NRF Center for Digital Risk & Innovation

Retail Fraud Taxonomy

Version 1.0

November 2024

PREPARED BY

National Retail Federation

TheChertoffGroup

RETAIL & HOSPITALITY ISAC

Contents

Executive Summary

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.

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.

Threat 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 of 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.

Future State

The NRF Retail Fraud Taxonomy is designed as a dynamic and continuously evolving resource. As threats evolve, and as more industry partners contribute, the intent is to add new schemes, techniques, mitigations and detection data sources. These contributions are vital for effectively disrupting and combating fraud.

For questions or comments, please contact:

- Christian Beckner, National Retail Federation: **becknerc@nrf.com**
- Jon Tran, Chertoff Group: **jon.tran@chertoffgroup.com**

Taxonomy Elements

Term	Description
Tactics	The fraudster's step-wise objectives or goals they aim to achieve during each phase of a scheme.
Techniques	The various methods a fraudster will use to support a tactic, including enumeration of those techniques.
Mitigation	Security concepts and technologies that can be used to prevent or disrupt a technique from being successfully executed.
Detection Sources	Telemetry that can be collected to detect fraud that is in progress or has occurred in the past.
Schemes	The ultimate objective of fraud activity, which can be broken down into a series of Tactics, Techniques and Procedures (TTPs).
References	Academic research, case studies, threat intelligence, security blogs, etc. that are used to inform the Retail Fraud Taxonomy.

Tactics

The fraudster's step-wise objectives or goals they aim to achieve during each step of a fraud scheme. These tactics organize and define the various phases of the lifecycle of a scheme. Not all phases are required for a scheme as there are actors that specialize in each phase. For example, a fraudster may achieve Control by exchanging an illicitly gathered gift card for a legitimate one assigned to them.

Tactic	Description
Pre-Compromise	Operations that occur prior to compromise
Initial Access	Stealing, generating, confirming or otherwise obtaining a legitimate gift card, account or other resource

Control	Physically or digitally gaining control of a resource from a customer or retailer
Monetization	Converting illicitly gathered resources into liquid funds or an item that can be converted into liquid funds

Schemes

The ultimate objective of fraud activity, which can be broken down into a series of Tactics, Techniques and Procedures (TTPs). More schemes such as Return Fraud will be added as the Taxonomy grows.

Scheme	Description
Gift Card Fraud	Tampering, generating, stealing or otherwise using a gift card in an unauthorized manner to extract resources
Account Takeover	Gaining unauthorized access to a victim's account

Techniques

The various methods a fraudster will use to support a tactic, including enumeration of those techniques.

Technique Table

Pre-Compromise	Initial Access	Control	Monetization
Reconnaissance	Shoplifting	Gift Card Extortion	Resale
Social Engineering	Social Engineering	Valid Accounts	Drop Shipping
Fake Pages	Gift Card Extortion	Fraudulent Account	Unwitting Buyer
Acquire Database	Check Gift Card Balance	Fraudulent Account Update	Checkout
Gift Card Number Generation	Application	Gift Card Return	Point of Sale
Password Reset	Phone Verification	Gift Card Merging	Guest Services
Proxy Abuse	In-Store Gift Card Verification	Gift Card Tampering	Online Web/Mobile
	Valid Accounts	Gift Card Redemption	
	Fraudulent Account	Loyalty Points Abuse	
	Fraudulent Account Update		

