Mitigating Recurrent Shoplifting through Crowd Intelligence System

The implementation of VALOORES Crowd Intelligence System at CVS Health has proven to be effective in mitigating recurrent shoplifting incidents. By leveraging geospatial data, CDR data, and CCTV footage, the system provides actionable insights that enable a proactive security response. The success of this solution demonstrates the potential of advanced technologies in enhancing retail security and ensuring a safer shopping environment.

Through big data analysis, map visualization, co-traveler analysis, and facial recognition, VCIS aids in swiftly detecting theft and fraud, offering a comprehensive solution to evolving security challenges in the retail landscape.

Table of Contents

Consequences of Retail Shoplifting

- Financial Losses for Retailers: Shoplifting results in substantial financial losses for retailers, which are often passed on to consumers in the form of higher prices. Smaller businesses may even be forced to close due to the impact of theft.
- Increased Prices for Consumers: Retailers often offset their losses by raising prices on their products, which affects all consumers. In essence, everyone pays a hidden "shoplifting tax" when they shop.
- Negative Impact on Employees: Retail employees are directly affected by shoplifting. They may face increased workloads due to inventory shrinkage and may be subjected to additional security measures, making their jobs more stressful.
- Legal Consequences: Shoplifters, when caught, face legal consequences such as fines, probation, community service, or even imprisonment. These penalties can have a lasting impact on their lives.
- Societal Costs: Shoplifting contributes to the erosion of trust in society and can lead to a sense of insecurity within communities. It also diverts law enforcement resources away from more serious crimes.

VCIS Confronting the challenges

With VCIS geospatial intelligence and advanced analytics, it is now possible to identify criminals and their patterns before, during, and after they commit crimes. In the current retail landscape, disruption is the name of the game. As the industry adapts to this new reality, we collaborate closely with retailers to confront these challenges head-on.

Big Data from Small Devices

In one example using mobile phone locations, multiple consumer patterns can be uncovered quickly when examining the typical retail location to identify possible criminal behavior. Consider how often a consumer might visit more than one big-box retailer on the same day when shopping. It may be expected that they needed help finding an item at store #1 and drove to store #2 in search of a product. Another consumer may be an auditor at a big-box retailer and visit multiple stores daily. And now we have many cases of workers for companies like Instacart and Uber who pick up numerous items each day from multiple retailers. Unlike single shoplifters or even regular customers, boosters travel from retailer to retailer, sometimes hitting multiple stores in multiple cities daily.

Some geospatial intelligence vendors have analyzed these patterns millions of times and identified anomalies that have now been converted into algorithms that can uncover these patterns in seconds, highlighting the suspicious travel patterns indicative of boosting. Subsequent geospatial data can analyze multiple booster travel patterns and look for common relationships between devices. Quickly, unknown fences, shipping companies, and other suspicious locations are identified for further investigations. Even basic searches, often called “behavioral patterns,” can show investigators where a device has traveled dating back years.

Map Visualization

VCIS queries and map visualization, primarily when used at the point of sale, has proven valuable in the detection of theft and fraud. Programmers and investigators have worked together to identify transactions or performance metrics that raise red flags, also known as anomalies. A typical example of an exception report is an employee using the void transaction button statistically more than others, indicating that merchandise is possibly being stolen at the POS. Other exception reports can be much more complex and discover many areas of theft and fraud in a company.

Co-traveler Analysis

VCIS utilizes a spatial-temporal analysis search to verify when two or more people have been together anywhere in the world. A simple-to-understand model would be instantly knowing if employees from company A ever had lunch, private meetings, or inappropriate relationships with any employee from competitor company B in the past few years. These patterns can also apply to boosters meeting up with partners and fences, conflicts of interest, intellectual property theft, and other types of crime involving sex trafficking, cartels, and organized crime activity. The use cases for geospatial intelligence are unlimited.

Facial Recognition through CCTV

Facial Recognition technology has a vast database of documented shoplifters, organized retail crime associates, disgruntled ex-employees and other individuals that pose a risk. The shoplifters, if entering a store, can be traced from video footage or following an apprehension. As soon as the shoplifter returns to the store, the camera enabled with face recognition algorithm can match that individual's face against the database of images on file. When the system recognises any potential match, the store security professionals can be alerted instantly. The technology therefore allows to observe the suspected individuals and reduce the number of shoplifting instances.

