Protect Your Business from Organized Retail Crime with the Power of AI

From Data to Defense: How OSINT Tools are Transforming Retail Loss Prevention

BABELSTREET

Introduction

What do you picture when you hear the phrase “retail theft?” For decades before the digital revolution, you probably would have imagined a teen at a local drug store, nervously slipping a $4 lip gloss into her purse. Or maybe a savvier criminal working on a rainy day, sweeping pricey electronics into the folds of an unlatched umbrella hanging from his arm.

Today’s reality is different. Large, tightly organized crime rings engage in widescale retail theft. Hackers, fraudsters, boosters, resellers, fences, and others work in tandem to rip off retailers. These gangs often operate as part of larger transnational criminal organizations, and their activities engender more serious crimes. Human beings are sometimes trafficked to take part in organized retail theft (ORT) rings. And proceeds obtained from purloined goods can fund the purchase and distribution of illegal drugs or finance terrorist operations.

Appriss Retail notes that “claims and appeasement fraud” — actions that exploit stores’ return-and-replacement policies — is one of the fastest growing areas of retail fraud.[1] According to the National Retail Federation, in 2023 this crime cost retailers between $21 billion and $35 billion.[2] Appeasement fraud increases online retailers’ costs, erodes their profit margins, and damages their brand reputations. Ubiquitous loss-prevention methods — address verification, credit-card verification, multi-factor identification, gift-card value checks, and order tracking among them — fail to keep pace with evolving fraud tactics.

This e-book discusses how open-source intelligence (OSINT) — or intelligence gleaned from processing and analyzing publicly available and commercially available information (PAI/CAI) — can help retail security managers, loss prevention directors, fraud investigators, and others spot and stop ORT. OSINT capabilities work for both retailers running their own ecommerce sites, and for those relying on third-party retail platforms such as Shopify or WooCommerce.

Common types of retail fraud

In addition to appeasement fraud, organized rings commit many types of retail theft. These include:

- Group attacks on brick-and-mortar stores
- Return of stolen items to physical stores. ORT rings use faked receipts to obtain cash refunds or store credit
- Gift card fraud. Organized rings steal value from gift cards, both online and in stores
- Coupon fraud. Some scammers hack corporate systems to gain access to coupon codes, stealing them or manipulating them so they have a much higher value than originally intended

The appeasement fraud challenge

Easy returns and fast replacements are significant aspects of the seamless shopping experience online retailers strive for. When a customer can't walk into a bricks-and-mortar perfumery to test cologne, retailers must make returns easy if the customer finds she dislikes the scent. They must provide a speedy replacement if the perfume bottle breaks in transit. Otherwise, the retailer risks losing a valuable customer.

Scammers know this and employ a variety of fraud types to exploit retailers' willingness to return or replace items that the customer doesn't like, that don't work, that are damaged in transit, or that are never received. These scams include:

- **Bracketing** - Fraudsters buy multiples of the same item, keep a few, and return the rest for a full refund. They bet the retailer won't notice if only 37 of the 40 gold chains purchased are returned.
- **False ID Tracking** - A member of an ORT ring requests a return shipping label from a retailer. He then sticks the label on a box or envelope, without including the item to be returned. Upon receiving the package, the retailer scans the barcode and marks the items as "returned" even though the purchased product is not contained inside.
- **Partially empty box fraud** - Fraudsters order two or more items set to arrive in the same box. One item is very pricey, the other cheap. They then claim that the high-value item was not in the box received.
- **False claims of non-delivery** - Scammers claim they never received items they actually did. The retailer either issues a refund or replaces the item.
- **Refund-as-a-service fraud** - Cybercriminals commit fraud on behalf of everyday consumers. These fraudsters promote their services online — both on social media and on dark web marketplaces. Do you want a refund for an expensive television without having to return the TV? Work with professional fraudsters. They will contact the company on your behalf with fake claims of non-delivery or fake damage reports. They may phone the retailer to manipulate customer service reps into believing that items are too costly or inconvenient to return. Scammers make their money by charging consumers a fee for this service. Research from Netacea[3] suggests that there are more than 1,600 ads for fraudulent-refund services running on social media forums.

