-OCI), the U.S. Department of Health and Human Services – Office of Inspector General (HHS-OIG), the Federal Bureau of Investigation (FBI), and various state/local law enforcement agencies. There were 24 criminal arrests and approximately US$8,000,000, two homes, and land were seized. The criminals were charged with Interstate Transportation of Stolen Goods (18 USC § 2314), Possession of Stolen Property (18 USC § 2315), Conspiracy (18 USC § 371), Monetary Transactions Derived from Specified Unlawful Activities (SUA's) (18 USC § 1957), Healthcare Fraud (18 USC § 1347) and Attempt and Conspiracy (18 USC § 1349). It was determined that there was a revenue loss of approximately US$30 million to retailers directly related to ORC and US$134 million to insurance and government programs related to healthcare fraud.

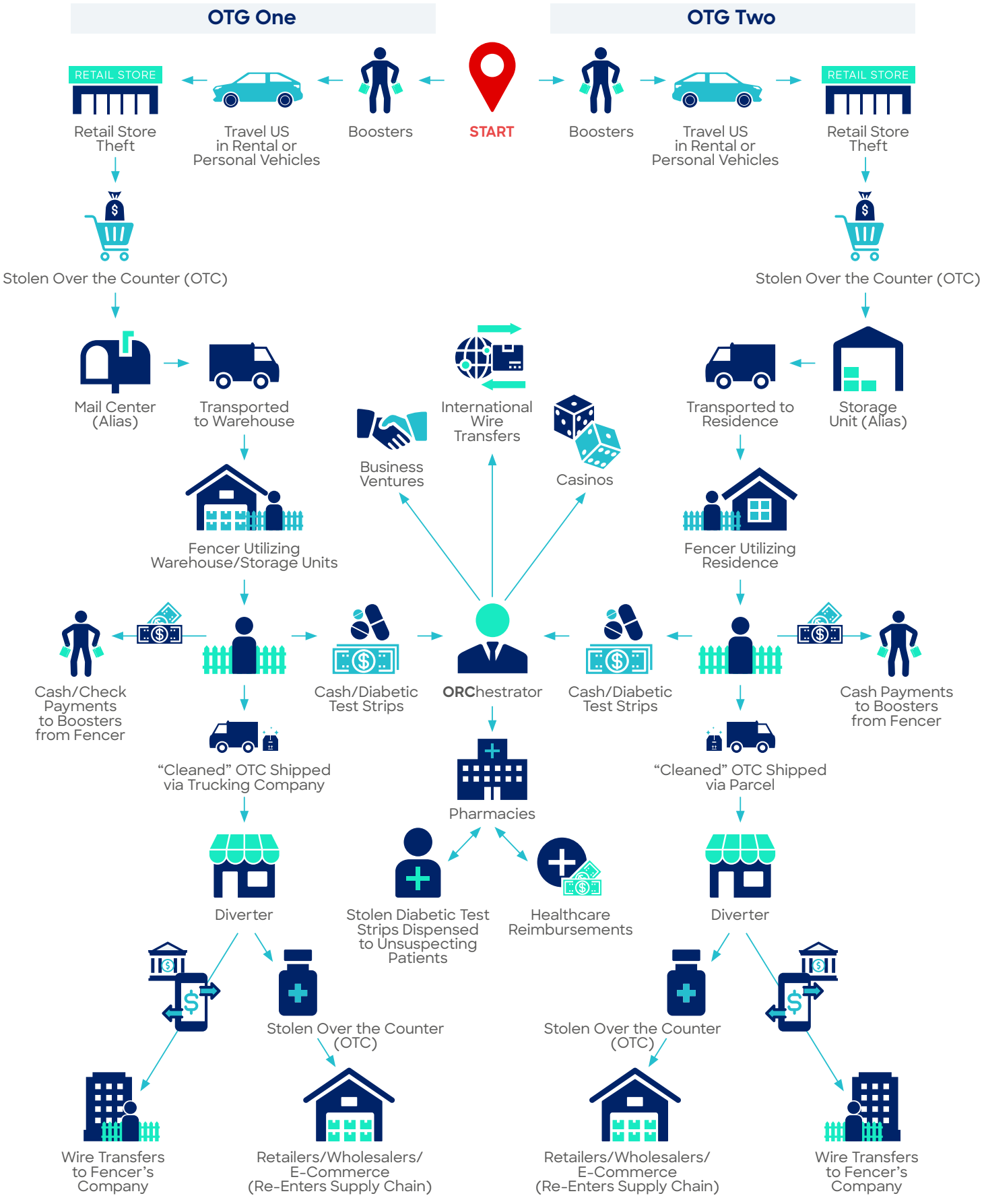
OTC medications that have been "cleaned," organized, and prepared for shipment

Aluminum-lined purse utilized by boosters to steal retail merchandise

Lighter fluid and heat gun used to "clean" stolen OTC medication

Inventory/payment lists utilized by boosters and fencers

Operation King of Thieves financial and stolen merchandise flows



Step one:	Boosters would steal health and beauty supplies from retailers across the US. The boosters have a written list of what was stolen and sent. In this case, diabetic strips were often stolen as the ORChestrator of the organization owned and operated numerous pharmacies.
Step two:	The boosters would sell to the fencers and the fencers would inventory the stolen items. Boosters shipped their stolen goods via a mail center or a storage unit to take to the fencer's warehouse or residence. The fencers maintained a list of what was received.
Step three:	Once the items were inventoried and the lists reconciled, the boosters would typically be paid in cash by the fencers; however, at times checks were issued. Should the booster continue to boost, the fencer would wire the booster money to cover travel and lodging expenses. These expenses were then deducted from their final payment.
Step four:	The fencers may further clean the stolen goods to send to a diverter. The diverter may use a shell or front company to ship the goods to retailers, wholesalers, or e-commerce platforms to re-enter the supply chain. The proceeds would go into the diverter's shell company bank account and be wired to the fencer's shell company.
Step five:	The fencers would provide the ORChestrator with the stolen diabetic strips instead of cash, and the ORChestrator and fencer would split the profits 50/50.
Step six:	The ORChestrator would distribute the test strips to his pharmacies to be dispensed to unsuspecting customers.
Step seven:	The ORChestrator would bill the healthcare companies for the test strips that were dispensed. This "cleaned" the money.