In case any individual successfully gets away with committing a crime, face recognition can add tremendous value. An image of the retail criminal can be taken from store CCTV and enrolled in the system. You might not have a clue who the person is, but your security team will know the moment they return to a store.

Case Study

Elements

Retailer: CVS Health
Store Locations: AOI Library
Timeline: Over the past month
Product Targeted: Shampoo, Powder Milk,…

Story

CVS Health, a prominent retail giant in the United States, is currently grappling with a notable uptick in shoplifting occurrences across numerous branches. This surge in incidents, which has been observed repeatedly over the past month, has ignited a growing apprehension regarding the efficacy of the store's existing security measures. The frequency and consistency of these thefts underscore a pressing need for a proactive and comprehensive solution to safeguard the store's assets and maintain a secure shopping environment for both customers and employees alike.

As CVS Health navigates this challenge, it faces the imperative of reassessing and potentially enhancing its security protocols to address the evolving dynamics of theft within its retail spaces.

Challenges

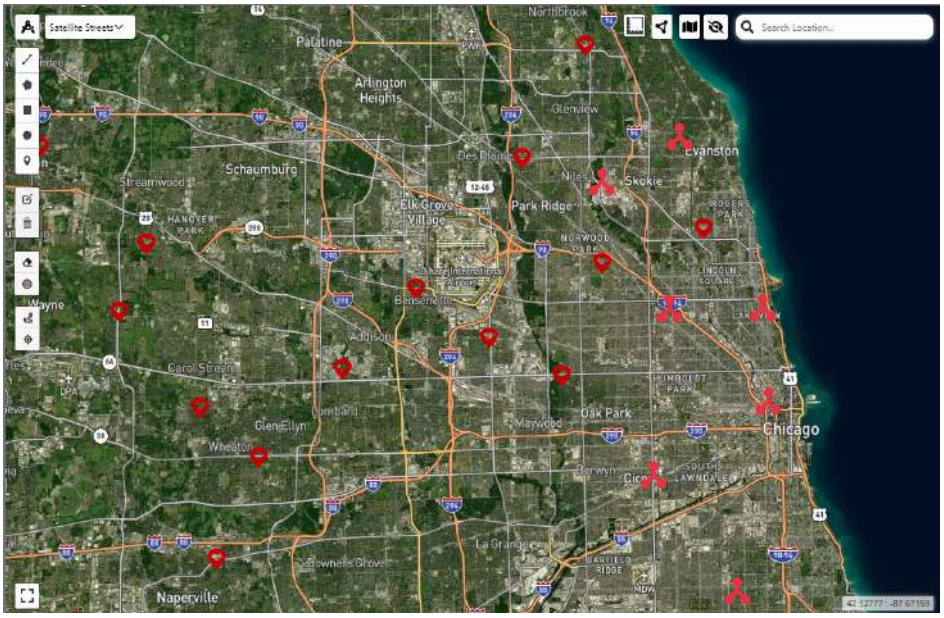
Recurrent Incidents: Shoplifting incidents have been consistently occurring, affecting the store's profitability and reputation.
Complex Environment: The store's size and complexity make traditional security measures challenging to implement effectively.
Diverse Shoplifting Techniques: Culprits employ various techniques, including distraction, concealment, and quick exit strategies, making it difficult to apprehend them.

Scenario

AOIs

First of all, we have saved all CVS Health branches where shoplifting incidents occurred as Areas of Interest on our map, aiming to enhance visualization and accessibility. This comprehensive mapping provides a clear visual representation on the map where users can navigate and access these specific branches, thereby streamlining their interaction with other locations or competitors.

