Organized Retail Crime

Kevin M. Lally, Jason H. Cowley and Abigail G. Urquhart

March 10, 2022

McGUIREWOODS

www.mcguirewoods.com

What is Organized Retail Crime ("ORC")?

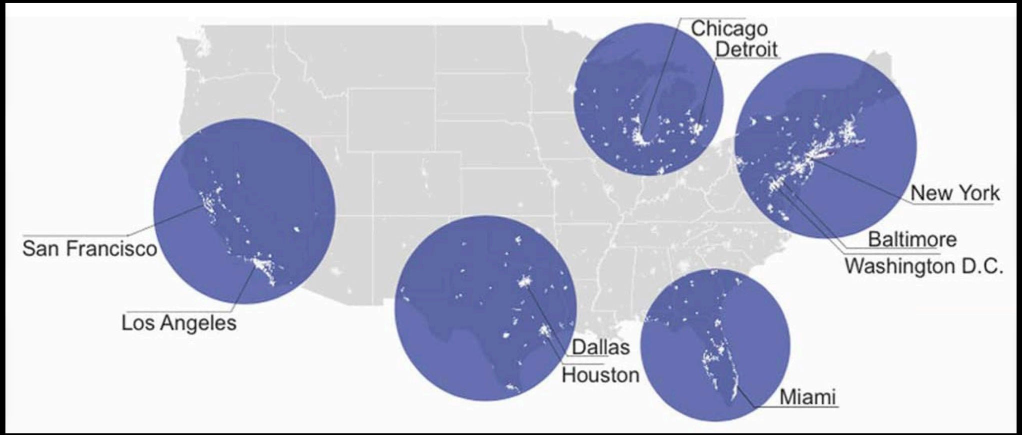
- Organized retail crime is any conspiratorial criminal attack on a retail establishment
  - Involving the association of two or more persons;
  - Engaged in illegally or fraudulently obtaining retail merchandise, tender, confidential data, or customer personal identifiable information for the purpose of converting it into financial gain
- Can operate on a local, regional, national, and/or international scale

Who Conducts ORC?

- Criminal Enterprises (*e.g.*, Mafia), terrorist organizations (*e.g.*, Hezbollah), drug cartels (*e.g.*, Sinaloa), street gangs (*e.g.*, MS 13), and smaller crews (*e.g.*, theft crew)
  - *Example*: Fencing rings suspected of trafficking in millions of dollars in stolen medicine and other retail goods had ties to MS-13
  - *Example*: Proceeds from infant formula theft traced to Hezbollah and Hamas

Examples of Current ORC Schemes

Top ORC Areas in U.S.



Trade Based Money Laundering

Cybersecurity Intrusions

Identity Theft

Merchandise Theft

Return Fraud

Insider Involvement

Consequences of ORC Can Be Dire

Direct Economic Loss

Organized retail crime cost retailers over $100 billion in losses a year

Government Enforcement

Investigations into ORC can give rise to criminal and regulatory investigations and enforcement actions concerning a retailer's internal controls

Reputational Harm

Brand dilution from counterfeit and/or resold goods

Loss of consumer confidence in ability to protect customer's safety and personal identifying information

Legal Liability

Potential criminal exposure

Class actions

Worker's compensation claims

Individual lawsuits filed by customers

Statutes & Legislation Addressing ORC

- California Penal Code § 490.4, organized retail theft occurs when two or more people work together to steal or facilitate the theft of retail merchandise, either in a physical store or online

- North Carolina Gen Stat § 14-86.6, penalizes organized retail theft as a Class H felony

- Retailers are urging Congress to take action to address the online sale of stolen and counterfeit consumer products by passing the Integrity, Notification and Fairness in Online Retail Marketplaces for Consumers Act

ORC Schemes

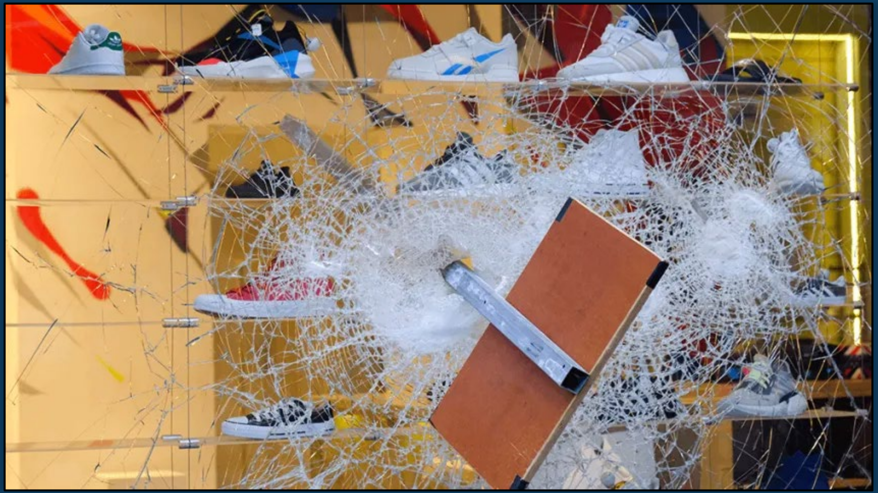
McGUIREWOODS

www.mcguirewoods.com

Smash & Grab

JCPenney
OW AT 11PM
IOLENT SMASH AND GRAB INSIDE A MALL
YEWITNESS NEWS
abc7
#abc7eyewit