Red flags associated with the King of Thieves case:

- Structured deposits/withdrawals to avoid identification (ID) requirements
- Business owner and associates may attempt to provide gifts of money, food, and beauty items to bank personnel
- Primary business may be registered with the state, but comes back to a PO box or storage unit
- Checks issued from wholesale, trading, and/or distribution-type companies, usually in even amounts, to individuals for which no relationship or lawful purpose can be established
- Checks from the business account do not note the purpose of payment in the memo section
- Large business-to-business wire transfers related to wholesale, trading, and/or distribution-type companies involved with health and beauty supplies, e.g. over the counter (OTC) medications, infant formula, diabetic supplies, shaving razors, electric toothbrush heads, hair growth items
- One or more wire transfers paid for by cash (within 24 hours of each other), usually under US$1,000, to an individual out of state
- Open-source information indicates previous involvement in ORC, fraud, theft, etc.
- Payments to multiple storage and/or warehouse companies

Red flags associated with the King of Thieves case (cont.):

- Numerous payments to rental car companies, especially in the area in which the subject resides
- Rental payments to multiple mail centers for PO boxes

Investigative recommendations and considerations:

- The criminal organizations in these cases will usually register a business with the state in which they are located to show they are legitimate. However, they are known to also register a separate business name within the county in which they are located. Therefore, record checks of these businesses should include searches within the state's Secretary of State database as well as the county clerk's assumed name/DBA database.
- Criminal organizations are also known to register their businesses to mail centers with PO box-type addresses but utilize storage units and warehouses to conduct the criminal activity. Therefore, this should be considered suspicious when factored with other red flags.
- Open-source searches can yield information on previous arrests, previous companies, etc. Doing some additional research on suspicious individuals can reveal a past history of criminal activity and/or businesses involved in ORC.

Operation At the Card Wash

Case study provided by Homeland Security Investigations, Long Beach, California

In 2019, HSI identified a national network of wholesale electronics distributors suspected of engaging in forms of trade-based money laundering by sourcing merchandise derived from various fraud schemes. These schemes have exploited the use of gift cards in laundering or masking criminally derived funds.

In one scheme, for example, a phone scam victim is coerced, under false pretenses, into purchasing and providing gift cards to scammers over the phone. The victims' gift card numbers and access codes are ultimately transmitted to straw-purchasers or "runners", who utilize the cards for transactions in retail stores acquiring high value consumer electronics or, even new gift cards.

These retail store cards, derived from telecom scams, were ultimately used by the wholesalers in the network to acquire consumer electronics for their inventory.

Victims are instructed by scammers impersonating government officials or technical support personnel to purchase various retail gift cards

After the victim has loaded funds onto the gift cards, scammers instruct them to provide the card's number and access code over the phone

Scammers digitally transmit the gift card numbers provided by victims to "runners" through cell phone messaging applications; runners are waiting at retail stores to conduct purchases of consumer electronics, ultimately laundering the victims' funds

Runners also launder funds by purchasing new physical gift cards with the digitally transmitted victim funds

Consumer electronics, (namely Apple, Nintendo, Google, and Amazon) suspected to have been acquired through the use of fraudulently funded gift cards, are believed to have then been resold internationally.

In 2021, HSI Los Angeles's investigation led to the federal indictment of four defendants related to a scheme to launder Target gift cards purchased by the victims of scams. The indictment alleged that the defendants obtained more than 5,000 gift cards from a group that called itself the "Magic Lamp", and sold gift card information via an online messenger application. Some of the defendants oversaw the distribution of gift cards to "runners," who used the funds on the cards at Target stores primarily in California to purchase consumer electronics and other gift cards. Through the purchases and other transactions at multiple Target stores, the defendants and their co-conspirators sought to conceal the fact that the gift cards had been originally funded with fraudulent proceeds.

Customs records indicated that from the beginning of August 2019 to the beginning of November 2020, a business operated by one defendant exported merchandise with a total declared value of over US$13 million, consisting of iPads, cell phones, Airpods, and Apple watches, to recipients in Hong Kong.

The result of the scheme's method is the value of the victims' funds being transferred through gift cards into consumer merchandise, effectively laundering the proceeds from the initial victim source.

Elements of the scheme:

- Trade-based money laundering
- Third party bank accounts
- Transnational criminal enterprises

Criminal statutes:

- Wire fraud
- Credit card fraud
- Interstate transport of stolen property
- Identity theft
- Money laundering
- Unlicensed money remitting

Characteristics of schemes similar to the At the Card Wash case:

- Entities, claiming to be wholesale businesses, remitting numerous payments to individuals (runners) instead of suppliers consistent with their line of business
- Wholesalers appearing to both purchase inventory and sell inventory to other wholesalers (which may normally diminish profit margins under legitimate circumstances)
- Payments sent to seemingly unrelated business types; for example, an electronics wholesaler sending funds to a car rental business
- Large, even-numbered fund transfers to entities appearing to be suppliers or buyers

Section Nine: Additional Red Flag Indicators and Emerging Typologies

Financial institutions, law enforcement, and retailers are all key stakeholders in combatting ORC. Financial institutions play an important role in uncovering syndicate organizations and tracing illicit financial flows throughout the formal banking sector. Investigations conducted by retailers and law enforcement will benefit from financial intelligence and investigation units having a greater awareness of typical ORC typologies and red flags.

Typologies tied to ORC may include current money laundering tactics, like using shell companies to hide the criminal's identity, or transaction laundering.

However, as technology advances and new threats emerge, it is important to take into consideration vulnerabilities in regulations and technology that criminals can exploit.

This section will cover red flag indicators of suspicious activities and typologies leveraged in an attempt to evade law enforcement detection. The existence of one single red flag indicator does not necessarily indicate unlawful criminal activity; however, multiple red flag indicators in a transaction or a series of transactions with no logical business explanation should elevate the concern of potential criminal activity. The presence of these red flag indicators should encourage further investigation and reporting, when appropriate.

Red Flag Indicators Related to Transactions

The red flags below illustrate how ORC could be identified through unusual or uncommon patterns of transactions.

Cash, check, and money order transactions

- Significant movement of cash funds between various states.
- Consistent pattern of cash deposits in a geographic location away from the customer's residence, rapidly followed by cash withdrawals in similar amounts (much like drug trafficking or other illegal activity).
- Large cash deposits into an individual's account which do not coincide with their occupation. Cash deposits are typically in US$100 denominations.
- Large cash or money order, often structured, withdrawals from a business account that does not coincide with business operations.
- Structured cash deposits to avoid ID requirements and reluctance to share source of funds.
- Check payments issued to multiple individuals for which no relationship or lawful purpose can be established.
- Check payments issued to multiple companies with "liquidator" or "wholesale" in their name. Overall funds may be co-mingled.
- None of the checks in the business account note the purpose in the memo section.
- Multiple checks written on the same day to cash, to ensure the amount of the check does not exceed US$10,000.
- Despite no reporting requirements, multiple checks written on the same day in amounts less than US$10,000.
- Checks written from the business account payable to cash are deposited in principal's personal accounts.
- Business checks written to cash on a regular basis in amounts that exceed a typical business's petty cash requirement.
- Business check cashed at a financial institution where the check originated from, instead of deposited into another business's bank account.
- Checks written to individuals, as opposed to legitimate business suppliers.
- Checks drawn from suspicious financial activities are negotiated in foreign countries.
- Multiple money orders in increments of US$500 or less deposited in the bank account where the remitter of the money order is the same as the authorized signers on the bank accounts, for which the checks are being deposited.