Underpinning many instances of appeasement fraud are account takeovers. In this type of scam, fraudsters use stolen passwords, usernames, or other credentials to obtain ownership of consumer accounts. These credentials are typically gleaned from the dark-web sale of information obtained through data breaches, including the high-profile breaches that have affected consumers at Home Depot, Target, Neiman Marcus, eBay, and CVS.[4] Despite retailers' significant efforts to implement stronger identity protection measures, Appriss estimates that fully 80 percent of all retail attacks are account-takeover attacks.[5]

How do account takeovers contribute to appeasement fraud? The scammer who bought 40 gold necklaces and only returned 37 of them may have used another person's credentials to do so. The same can be said for the fraudster who received a TV he later falsely claimed was never delivered.

While this e-book has concentrated on claims and appeasement fraud in the digital arena, it is important to note that these crimes can also take place in bricks-and-mortar stores. Criminals may steal items only to later return them using a fake receipt to obtain a cash refund or return stolen items without a receipt for store credit. Additional tactics include removing an expensive item from a box, filling the box with worthless items of approximately the same weight, resealing and returning the box, and claiming a refund.

Whether stolen from e-commerce sites or physical stores, purloined goods are often resold in online marketplaces as well as on other popular social media sites and dark-web marketplaces. The largest ORT rings may also sell to other organized criminal enterprises to handle resale, often internationally.

OSINT helps curb ORT rings, improve customer service

Retailers are well aware of organized retail theft. They have instituted stricter return measures to try to stem the fraud. The National Retail Federation reports that in 2022, retailers accepted roughly 22% of all returns without requiring a receipt. That percentage was halved in 2023.[6] But there's a problem with this approach. Too often, legitimate customers are caught in the anti-theft net. One-size-fits-all policies that limit the flexibility of online returns, restrict the window for returning a product, cap the number of missing orders that will be replaced, or that substitute store credits for cash refunds all risk alienating consumers.

OSINT solutions can help retailers balance competing needs, stopping fraud while better serving valuable customers.

How?

- By examining and analyzing huge amounts of PAI and CAI, OSINT solutions can give retail fraud specialists a comprehensive view of the global fraud landscape. This empowers them to understand, anticipate, and even combat emerging ORT trends.
- By using AI to detect patterns and anomalies, OSINT solutions can help fraud specialists spot suspicious activity that may indicate distinct instances of fraud.
- AI further helps fraud specialists identify members of ORT rings by uncovering hidden connections among seemingly unrelated individuals and transactions.

In doing all this, OSINT solutions can provide retailers with the information they need to develop policies that stop organized retail theft rings while continuing to provide a positive experience for valuable customers.

Why Babel Street?

The Babel Street AI-powered Ecosystem delivers advanced data and analytics solutions that transform diverse data sources into actionable insights. The Babel Street Insights OSINT solution provides persistent searches of thousands of sources of PAI and CAI. To provide retail security professionals with insights needed to stem ORT, our technology scours data sources published in more than 200 languages and translates results into the user's language of choice. Information sources include more than a billion top-level domains; commercially available sources; and real-world interactions generated on chats, social media posts, online comments, and message boards.

Insights further enhances security through searches of the deep and dark web — or web sites that are inaccessible by standard search engines. Because the nature of the tools used to access the dark web ensure anonymity, it is a hotbed of illegal activity — including communications among members of ORT rings. Dark web search capabilities enable investigators to scan posts and other information they wouldn't otherwise be able to see.

With Babel Street Insights document search capabilities, retailers can learn about current and emerging ORT trends arising in different parts of the world. Tailored search capabilities empower retailers to search by region, fraud type, overall trends, distinct publications and sites, and other parameters.

