How to Run Effective Retail Loss Prevention Investigations

Retail loss prevention is a top priority, with the average shrink rate representing $94.5 billion in losses across the industry. To combat rising rates of organized retail crime, insider theft, fraud, and associated violence and hostility, security teams need the right tools and processes in place to recognize early warning signs, take remedial action, streamline investigations, and benchmark loss and recovery performance over time.

**Leverage the following checklist to ensure you have a comprehensive investigative process in place.**

Pre-Incident

Establish systems and processes

Ensure loss prevention teams have the right tools in place to proactively monitor assets and establish processes to mitigate risks, reduce response times, and create standardization in an investigation workflow across the team.

Define assets for protection Employees, store product, inventory in the supply chain, customers, corporate equipment	
Consolidate connected systems data Vehicle, video surveillance, access control, CRM, HR records, historical case records	
Centralize processes and systems, including research and monitoring tools Criminal, civil records, OSINT, social media, dark web, local news reports	
Set up incident reporting and triage processes Tip lines, online portals, reported incidents (from the field)	
Standardize templates for common incidents to streamline intake and investigations Templates for missing inventory, car burglary, theft of product from supply chain, suspicious person or vehicle	
Set up notification flows based on incident type or severity Corporate security, store or mall guards, legal, HR, IT, PR, police or EHS	
Clarify who has authority to close a report	
Select conditions for report closure Loss recovered, all leads exhausted, referred to police, threat mitigated, unresolved	
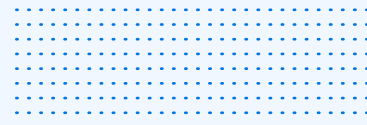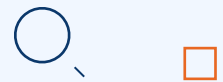
Monitor and identify potential threats

By establishing situational awareness based on systems and tools, teams can monitor data for pre-incident indicators that increase the risk of theft or loss.

Monitor unusual alerts from connected systems License plate recognition, access controls, social mentions/threats, visitor management check-ins	
Monitor connected systems for sources of threatening or concerning behavior Localized crime trends, ORC patterns, HR reports, updates to other or historical cases that trigger a pattern alert	
Monitor alerts from adjacent systems Intrusion detection, endpoint protection, cyber threat intelligence, fraud detection	
Identify pre-operational indicators of theft Complaints, external or internal tip lines, direct employee or guard observation, connected system alerts, casing/surveillance	
Connect/coordinate with local police about any identified trends or concerns to ensure a coordinated action plan if an incident occurs	
Take remedial actions to mitigate threat before loss occurs or if connected with threats to safety Escalate to HR, issue be on the lookout (BOLO) to store or mall guards, increase surveillance	

Incident Intake and Investigation

Capture and prioritize the incident

With the aid of the established systems and processes, teams can quickly capture the loss and notify appropriate stakeholders for further investigation, as needed.

Capture the basic who, what, when, and where details How was the loss identified, what is missing, when and where did it happen	
Obtain photographs or videos of the location (if relevant)	
Set incident priority based on inventory value or a connection with violence Low priority incidents may be closed without further investigation	
Coordinate with local police (if deemed appropriate) Record police response, if any police incident number, intelligence learned	
Assign lead investigator and initiate investigation workflow	

Action investigation steps

Leveraging a consolidated platform for documentation, investigation and collaboration, teams can accelerate detailed investigations to scope, document, and resolve the incident.

Collect relevant information from individuals to understand the incident, the timeline in which it occurred, and what parts of the business were disrupted Interview the person who reported the incident, the victim(s), manager of the affected area (e.g. manufacturing, headquarters, off-site)	
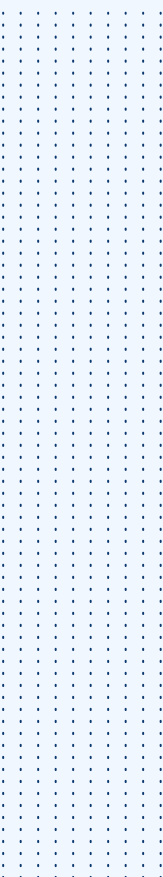
Collect supporting evidence to identify a person of interest, examine their history and track down lost goods Research public records, social media, dark web, third-party surveillance footage (e.g. mall security)	
Analyze previously documented incidents and investigations to determine if there are any connections or related incidents	
Access and review crime data in incident database to determine patterns, metrics, and trends Review all data from recent years, or past 30-90 days of data at minimum	
Expand notifications as needed Mall security, media relations	
Log follow up requirements and communications Each dispatch, assignment, activity, piece of evidence, or communication between individuals, across functions, or with external third parties	
Clarify recovery process (who recovers) and cost recovery (if relevant)	
Take any appropriate actions, both immediate and post-investigation, to contain or mitigate the threat Increase security patrols, add lighting or additional locks, hold security awareness briefings, increase physical surveillance or camera surveillance	
Regularly review case disposition status (open, closed, ongoing)	

Post-Incident

Analyze data, metrics and trends

Teams with robust metrics and dashboards can analyze incident trends and data to inform preparation and response activities, preserve knowledge, and evolve investigation best practices.

Track investigation data across a wide variety of variables Case disposition status, case resolution rate, incident type, personnel, location, loss and recovery rates	
Build custom reports against any collected data field or emerging threat signal to gain investigation insights	
Define document retention period to ensure you're legally compliant and to guard against re-emergence of issues	

Prevent theft and improve security operations with Ontic

Ontic's Incidents, Investigations and Case Management solution is the only software integrated with an end-to-end threat management platform to capture pre-incident indicators and alerts from any source to help security teams act on high-risk signals before they turn into costly losses.

Learn More