Wire transactions

- Wire transfers where no business relationship can be established between the customer and the originator of the wire.
- Wire transfers sent in large, round dollar, repetitive amounts on a consistent date (e.g. weekly or monthly).
- Payments received with no apparent links to legitimate funds (purchase of product, creation of product).
- Wire transactions containing limited content and lacking related party information.
- Payments to or from the business with no stated purpose, and no reference to goods or services or information provided in the purpose field (such as an invoice or contract number).
- Challenge in obtaining sufficient information to positively identify originators or beneficiaries of accounts, or other banking activity, when leveraging open-source internet, commercial databases, or direct inquiries to the customer.
- Unusually large number of beneficiaries receiving funds from one company. This may be indicative of payment to fencers.
- Wholesale retailers sending multiple wire transfers to individuals not affiliated with the company or located in different jurisdictions.

Automated clearing house (ACH) transactions

- Large volume of credit transactions from online marketplaces for sale of stolen goods.
- Large and frequent deposits from online payments systems which have no apparent online, brick and mortar, or auction business.

Prepaid cards

- Customers purchasing several pre-paid cards; purchases are not commensurate with normal business activities.

Cryptocurrency

- Cryptocurrency exchange deposits that significantly exceed the stated income on account applications with no identifiable source. Further due diligence yielding information that the customer has an extensive criminal history.
- Customers using mixers, privacy coins, or private wallets to further mask their identity.
- Customers buying, selling, or trading cryptocurrency through third party payment processors.

Red Flag Indicators Related to a Customer or a Customer's Business

- Business is a shell company, registered in a high-risk national (e.g. Delaware or Wyoming) or high-risk international jurisdiction, and has structured ultimate beneficial ownership below standard reporting of 25%.
- Business is a warehouse, merchandise seller, or other similar business line with no evidence of purchasing goods or products.
- Business has dramatically different amounts and patterns of currency deposits from similar businesses.
- Size and frequency of currency deposits increase rapidly with no corresponding increase in credit transactions.
- Customer repeatedly uses bank locations that are geographically distant from the customer's physical locations without logical business purpose.
- Customer uses personal account for business purposes.
- Customer conducts multiple currency deposits to various accounts that appear unrelated.
- Searches indicate that buyer/seller have identical addresses, with the same individuals listed as registered agents.
- Individual receives deposits from retailers or export companies where the client does not have any apparent business relationship.
- The principal of the business uses the bank's smartphone applications to send multiple transfers in the tens of thousands of dollars to their personal accounts.
- Occupation listed for the customer is not commensurate with the volume and type of financial activities.
- Customers tied to the suspicious activity may all have the same physical address listed.

Red Flag Indicators on Customers' Bank Statements

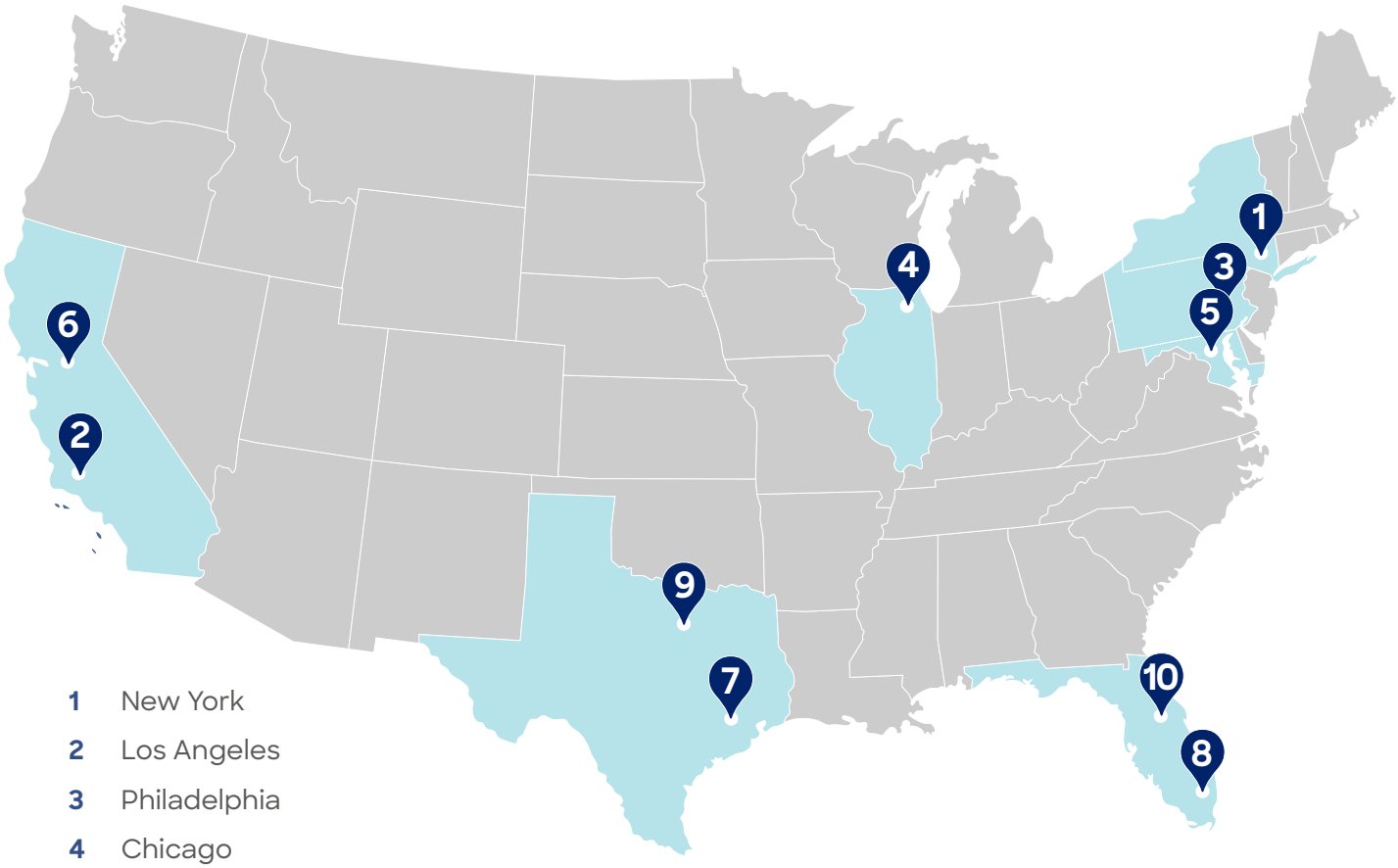
- Frequent cash deposits or withdrawals.
- Even dollar payments between illicit wholesaler and diverter.
- Repeated payments to transportation (trucking) company/companies.
- Ongoing payments to replenish shipping supplies, such as pallets, boxes, tape labels, and shrink wrap.

Red Flag Indicators Related to Domestic and International Geographical Risks

These risks are associated with source, destination, and transit jurisdictions of a transaction. They are also relevant to risks associated with the originator of a transaction and the beneficiary of funds. In addition, they may be applicable to the customer's nationality, residence, or place of business.

- Subjects sending transfers to receivers in multiple countries with no apparent relationship.

Cities ranked by volume of reported ORC cases (not including shoplifting)



1 New York
2 Los Angeles
3 Philadelphia
4 Chicago
5 DC/Baltimore
6 San Francisco
7 Houston
8 Miami
9 Dallas
10 Orlando/Tampa

Source: chart provided by Ben Dugan, President of C.L.E.A.R.

