NRF Center for Digital Risk & Innovation

Retail Fraud Taxonomy

Executive Summary

PREPARED BY

NRF National Retail Federation

TheChertoffGroup

RETAIL & HOSPITALITY ISAC

The Retail Fraud Taxonomy is a knowledge base of retail theft, fraud and abuse techniques derived from real-world observations, aimed at enhancing the community's ability to define, understand, prepare for, mitigate and detect fraud. The Taxonomy provides coverage of fraud behaviors, mitigations and detections from a wide range of fraud professionals. By categorizing techniques and related countermeasures, the Framework serves as an effective tool for education, communication, security assessments, team exercises and resource prioritization. This will help organizations bolster their defenses against the evolving landscape of fraud threats.

This document provides a high-level public summary of the Retail Fraud Taxonomy. The full Taxonomy is available at NRF.com. NRF and its partners plan to further update this taxonomy over the coming year and develop new tools to support its use and adoption. If you are interested in participating in these activities, please reach out to NRF at cdri@nrf.com.

Collaboration

The Retail Fraud Taxonomy is a collaborative initiative led and sponsored by the National Retail Federation (NRF), through its Center for Digital Risk & Innovation, in partnership with the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) and the Target Corporation along with other retail industry members. The Chertoff Group serves as technical advisor and project manager.

Purpose

Define Common Language

Provides a consistent set of terms and definitions to describe retail fraud behavior to standardize communication across different industries and domains. This unified language facilitates enhanced cross-team collaboration and improves industry-wide communications, ensuring that all stakeholders have a clear and common understanding of the threats they face.

Education and Awareness

Establishes a standardized lexicon and methodology to describe fraud techniques so professionals can effectively educate the industry and disseminate awareness about potential threats and their countermeasures. This common framework enables a unified approach to understanding and combating retail fraud, ensuring that knowledge about risks and defensive strategies is consistently communicated across various stakeholders.

Theat Modeling and Tabletop Exercises

Offers practical, real-world techniques to aid in modeling potential fraud schemes and developing scenarios. This can guide participant actions and responses. This approach ensures that simulations are grounded and provide actionable insights, enabling participants to effectively strategize and respond to dynamic threat environments. This method not only enhances the realism of training exercises but also boosts the preparedness of teams to manage and mitigate actual fraud incidents.

Security Assessment and Resources Prioritization

Proposes actionable mitigations and detection strategies tailored to counter specific techniques, facilitating the measurement of defensive effectiveness and the prioritization of security investments. This approach enables organizations to strategically allocate resources toward the most critical defenses, ensuring a robust security posture that is both responsive and adaptable to evolving threats.

Use Case(s)

Development and Controls, Business Processes and Policies

Design more secure systems and processes. By understanding the tactics and techniques commonly used by fraudsters, fraud professionals can architect systems that are inherently more resistant to fraud schemes. This will involve implementing specific security controls at various points in the architecture to mitigate and detect potential fraud schemes identified in the Fraud Taxonomy.

Business Case Justification

Conduct a thorough gap analysis to determine where current theft, fraud and abuse countermeasures might be lacking. By mapping existing defenses against the comprehensive list of techniques outlined in the Taxonomy, organizations can identify critical gaps and justify the expenditure required to address these gaps.

Information Sharing

Utilize a common language for collecting, analyzing and disseminating information on retail theft, fraud and abuse threats.

Testing

Simulate known techniques and campaigns. This approach helps in identifying how well an organization’s defenses can withstand specific types of schemes. Testers can select relevant techniques that align with the fraudsters that target the organization, providing a targeted and realistic testing scenario.

Vendor Evaluation

Evaluate how well a vendor's solution performs against known techniques during live demonstrations or through independent testing. This assessment can include how quickly and accurately the solution detects and responds to simulated techniques. Comparing these results against other products can help identify which solutions offer the most effective protection.