We took CVS Branch located at 4801 N Central Ave, Chicago, IL 60630, USA as a sample to execute this investigation. *(Screenshot below)*



List of Employees

To compile a list of devices associated with CVS Health employees, we executed different "device travel pattern" **DTP** queries, each one between the home address of an employee (during the night) and the CVS Heath branch (during working hours). By executing this query, we discern the device IDs linked to each employee which allows for the identification and tracking of devices associated with CVS Health employees, providing valuable insights for various purposes in the following steps of this case study. *(DTP Worker 1/2/3/4/5/6/7/8/9/10)* The compiled list of device IDs is the following:

Worker 1: 931c33a9-09c4-4b52-978c-9fa1874ff0c7

Worker 2: c63aacaf-cc84-4b6d-8129-d87a80c9e6b5

Worker 3: daf71301-64bd-4119-85ae-7f4fee4f7e3f

Worker 4: cdd19025-b33b-4321-8287-2ba12a102c98

Worker 5: db45a6f0-1250-4064-955d-0c09db6f5347

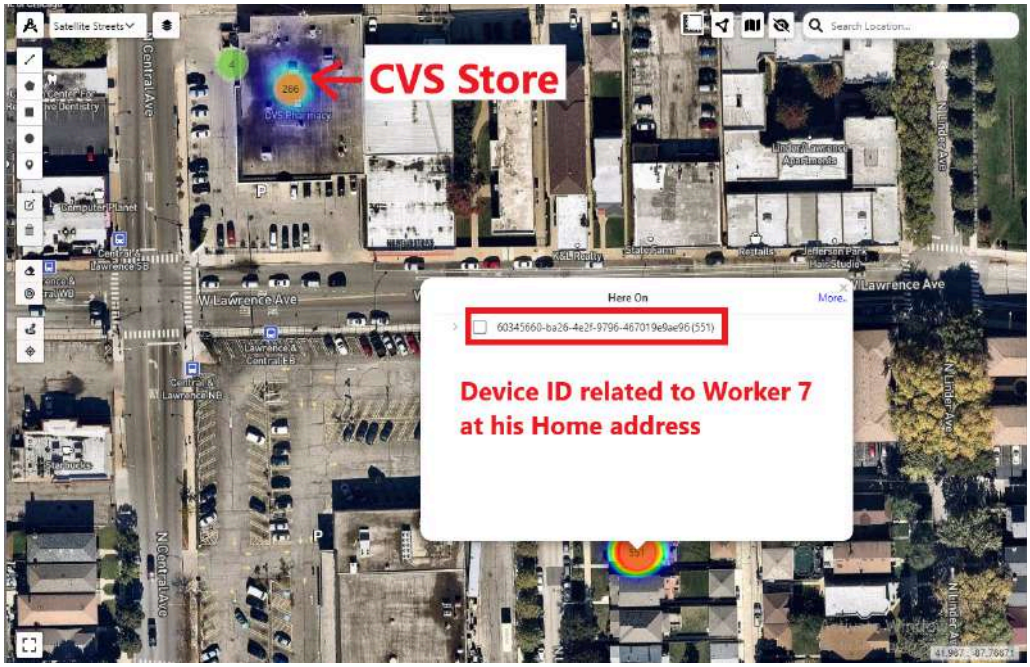
Worker 6: 85a59dda-c857-48e3-8c31-b43b7c96b6cf