Red Flag Indicators Tied to Open-Source Intelligence (OSINT) Research, Including Online Marketplaces[12]

What is OSINT?

OSINT is defined as "data produced from publicly available information that is collected, analyzed, and disseminated while addressing a specific intelligence requirement."[13]

Investigators can use publicly available information to investigate a person, place, or event. It can also be used to geolocate pictures. The surface web is just one aspect of analysis; the deep and dark web can also be utilized, with specific tools to uncover intelligence or nefarious activity conducted.

Caution: misinformation can be high using only OSINT intelligence analysis, therefore, the intelligence should be verified with company or institution records to the extent possible. If not, include the information as a red flag in your investigation.

- Online search indicates that buyer and seller have identical addresses with the same individuals as registered agents.
- Open-source internet search fails to support the client's stated business or revenue.
- Merchandise still in shipping plastic (cargo theft).
- Large variety of sizes available.
- A variety of merchandise, new with tags.
- Different sellers using the same photos, or posting photos of merchandise with the same background.
- Merchandise photos with sensor tags or other electronic article surveillance (EAS) devices still attached.
- Defaced product labels.
- Using stock retail photos.
- Photos of merchandise taken inside a vehicle.
- Item price is significantly less than price of other sellers on the marketplace or below manufacturers cost.

12. Retail Industry Leaders Association, https://www.rila.org
13. Air Force Open Source Intelligence (OSINT), May 2012, afi14-130.pdf (fas.org)

- Specific language using words such as: “like new”, “new in box” or “NIB”, “new with tags” or “NWT”, “unopened”, “taking orders [for product]”, “DM for orders or size”, “factory sealed”.
- Company (shell) website not functioning or has no information.
- Reviews about the company may be scarce, indicating a new seller or one that is working from seller ID to seller ID. However, it is also important to point out that often times the ORC seller may appear to be a very legitimate business and may have many positive reviews.
- Company’s address using a Google Earth search shows land with no building, a warehouse with no sign, or a building without the company’s name/storefront.
- Company’s website does not allow you to buy a product outright, indicates you must contact the retailer first.
- Multiple usernames using the same internet protocol (IP) address.
- Usernames that are not standard first/last names. May include a handle, street name, nickname, or a business entity beginning with “Pawn” or “Flea Market”, or more often names like “below sale”, “wholesale”, or “wholesale OTC”.

Common Indicators on the Surface Web Relating to Stolen Goods[14]

Common Emojis Used in ORC	Common Emojis Used While Interacting with Customers or Posting the Products on Social Media/Online Marketplaces
	 Translation from left to right: on lock - controlling the hustle/ game, running things, credit card hustling, making money Translation from left to right: got a bag of money, credit card hustling, running, made 17k

Source: RILA

14. Data from RILA (Retail Industry Leaders Association) home page, https://www.rila.org

Section Ten: Emerging Typologies

Front and Shell Companies

Money laundering typically occurs in three main stages: placement, layering, and integration.

OTGs may be using shell companies to process illicit funds from stolen goods, masking the identity of the funds to make transactions appear legitimate.

Therefore, know your customer (KYC) procedures and enhanced due diligence (EDD) are vital mechanisms to determine if the account is functioning as a front or shell company. While there are many possible configurations of these networks, the figure below shows a common business model within the ORC cycle where OTGs can hide illicit proceeds within front and shell company ownership.

Leveraging front and shell companies in ORC

Warehouse/ Wholesaler Front Companies

The fencer's warehouse is typically a **front company**, with the characteristics of a legitimate business; however, stolen retail products are co-mingled.

Diverter(s) Front Companies

The diverter is a **front company** that receives the stolen inventory in bulk and sells it to a retailer. In large schemes, there could be several front companies acting as diverters.

E-Commerce Front Companies

The fencers or other individuals within the OTG may set up **e-commerce front companies**, where the stolen goods are advertised for re-sale. These are on typical online marketplaces.

Brick and Mortar Front Companies

The fencers may own or sell to a brick and mortar store. Similar to the wholesaler and diverter, the brick and mortar store can act as a **front company** and sell the stolen goods or co-mingle with legitimately purchased goods. These stores can be owned by the fencer, diverter, or the ORChestrator.

Professional Money Laundering Shell Companies

The OTG will typically leverage a professional money launderer to launder the illicit money through multiple different shell companies. These companies are NOT typically in the names of the warehouse, wholesaler, or diverter. These are unrelated and the bank accounts would typically just show the sale of stolen goods.

Exploiting E-Commerce

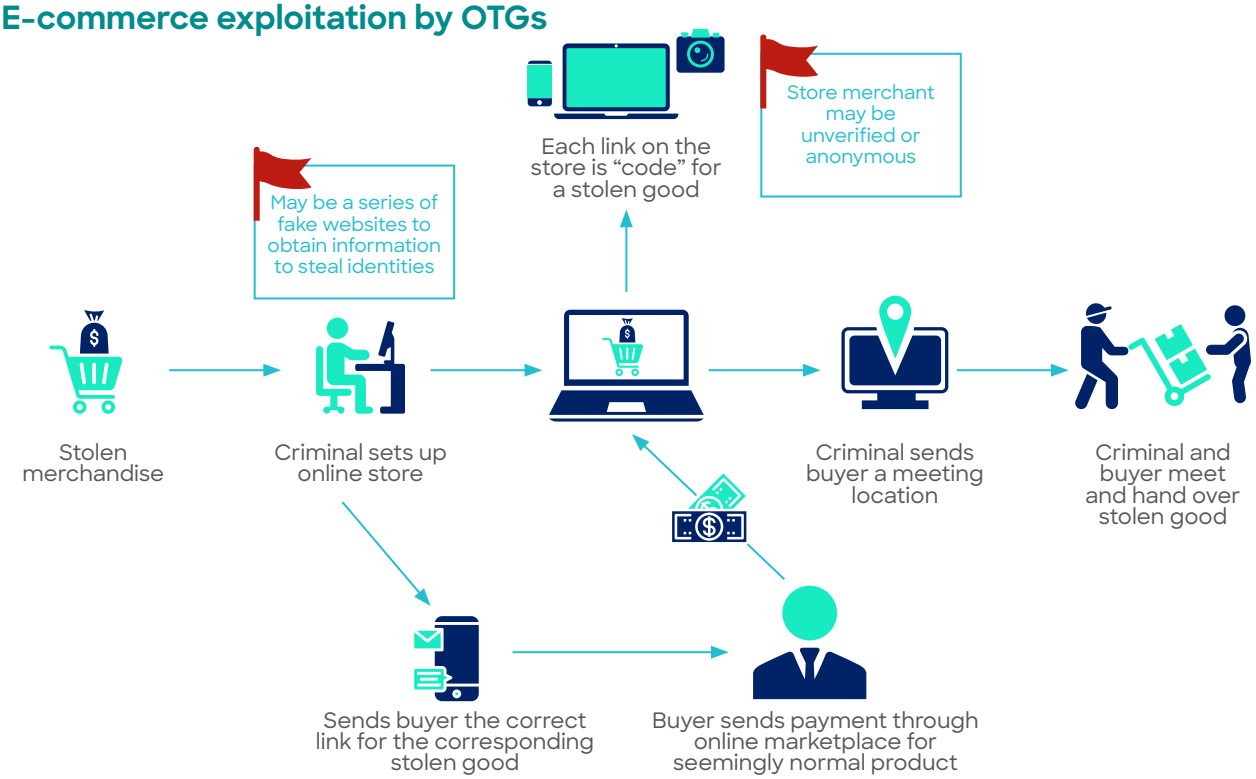
The COVID-19 pandemic increased online shopping and the number of online marketplaces. Some of these online marketplaces allow anonymous merchants to own shops and sell merchandise.