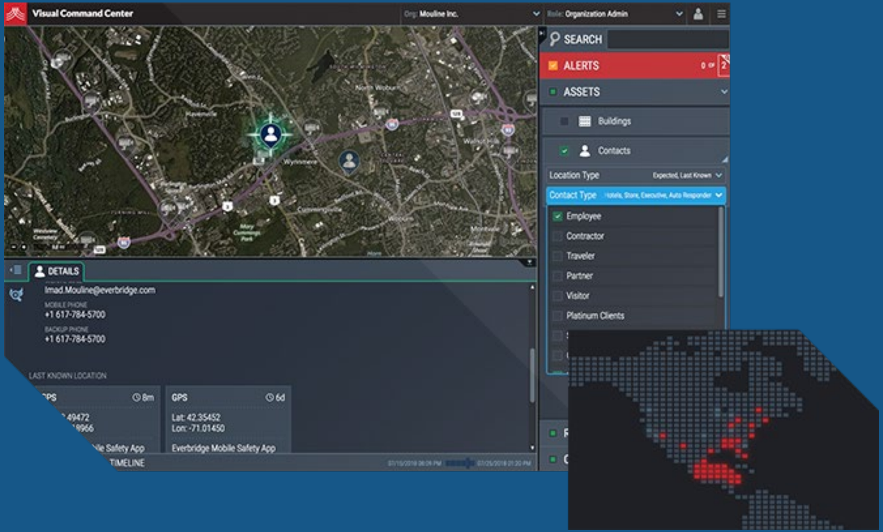
Smash & Grab



- Typically conducted by robbery crews
- Historically high risk, low reward
- CVS's director of organized retail crime and corporate investigations testified before Congress that it reports an ORC-related offense every three minutes, at an average of $2000 worth of goods stolen
- An emerging trend has involved groups of previously unconnected individuals who organized on social media

Smash & Grab – Prevention

- **Use of Technology**
  - Radio-frequency identification data (RFID) chips
  - Facial recognition technology denying entry to those attempting to conceal identities
  - Everbridge technology to monitor for high-risk times
- **Staff Training**
  - Violence non-escalation and de-escalation strategies