Worker 7: 60345660-ba26-4e2f-9796-467019e9ae96

Worker 8: 487aa6cd-a8e9-4545-9a39-dada1773f6b6

Worker 9: bcd7b60e-e6d5-4937-b274-257b31fa97cf

Worker 10: 447f6695-e3e6-416e-b204-bed8b5958de8



Inventory

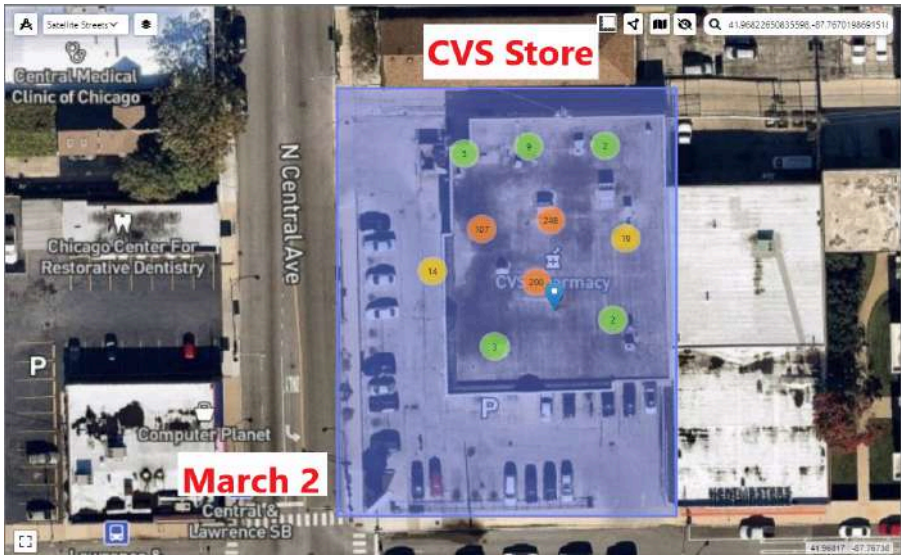
Maintaining an inventory list that details every product type and the corresponding days of the month when shoplifting incidents occurred. This detailed inventory serves as a valuable reference point, allowing for a later comparison with the list of connected devices present on those specific days. By analyzing these patterns, we can establish meaningful connections between the inventory list and the devices associated with shoplifting incidents. This integrated analysis provides a comprehensive view, helping to identify potential correlations, and understand the modus operandi of shoplifters.

Invetory List

	Paul Mitchell Extra Body Foam	Paul Mitchell Hair Repair	Paul Mitchell Shampoo	Paul Mitchell Sculpting Lotion	Pampers Baby Dry Diapers Size 3	Huggies Ultratrim Size 5 Unisex Diapers	Avent Newborn Nipples	CVS Anti-bacterial Washcloths	Jose Cuervo Especial Gold Tequila	Dewers Scotch
March 1	1						2			1
March 2		2				1		1		
March 3		1	1						1	
March 4										
March 5	2						3			1
March 6			2					1		
March 7					1					
March 8			2			1			1	
March 9				1	1					
March 10										
March 11								2	1	
March 12										
March 13	1			1						1
March 14	4						1			
March 15		1				1				
March 16					1				1	
March 17										
March 18										
March 19										
March 20						1				1
March 21				3						
March 22			1					1		
March 23							4			1

Activity Scan per Day

At the selected CVS Health branch, we executed an activity scan **AS** query for each day of the month during operational hours. This query aimed to detect crowd activity and density, capturing the device IDs of all individuals present at the store on each day of the month. These queries, labeled as D1, D2, D3, and so forth, were saved. The intention is to later compare this data with the Inventory list, documenting each product type and the days on which shoplifting occurred. By correlating these datasets, we aim to pinpoint potential connections between the devices present and the days when specific products were shoplifted. This strategic approach allows for a nuanced analysis, facilitating the identification of patterns and contributing to the development of targeted security measures at CVS Health branches.