Therefore, e-commerce websites can be exploited by OTGs to re-sell their stolen merchandise.

Despite this, it's estimated that only nine percent of retailers view e-commerce crime as a priority.[15]

The below figure shows how an ORC criminal can exploit e-commerce platforms for financial gain regarding high-end or designer goods. However, fencers or cleaners can ship clean merchandise directly to the buyer via the online marketplace with anonymity, depending on the website, to bypass the in-person meet up. It is likely the criminals will ship from the shell company name with a fake or front address to mask their identity.

E-commerce exploitation by OTGs



The above image is more typical of activity on certain marketplaces like Facebook Marketplace, Craigslist, or even apps like OfferUp or Let Go. ORC transactions also happen on platforms like eBay and Amazon and can appear as very legitimate transactions.

15. SecurityTags.com, May 2021, 10 Retail Theft Statistics in 2021, https://securitytags.com/retail-theft-statistics-2021/

Example of steps for selling stolen sensitive or designer goods on e-commerce websites, using a shell company

Step one:	The stolen merchandise will be photographed and uploaded as a listing on the online marketplace, either anonymously or with a shell company name/store.
Step two:	If selling a sensitive or designer good, it is likely that the criminal will not upload the actual good. Instead, they will upload a disguise good and will send a message to their buyer via an encrypted messaging system with their code for the correct stolen good.
Step three:	The buyer will purchase a seemingly normal product through the online marketplace. They may use cryptocurrency or third-party payment processors to further mask their identity.
Step four:	The payment is given to the criminal through the online marketplace. They will then send the buyer, via encrypted messaging, coordinates and a time to meet (if the good is very sensitive), or will ship the good directly to the buyer under their shell company name.
Step five:	If the good is very sensitive, the buyer will go to the location and pick up the good. The funds have already been given to the criminal through the online marketplace.

It is important to note this process will only be used for stolen sensitive goods or designer goods.

In many cases of ORC using online marketplaces, the goods will be "cleaned" of their original tags and packaging and made to look like a legitimate retailer is selling them online; they can be bought directly through the online marketplace and shipped to the customer.

Trade-Based Money Laundering (TBML) Schemes Relating to Organized Retail Crime (ORC)

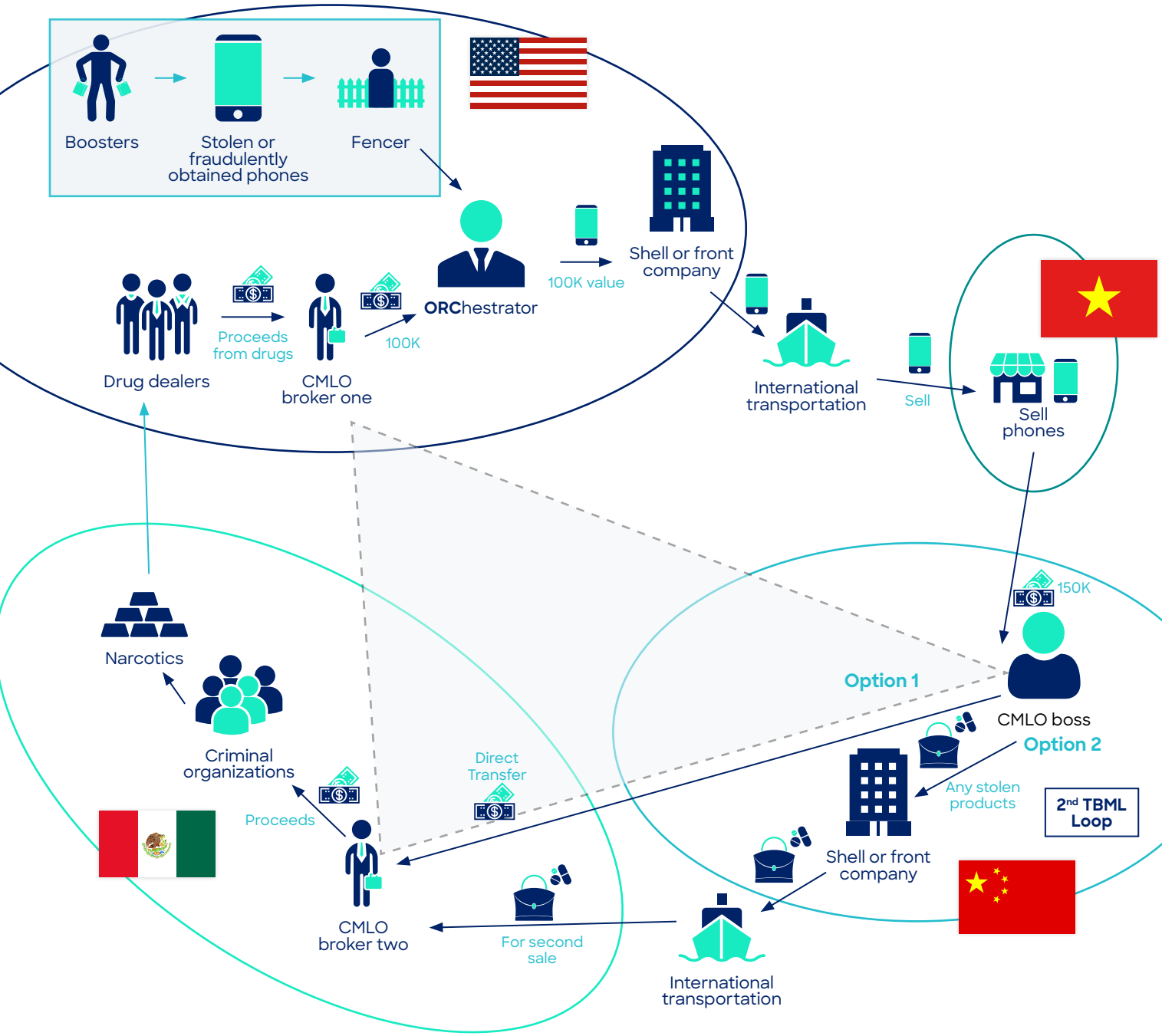
Complex organized retail crime (ORC) syndicates use intricate methods to hide their financial flows and mask the illicit nature proceeds stem from.

One common method of money laundering that criminal organizations, including ORC criminals, leverage is trade-based money laundering (TBML).