The social media monitoring capabilities of Babel Street Insights allow retail theft professionals to scour the internet for ORT communications. Sites examined include known ORT chat channels such as Telegram (where OT rings often share strategies, tips, and targets) and Reddit, other top-level social media sites, and dark web forums and marketplaces. As retailers seek to improve return policies, they can also monitor these sites for discussion on whether new policies deter ORT rings, or if criminals have found loopholes for bypassing them.

Piercing criminal networks — understanding who is connected to whom, and which organization is targeting which retailers — is an important part of combatting ORT. Babel Street's AI-powered

relationship-mapping capabilities examine thousands of associations within a specific social network or dark-web discussion group, uncovering previously unknown or hidden connections, and identifying those participants who wield the most influence. (Visualizations of these relationships are also provided.) Once influencers are identified, Babel Street enables users to delve deeper into those influencers' online profiles, activities, and associates. This process can help connect online aliases to real-life individuals. Retailers can then share this information with the FBI's Uniform Crime Reporting program, and other law enforcement agencies.

Address-match capabilities provide further insight. Imagine that a retailer has determined strong connections between Harry Jones, John Smith, and Tom Anders. Using Babel Street to delve deeper into their identities, the retail analyst learns that their residences are 123 Main Street, #103; 123 Main St., Apt. 103, and 123 Main St. Applying Babel Street's address match capabilities to their own databases, retailers quickly learn that these three potential fraudsters share an address — and that a suspiciously high number of "replacements for non-delivery" have been requested from that apartment. The retailer may choose to stop sending items to this particular address.

Finally, using insight from Babel Street OSINT solutions, retailers can move beyond rules-based return-and-replacement policies to a more personalized approach. The process starts with knowing each customer better. AI capabilities improve identity verification by linking all customer information on file — including names, addresses and phone numbers; loyalty card information; and credit card information. Retailers can then sort customers into different tiers based on shopping profiles, and historical purchasing and return behaviors. The retailer may choose to implement different return policies for each consumer tier.

ORT rings are constantly finding new ways to exploit retailers' customer appeasement efforts. Babel Street's AI-powered OSINT solutions empower businesses to proactively identify and mitigate retail threat risks, protect their assets, and improve the retail experience for valued customers.

Endnotes

[1] Appriss Retail, "Appriss Retail 2024 Claims and Appeasements Report," May 2024, https://apprissretail.com/resources/2024-claims-and-appeasements-report/

[2] National Retail Federation and Appriss Retail, "2023 Consumer Returns in the Retail Industry," December 2023, https://nrf.com/research/2023-consumer-returns-retail-industry

[3] Netacea, "Threat Report: Refund Fraud-as-a-Service," September 2022, https://netacea.com/reports/threat-report-refund-fraud-as-a-service/

[4] Artic Wolf, "10 Major Retail Industry Cyber Attacks," June 2023, https://arcticwolf.com/resources/blog/10-major-retail-industry-cyber-attacks/

[5] Akrose Labs, "Q2 2022 State of Fraud and Account Security," 2022, https://www.arkoselabs.com/resource/2022-q2-state-of-fraud-account-security-report/

[6] National Retail Federation and Appriss Retail, "2023 Consumer Returns in the Retail Industry," December 2023, https://nrf.com/research/2023-consumer-returns-retail-industry

Babel Street is the trusted technology partner for the world's most advanced identity intelligence and risk operations. The Babel Street Insights platform delivers advanced AI and data analytics solutions to close the Risk-Confidence Gap.

Babel Street provides unmatched, analysis-ready data regardless of language, proactive risk identification, 360-degree insights, high-speed automation, and seamless integration into existing systems. We empower government and commercial organizations to transform high-stakes identity and risk operations into a strategic advantage.

Learn more at babelstreet.com

All names, companies, and incidents portrayed in this document are fictitious. No identification with actual persons (living or deceased), places, companies, and products are intended or should be inferred.

BABELSTREET