Knowledge Graph

1. Stolen Item

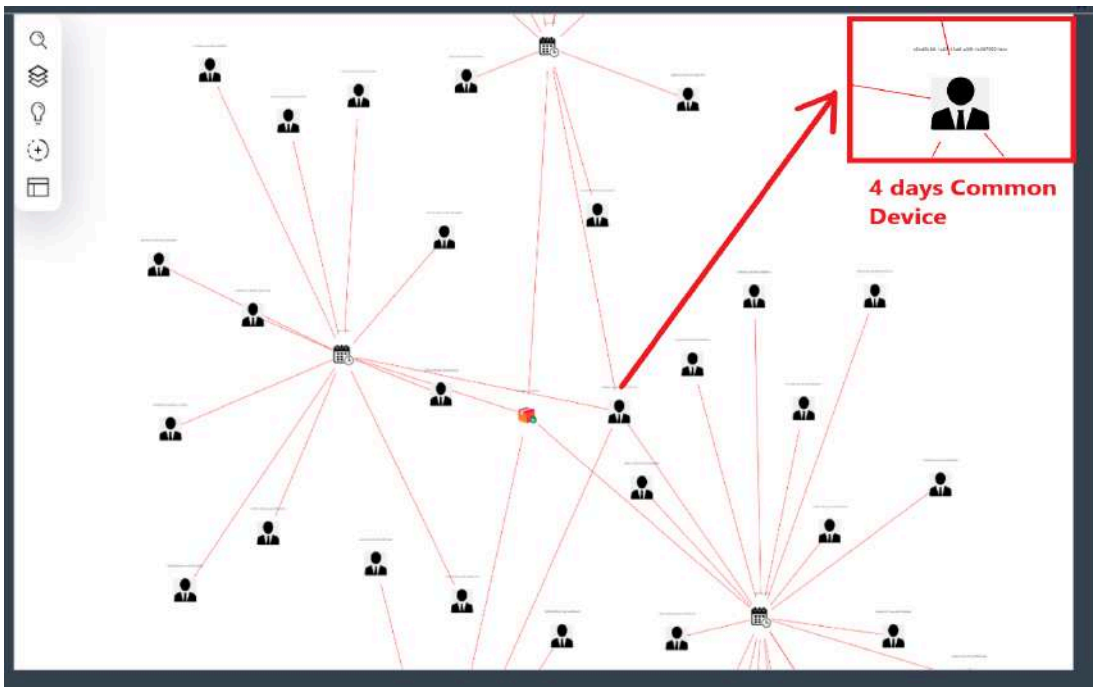
The saved AS queries are integrated into the knowledge graph to illuminate the common devices present on days when shoplifting incidents occurred for specific products. This integration enables a visual mapping of device intersections, providing a clear depiction of shared occurrences across the selected days and investigating devices with higher connections.

Central Node: The primary focus of the knowledge graph is a central node, which represents the stolen item: “Paul Mitchell Sculpting Lotion”. This central node serves as a pivotal point for connecting various pieces of information related to the shoplifting incident.

Connected Nodes - Days: The graph includes nodes representing the days on which the shoplifting occurred. These nodes are connected to the central node, indicating the temporal aspect of the incident.

Peripheral Nodes - Devices: Peripheries or outer nodes in the graph represent the devices that were present during the shoplifting incident. Each peripheral node is linked to the central node, indicating its association with the date. This establishes a clear connection between the item and the devices involved.

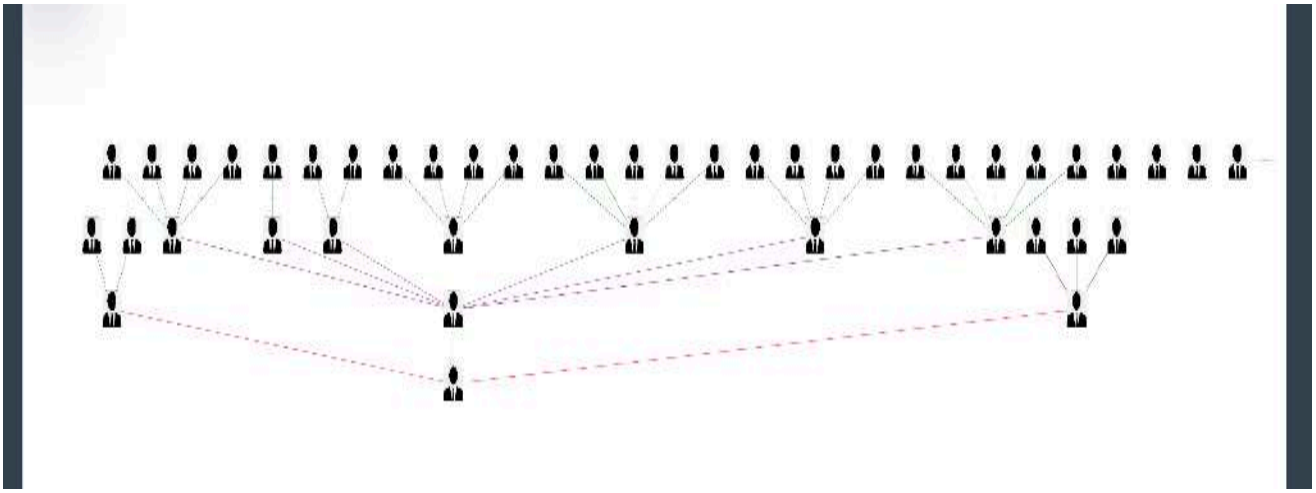
The screenshot below provides a snapshot of the interconnected nodes, aiding in a more intuitive understanding of the relationships between the stolen item, days, and devices. *(Paul Mitchell Sculpting Lotion)*