The Financial Action Task Force (FATF) defines trade-based money laundering as the "process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins". There are numerous different approaches to TBML, therefore the example given for ORC criminals may not always look the same for all money laundering schemes around the world. The figure on the following page outlines a previously thwarted money laundering scheme used by a complex organized retail crime syndicate, including using Asian brokers and Mexican drug cartels.

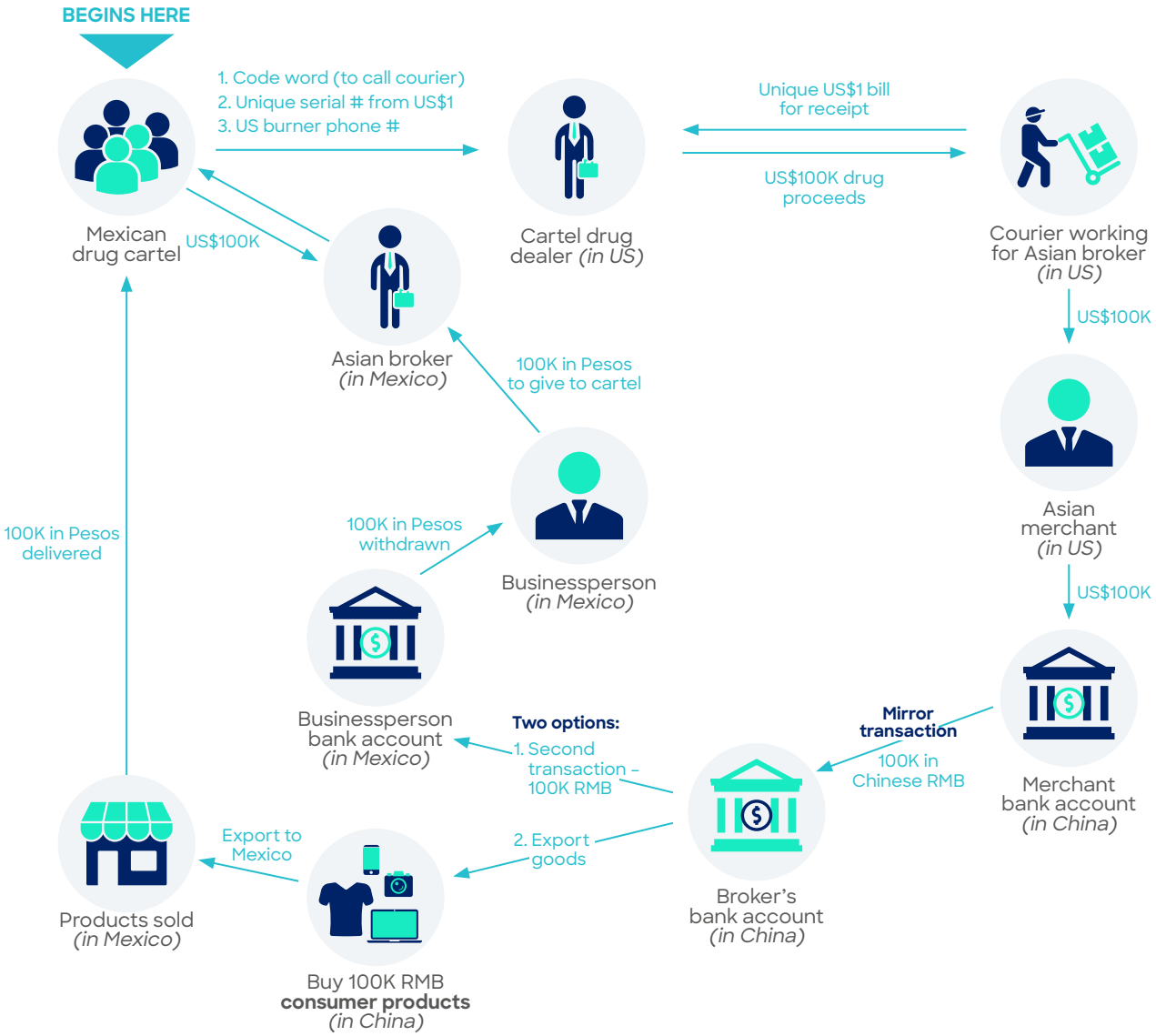
TBML scheme using Asian brokers and Mexican drug cartels

1. Boosters steal or fraudulently obtain phones from a large retailer
2. Boosters sell the phones to a fencer at lower than retail value for cash
3. Fencer sells the phones to the ORChestrator
4. Orchestrator amasses a large volume of phones, enough to fill a shipping container
5. ORChestrator sells phones to an Asian broker for re-sale in a foreign country
6. Financial flows follow an Asian broker transaction laundering scheme
7. Broker recovers investment and makes a profit from stolen phones and cycle



Asian broker transactions using Mexican drug proceeds tied to ORC[16]

1. Asian brokers give the cartel a burner phone number, a unique US dollar serial number, and a code word.
2. Cartel gives their dealer in the US the phone number to call, introduces themselves with the code word, and meets the broker with the unique one dollar (to be deemed legitimate).
3. The Asian broker gives the dirty drug money to a US based Asian merchant.
4. Merchant transfers the equivalent of money to the broker in Asia's account.
5. Broker can decide to either do a second mirror transaction to a businessperson in Mexico or export goods to Mexico.
6. Either the revenue from the products sold in Mexico or the businessperson will deliver the equivalent in pesos to the cartel.



16. Reuters, December 2, 2020, Factbox: Step by step - How Chinese 'money brokers' launder cash for Mexican drug cartels, https://www.reuters.com/article/us-mexico-china-cartels-factbox/factbox-step-by-step-how-chinese-money-brokers-launder-cash-for-mexican-drug-cartels-idUSKBN28D1LW

PART THREE: EFFECTIVE REPORTING OF ORC ACTIVITY AND OTHER AFC PROGRAM CONSIDERATIONS FOR FINANCIAL INSTITUTIONS

Section Eleven: Suspicious Activity Reporting Considerations

SAR Form Considerations

Currently the SAR form does not have a specific SAR field for organized retail crime related activity.

Therefore, if a financial institution is filing a SAR that is potentially associated with or the circumstances suspect ORC, it is recommended that they use SAR field (38)(Z) (other suspicious activities), and manually write "organized retail crime".

A financial institution should ensure any other appropriate SAR fields are checked that correspond with suspicious activity identified throughout the investigation. For example, as applicable, suspicion concerning the source of funds, use of multiple transaction locations, and two or more individuals working together.

Targeted Suspicious Activity Terms (TSATs)

Law enforcement will proactively use data analysis to identify new cases and complement existing ORC cases by running a series of TSATs and criteria against SAR filings.

Therefore, it would be beneficial to consider including the following targeted terms in your narrative, as appropriate:

Targeted suspicious activity terms (TSATs)

SAR Narrative and SAR Supporting Documentation Considerations

Law enforcement considers it highly useful information to include TSATs in the SAR narrative.

If a financial institution is filing on ORC activity or subjects tied to an OTG, it is recommended, as applicable, that the above TSATs be used. It would also be useful to describe the relevant behavior and connections between the activities reported and ORC and/or OTG.