Location Type: Expected, Last Known

Contact Type: Hotels, Store, Executive, Auto Responder

☑ Employee
□ Contractor
□ Traveler
□ Partner
□ Visitor
□ Platinum Clients

Imad.Mouline@everbridge.com

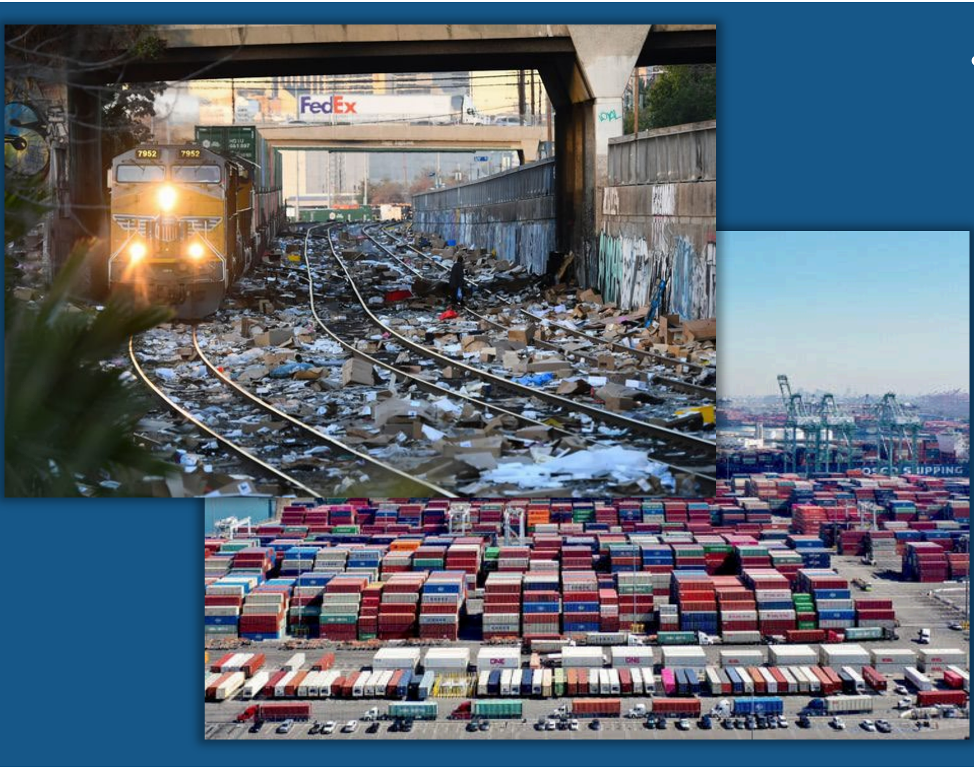
MOBILE PHONE
+1 617-784-5700

BACKUP PHONE
+1 617-784-5700

GPS 8m
49472
9966
Safety App

GPS 6d
Lat: 42.35452
Lon: -71.01450
Everbridge Mobile Safety App

Supply Chain Theft



- Thefts targeting trains, commercial vessels, trucks, and warehouses
  - U.S. Cargo thefts increased 23 percent in 2020
  - Average value of thefts in 2020 increased by 41 percent
  - Union Pacific railroad stated thefts targeting its trains are up 160% over the past year in Los Angeles County, with an average of 90 containers broken into every day over the last three months

Supply Chain Theft – Mitigation

- **Beware of Insiders**
  - 70 percent of supply chain and cargo theft is associated with insider involvement, whether intentional or accidental
  - Conduct background checks; limit information sharing; establish robust internal controls to facilitate reporting; and engender employee loyalty
- **Ensure Integrity of Full Supply Chain**
  - Know Your Business – conduct comprehensive vendor background checks
  - Enter into service level agreements with vendors laying out responsibilities for controls and responses to potential attacks
- **Technology and Security Plans**
  - Drones, specialized fencing, and trespass-detection systems
  - Trace and track technology that can identify product by SKU number

Trade Based Money Laundering ("TBML")

- Involves the exploitation of trade transactions to transfer value and obscure the origins of illicit funds

- Accounts for laundering of hundreds of billions of dollars of illicit funds annually

- Schemes generally use illicit proceeds to purchase goods, but can also involve misrepresentations of the price, quantity, or type of goods in trade transactions

TBML – Black Market Peso Exchange

TBML – Mitigation

- **Anti-Money Laundering**
  - Create control systems that monitor
    - Bulk cash payments
    - Over, under, and multiple-invoicing
    - Over and under shipment
- **Know Your Business/Know Your Customer**
  - Implement third-party due diligence policies, screening, and processes, including researching product range and pricing
  - Understand when to employ enhanced due diligence procedures

Credit Card Skimming

- “Skimmers” allow criminals to steal credit card information in two ways:
  - *Physical Skimming:* Installing a universal key into a credit-swiping machine to steal information from unwitting customers
  - *Digital Skimming*: Embedding malicious code on vulnerable e-commerce websites
- One major U.S. retailer confirmed that data from approximately 40 million credit and debit cards was stolen at its stores in less than one month using credit card skimmers

Credit Card Skimmers – Mitigation

- **Physical Skimmers**
  - Employee training
  - Adopt EMV Chip Scanners
- **Digital Skimmers**
  - Utilize software to prevent digital credit card skimming
    - *Example:* Target's software Merry-Maker is open-source
  - Decrease the company's exposure to customer credit card information
    - *Example:* Use known payment systems, such as PayPal, rather than accepting payment directly through website
- **Immediately Report Potential Skimming**
  - Law firms can help navigate legal reporting requirements. Immediate reporting facilitates investigation and helps protect company from lawsuits

Cyberthreats

- In 2020, 24% of cyberattacks targeted retailers, more than any other industry
- The average cost of a data breach in retail in 2021 is $3.27 million
- 16% of UK retailers said they had experienced a cyber-attack or an attempted attack every day according to recent research from Zynstra

Common Cyberthreats Impacting Retail

Attacks on IOT devices, payment systems and machine learning systems

Ransomware

Data Breaches

Phishing

Insider Attacks

Refund Fraud

Website App Attaches

Stealing business information during trade negotiations with foreign governments

Cyber Threats - Legislation

Federal

- The U.S. Senate approved new cybersecurity legislation that will require critical infrastructure organizations to report cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and ransomware payments within 24 hours
- SEC requires public companies to disclose cyber incidents and are considering revisions to make controls more robust and reports more immediate and fulsome
- There are sector-specific requirements, like HIPAA in healthcare

State

- All 50 states have a breach notification statutes that require reporting of incidents to the authorities, most of which require notifications to regulators
- All 50 states also have breach notification statutes that requires reporting incidents to individuals
  - *Example*, North Carolina's Data Breach Notification Statute, N.C.G.S.A. § 75-61, requires notifications be made "without unreasonable delay"

Solutions

Coordinate with Law Enforcement and National Retailers
Establish strong relationships with law enforcement and build up cases to make referrals

Develop Strong Internal Controls
Internal controls should be aimed at limiting the number and severity of offenses; exposure to liability; and ensuring meeting state and federal reporting requirements

Lobbying
Advocate as an industry for more targeted and punitive legislation at the state and federal level

Questions or Comments?

www.mcguirewoods.com