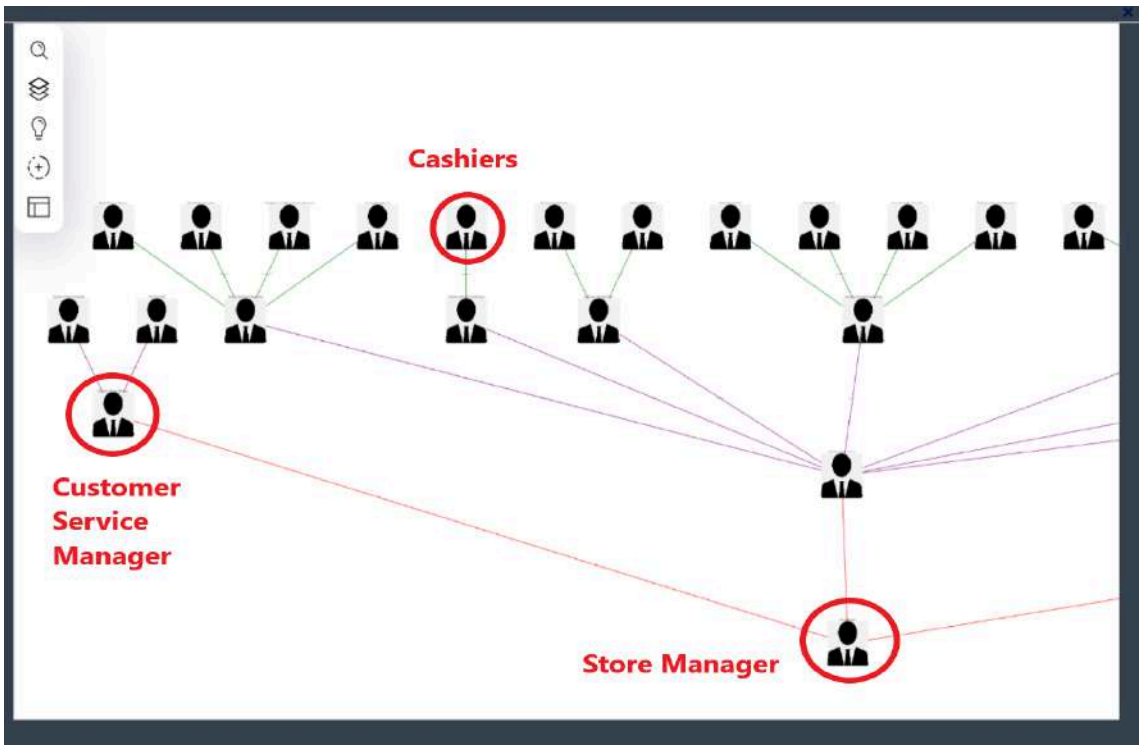


2. Position Hierarchy

The knowledge graph in this context is employed to visually represent the hierarchical structure of employees within a CVS store, emphasizing the direction from the highest-ranking positions to the lowest. Each level or position in the hierarchy is represented by a node in the knowledge graph. The nodes are interconnected to showcase the relationships between different levels of employees. For example, a higher-level node may be connected to multiple lower-level nodes, indicating a supervisory or managerial relationship. *(Position_Hierarchy)*

This graphical representation provides a valuable tool for comprehending the organizational dynamics and can be particularly useful for management and decision-making purposes.