While it is not common for financial institutions to pull and retain photos, or video surveillance, of individuals suspected of being involved in criminal activity making deposits or withdrawals for every SAR filed, it can be highly useful to law enforcement. Therefore, it is recommended, as part of the SAR narrative, that financial institutions indicate that photo/video surveillance is available; however, further indicate due to photo/surveillance data limitations (e.g. being purged after a set timeframe), if law enforcement does identify any SAR where they would like the photo/surveillance footage, they should reach out to the financial institution that filed the SAR and request for them to pull and retail the footage ASAP as part of current or future SAR supporting documentation.

This is important for law enforcement to understand, as typically the photo/video footage would have been purged by the time a subpoena is issued.

Additionally, if a bank employee has communication with a subject, or witnesses the subject conducting a suspicious activity, and the information obtained during the communication or witnessed during the transaction is pertinent to the SAR filing, the bank should retain the name of employee, position, date, and time of communication as part of the SAR supporting documentation. This is highly useful information to law enforcement when investigating and prosecuting cases.

Lastly, as previously described, law enforcement agencies utilize asset forfeiture to disrupt and dismantle OTGs by seizing and forfeiting proceeds of their crimes and to compensate the victims of those crimes.

While filing SARs, bank employees could facilitate the identification of assets owned or used by individuals suspected of ORC, if any assets that could be identified as part of their banking relationship with such individuals are listed in the narrative.

SAR filing notification considerations

Should you file a SAR that you believe is connected to ORC or an OTG, upon filing the SAR notify HSI at: **HSI.OTG@hsi.dhs.gov**.

Section Twelve: Other AML Program Considerations and Enhancements

USA Patriot Act: Information Sharing

314(a)	314(b)
Section 314(a) encourages information sharing between law enforcement and financial institutions regarding individuals, entities, and organizations engaged in or reasonably suspected of engaging in terrorist activity or acts of money laundering. If during your search you have a positive match and during your subsequent investigation to determine if a SAR should be filed, the business name includes warehouse, merchandise, liquidator, or some of the other high-risk businesses for ORC, you should determine if ORC is possibly involved and if so, consider the SAR recommendations noted herein during their filing.	Information sharing among registered financial institutions remains an effective mechanism to detect and report the proceeds of illicit financial crimes. Applicable financial institutions should strongly consider registering with the Financial Crimes Enforcement Network (FinCEN), and leveraging the 314(b) mechanisms to let other financial institutions know that the information they are sharing or requesting specific to individual, organization, or financial activity is because of suspected money laundering tied to ORC or an OTG.

Training

Should a financial institution determine they have increased ORC risk based on their customer risk profile within a specific business line, they should consider enhancing their existing AML/BSA training program to include:

- An introduction to ORC and how individuals or businesses tied to ORC may be a risk or threat to the financial institution
- Nexus of ORC to the US National Priorities and other predicate offenses and suspicious and unlawful activities (SUAs)

- Red flags and examples of financial activity tied to ORC (this could be high-level training for tellers on red flag cash activity or more comprehensive training for AML investigators and lenders on TBML case examples)
- Reinforcing the importance of alerting the appropriate parties of potential suspicious activity
- SAR filing obligations related to money laundering and other illicit financial crimes, including ORC

Remember to document your ORC training, including the dates of the training sessions, attendance records, and content presented.

Due Diligence for Businesses Typically Used as Front Companies for ORC

Business customers, such as wholesalers, merchandise liquidators, wholesale and online auctions, may pose higher risks for co-mingling or laundering illicit monies tied to ORC or OTG activity. In the next section, several North American Industry Classification System (NAICS) codes have been provided to assist financial institutions in identifying businesses that may pose a higher risk for ORC or OTG activity.

Should a financial institution determine that a customer poses a higher risk because of the nature of the business, subsequent volume of actual or anticipated activity, opaque ownerships, or business structure, enhanced due diligence both at account opening and throughout the relationship would be prudent.

Below are suggested enhanced due diligence considerations for higher-risk accounts tied to potential ORC or OTG activity. These recommendations would complement already existing standard customer due diligence, including the collection of beneficial ownership and controlling party information, conducted by the financial institution.

Account opening

The financial institution should understand the following:

- Source of funds and wealth, including volume of currency and total sales, and primary method of conducting transactions
- Customer's primary area of business
- Business operations
- Major customers and suppliers
- Business registration in comparison to business operations and anticipated location of account activity

Ongoing monitoring

The financial institution, as either part of high-risk account monitoring or through transaction monitoring of these higher-risk entities, should consider the following, as part of their review:

- Compare by both dollar and volume the number of credit transactions in comparison to similar customers (by NAICS code) in a similar geographic area. If a customer sells their products on an online marketplace, the financial institution should do a comprehensive investigation of the customer's store to look for potential red flags, like those identified in this report.
- Conduct trending transactional analysis, such as a vertical or horizontal analysis of the bank or financial statements and request any relevant invoices or receipts to substantiate any transactional anomalies or variations.
- An enhanced focus on the customer's suppliers. The customer's bank account should evidence purchase of goods from suppliers to subsequently sell. If the customer only had credits for sales, that is a red flag.