3. Suppliers' Details

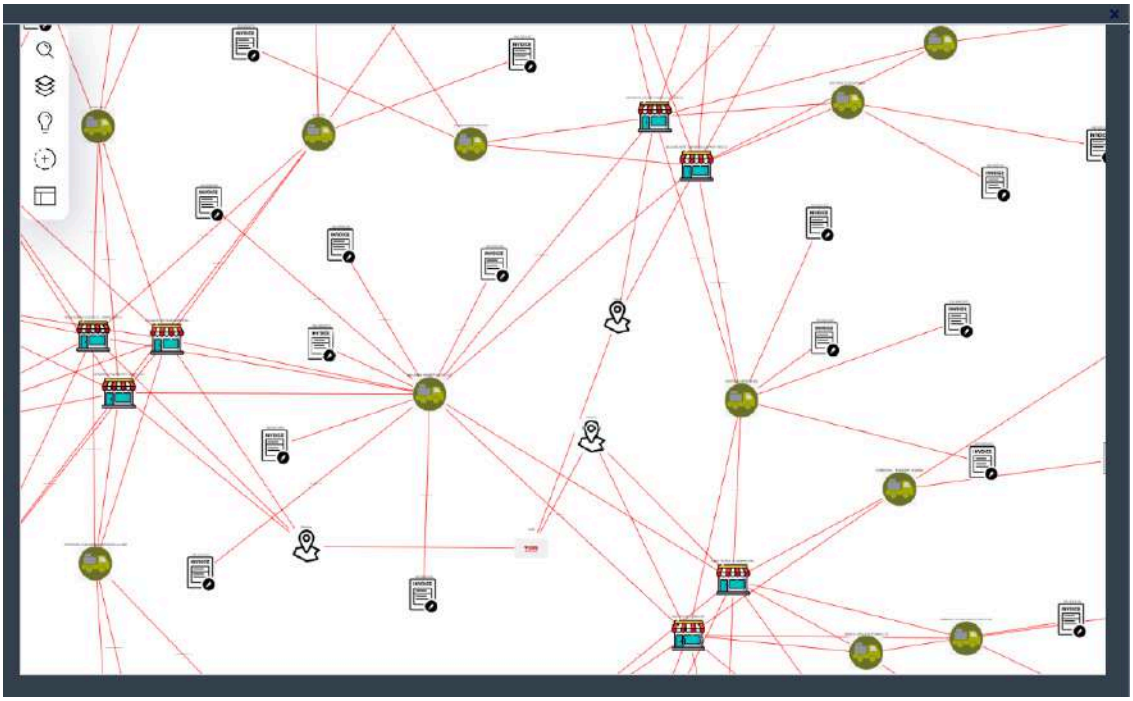
This knowledge graph creates a visual representation of the relationships between CVS Store branches, their associated suppliers, and the invoices corresponding to each supplier. This graphical representation facilitates a comprehensive understanding of the retail supply chain and financial transactions. *(Suppliers_Details)* Here's a detailed elaboration:

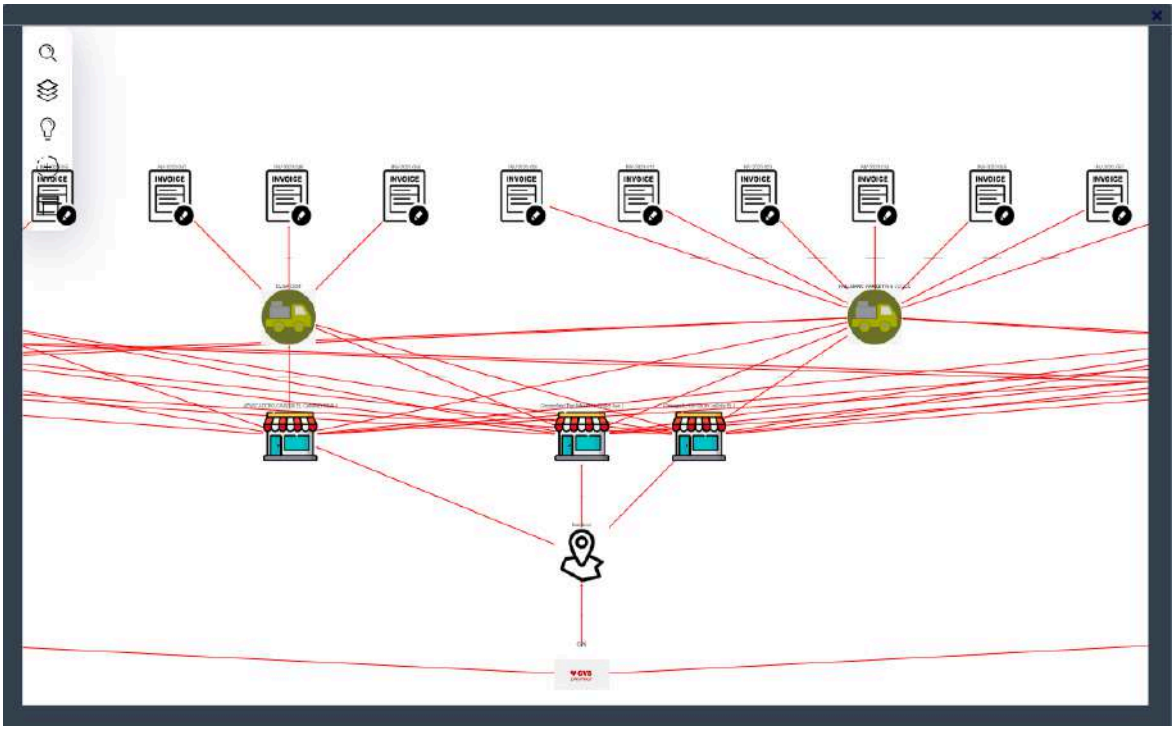
Central Node - CVS Store: The starting point or central node in the knowledge graph represents the CVS Store itself. This node serves as the anchor for the entire visualization, acting as the core entity around which the branches, suppliers, and invoices revolve.

First-Level Nodes - Branches: Branch nodes are connected to the central CVS Store node, representing the various branches of the retailer. These nodes reflect the geographical or organizational distribution of CVS Store locations.

Second-Level Nodes - Suppliers: Connected to each branch node are second-level nodes representing the suppliers that the corresponding branch deals with. Each branch may have multiple suppliers, and the connections illustrate the relationships between branches and their respective suppliers.

Peripheral Nodes - Invoices: Further extending the graph, third-level nodes represent the invoices associated with each supplier. The connections between supplier nodes and invoice nodes indicate the specific invoices linked to a particular supplier. This hierarchical structure helps organize the information in a way that is visually intuitive.





Intersecting Devices

The previous analysis steps have resulted in a comprehensive report that highlights the most intersecting or connected devices during the days when shoplifting incidents occurred for a specific item. The goal is to identify devices that exhibit a high degree of connectivity during these critical periods. Here's an elaboration on the implications and the subsequent actions based on this analysis:

Analysis Outcome: The detailed report generated from the analysis presents a clear picture of the devices that consistently appear during the days when shoplifting incidents involving a specific item took place. This includes the identification of intersected devices IDs and their frequency of occurrence.

Identification of Suspicious Devices: The focus is on isolating and identifying the devices with the highest number of connections or intersections across multiple shoplifting occurrences. These devices are considered the most connected during the critical periods under investigation.

Further Investigation: Suspicious devices are flagged for further investigation. This involves a deeper analysis of the activities and patterns associated with these devices during the identified shoplifting days.

Connected Devices

Identifying the suspects and comparison with CCTV

Executing "Device History" queries involves tracing the historical data of the devices that intersected during days when shoplifting incidents occurred. This process aims to identify these devices and subsequently compare the results with the footage obtained from CCTV cameras.

In more detail, for each of the most intersected devices, the system retrieves their historical data, encompassing details such as locations visited, dwell times, and movement patterns within the retail store. This historical context aids in understanding the devices' regular behavior and helps identify anomalies or patterns associated with shoplifting incidents.

Once the device histories are extracted, the next step involves a meticulous comparison with CCTV footage. This dual analysis allows for a comprehensive examination of the devices' physical presence and actions in the store. It helps cross-verify the data obtained from the geospatial and historical device queries with real-time visual evidence captured by CCTV cameras.

By integrating device history queries with CCTV footage analysis, the retail store gains a multi-dimensional perspective on the potential involvement of specific devices in shoplifting incidents.