2022 NAICS codes and descriptions

459510
Used merchandise retailers

455219
All other general merchandise retailers

456199
All other health and personal care retailers

459999
All other miscellaneous retailers

456120
Cosmetics, beauty supplies, and perfume retailers

493110
General warehousing and storage

45120
Wholesale trade agents and brokers

423990
Other miscellaneous durable goods merchant wholesalers

424990
Other miscellaneous nondurable goods merchant wholesalers

423690
Other electronic parts and equipment merchant wholesalers

423910
Sporting and recreational goods and supplies merchant wholesalers

488991
Packing and crating

423920
Toy and hobby goods and supplies merchant wholesalers

423840
Industrial supplies merchant wholesalers

452319
All other general merchandise stores

339999
All other miscellaneous manufacturing

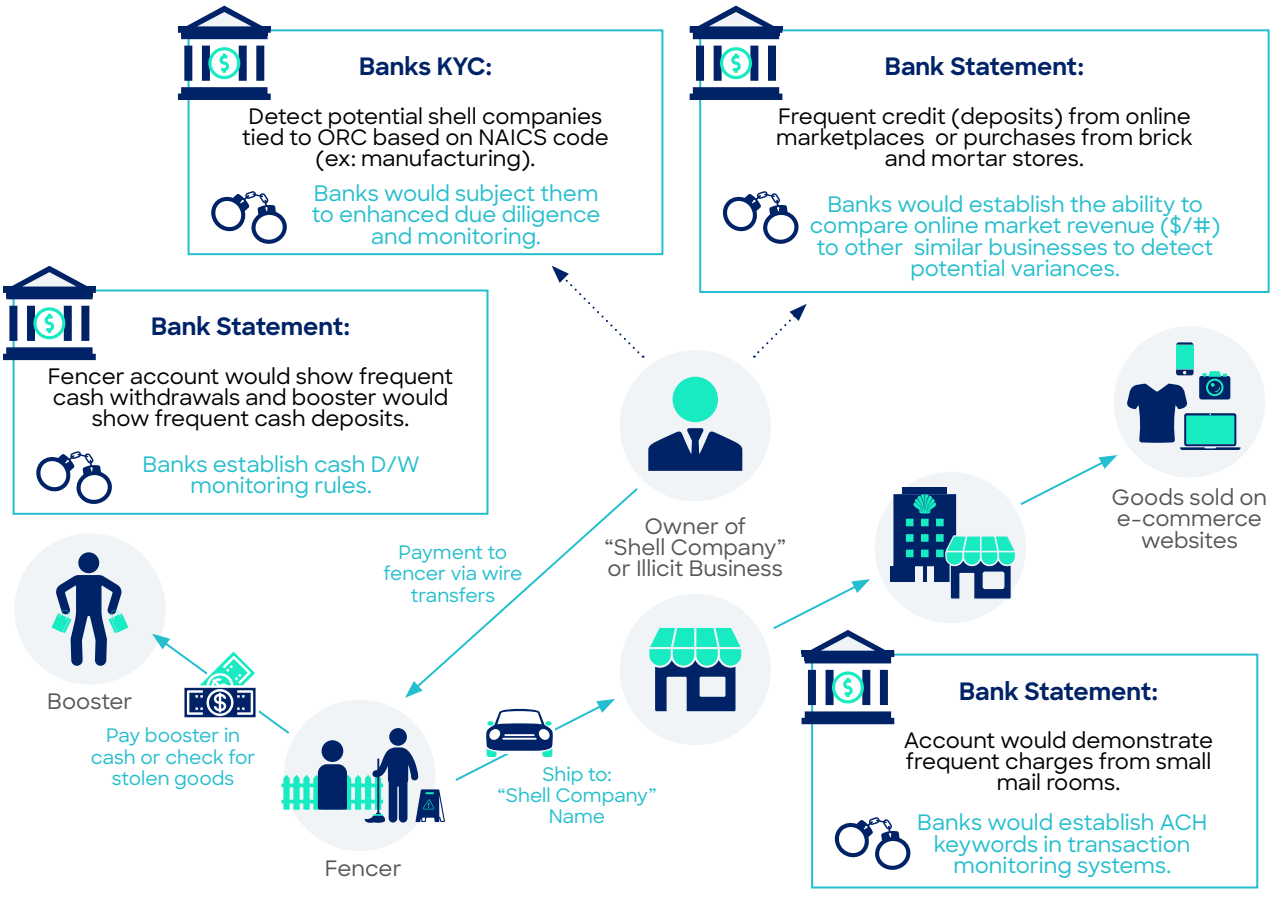
Transaction Monitoring and Red Flag Identification

An effective transaction monitoring system will detect potential money laundering, terrorist financing, and other illicit financial crimes based on the money laundering risks identified within your financial institution.

With billions of stolen retail products sold by OTGs and subsequently sold through online marketplaces, shell warehouses, or co-mingled through an existing business such as a pawn shop or liquidator, it is likely your financial institution has exposure to processing illicit funds tied to OTGs. It is recommended that financial institutions review the red flags identified within this report and evaluate whether their transaction monitoring program would alert them to red flags or typologies tied to ORC and OTG.

Supplementing the red flags and typologies in part two and additional AML program considerations, the below graphic provides a quick reference for where a financial institution investigator may see financial touchpoints related to ORC or OTG activity, and considerations for enhanced monitoring techniques to detect potential related activity. It is recommended, as part of a financial institution's training on ORC, the information in the below figure is considered as well as the red flags and typologies discussed herein.

ORC financial touchpoints



Conclusion

It is tempting for criminal organizations to commit organized retail crime, due to its low cost, high value nature. In the United States, jails are overcrowded, and instances of theft are becoming increasingly decriminalized. Therefore, it can be attractive as a revenue stream for criminal organizations. ORC can be committed to further fund other illicit activity, like drug trafficking or terrorism.

As proceeds from ORC have numerous financial touchpoints, it is important that financial institutions increase awareness around retail crime in order to assist law enforcement investigations. ORC is damaging economically and can also be violent, with many people losing their lives during thefts. Financial institutions and law enforcement investigators can use this guide to increase their awareness of suspicious activity tied to ORC to enhance investigations and increase public-private partnership.

About ACAMS

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS' 60 Chapters globally further amplify the association's mission through training and networking initiatives. Visit **acams.org** for more information.

About Homeland Security Investigations (HSI)

HSI is the principal investigative arm of the U.S. Department of Homeland Security, responsible for investigating transnational crime and threats, specifically those criminal organizations that exploit the global infrastructure through which international trade, travel and finance move. HSI's mission is to investigate, disrupt and dismantle terrorist, transnational and other criminal organizations that threaten or seek to exploit the customs and immigration laws of the United States. HSI has broad legal authority to conduct federal criminal investigations into the illegal cross-border movement of people, goods, money, technology and other contraband throughout the United States. HSI utilizes these authorities to investigate a wide array of transnational crime, including terrorism; national security threats; narcotics smuggling; transnational gang activity; child exploitation; human smuggling and trafficking; illegal exports of controlled technology and weapons; money laundering; financial fraud and scams; labor trafficking and employment crimes; cybercrime; intellectual property theft and trade fraud; identity and benefit fraud; and human rights violations and war crimes. Visit **Homeland Security Investigations | ICE** for more information.

ACAMS | U.S. Immigration and Customs Enforcement

Authors and Contributors

Authors:

- **Lauren Kohr**, Senior Director AML, Americas, ACAMS
- **Tiffany Polyak**, Project Coordinator/Researcher, ACAMS

Thanks to the following key contributors to this guide:

- **Raul Aguilar**, Deputy Assistant Director, Transnational Organized Crime Division, Homeland Security Investigations
- **Thomas Welch**, Financial Crimes Unit Chief, Homeland Security Investigations
- **Robert Skidmore**, Special Agent/Program Manager, Homeland Security Investigations
- **Christopher Cutaia**, Special Agent Homeland Security Investigations
- **Stephen Richardson**, HSI FinCEN Liaison, HSI Financial Crimes Unit
- **Billy Melton**, National Program Manager, HSI Financial Crimes Unit
- **Ben Dugan**, President of the Coalition of Law Enforcement and Retail (C.L.E.A.R.)
- **Lisa LaBruno**, Senior Executive Vice President, Retail Industry Leaders Associations
- **Kevin McMenimen**, ORCAS in ACTION ORC Initiative, Loss Prevention Magazine (LPM)

LPM LOSS PREVENTION MAGAZINE

Coalition of Law Enforcement and Retail CLEAR A National Association

RETAIL INDUSTRY LEADERS ASSOCIATION

Other ORC Resources

Loss Prevention Magazine: **Loss Prevention Magazine - The Authority on Loss Prevention & Asset Protection**

Coalition of Law Enforcement and Retailers (CLEAR): **Home Page**

Retail Industry Leaders Association: **Home Page**

HSI Cornerstone: **Cornerstone | ICE**

Organized Retail Crime Resource Center: **ORC Associations**

2022 ACAMS. All Rights Reserved.
V25052022