	Password Reset		
	Credential Stuffing		

Reconnaissance FT1001

- **Tactics:** Pre-Compromise
- **Schemes:** Gift Card Fraud, Account Takeover
- **Description**
  - Fraudsters actively or passively gather information that can be used to support operations. Information may include details of the victim organization, infrastructure or staff/personnel. This information can be leveraged by the fraudster to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute future operations.
  - Threat actors will attempt to create accounts, wish lists and other related assets using lists of usernames and credentials from breached databases. If the attempt fails, it signals to the actor that the account already exists and is a good candidate for credential stuffing.
- **Mitigation**
  - Training and Awareness
    - At physical locations, train employees to identify and report suspicious individuals to security.
  - Document Control
    - At physical locations, keep all company, store or corporate-related documents, manuals or communication in a non-public or secure area not visible to non-employees.
  - Security Guards
    - At physical locations, utilize security guards to identify and deter reconnaissance attempts.
  - Software Configuration
    - Fully decommission obsolete login software that may not be protected by current security protocols.
    - Redirect login requests to obsolete software to follow the approved login flow.
- **Detection**
  - Network Traffic Address Attributes
    - Automated network reconnaissance will scan internet resources in a manner that a normal user typically will not. Monitor for connections to suspicious ports and traversal to suspicious directories such as www.mywebsite.com/admin or www.mywebsite.com/phpadmin.
  - Online Identities
    - When account creation is not a high barrier, often fraudsters will create test accounts to support development of automation or defender rule logic testing. These test accounts may be identified with false information about identity, but also may be indicators of the capabilities the fraudster is developing. Identifying and monitoring such accounts can reveal important information about the actor's operation and intention.

        - Monitor account creation endpoints for abnormal behavior. Actors will use account creation as a method to test credential lists to determine whether an account already exists at the targeted site before submitting a login request using those credentials.
    - Video Surveillance Systems
        - At physical locations, use video surveillance to identify and report suspicious individuals to security.
- **References**
    - MITRE ATT&CK
    - Industry Partner Collaboration

Social Engineering FT1002

- **Tactics:** Pre-Compromise
- **Schemes:** Gift Card Fraud, Account Takeover
- **Description**
    - The fraudster will use various means such as phishing or phone calls to fool victims into divulging resource information. Fraudsters may also target helpdesk or customer support to divulge resources or information or fraudulently update an account. This information can be used to support other tactics and future operations.
- **Mitigation**
    - Software Configuration
        - Configure email gateway to filter message based on validity checks of sender domain and integrity of messages in combination with phishing email detection capabilities.
    - Training and Awareness
        - Utilize consumer fraud awareness and education campaigns, signage, pop-ups and other forms of communication.
- **Detection**
    - VoIP Attribute
        - Monitor for known VoIP numbers that are typically used for fraud.
- **References**
    - MITRE ATT&CK
    - Avoiding and Reporting Gift Card Scams

Fake Pages FT1003

- **Tactics:** Pre-Compromise
- **Schemes:** Gift Card Fraud, Account Takeover
- **Description**
    - The fraudster creates a web page that may mimic a legitimate website to fool victims into divulging information. This website may visually appear to be legitimate or have a URL that is like the legitimate website.
    - One example of this is to register a domain that looks or sounds like a legitimate website. If www.legitimatewebsite.com was the target, the fraudster may register a website similar to www.legitimatewebsite.io or www.legitwebsite.com. Using this, along with similar visual elements, the fraudsters can fool victims into divulging information such as account name and password.

- **Mitigation**
  - Website Takedown Requests
    - When a fake page is identified file a takedown request with the Website Host and DNS Registrar.
  - DNS Registration
    - Identify potential URLs that may be mistaken for the legitimate website and register them so they cannot be used by fraudsters.
- **Detection**
  - Network Traffic Attributes
    - Monitor domain registration, certificate transparency logs and phishing sites to identify sites established with your branding but designed to fool your customers into divulging information.
- **References**
  - Industry Partner Collaboration

Acquire Database FT1004

- **Tactics:** Pre-Compromise
- **Schemes:** Gift Card Fraud, Account Takeover
- **Description**
  - Fraudster will, through legitimate or illegal means, acquire databases that may be used for future operations. These databases may range from legitimate marketing information sold by reputable companies to data stolen from victims.
  - Some examples of databases that can be acquired to support operations are account databases, marketing information, gift card numbers and personally identifiable information (PII).
- **Mitigation**
  - Password Policy
    - Encourage using strong passwords with sufficient length and complexity. Discourage reusing passwords.
- **Detection**
  - Online Identities
    - Subscribe to breach databases and monitor logins for usage of known or publicly compromised credentials.
- **References**
  - MITRE ATT&CK
  - Top 10 Digital Commerce Account Risks & How to Mitigate Them by Gunnar Peterson
  - Authentication and Access to Financial Institution Services and Systems

Gift Card Number Generation FT1005

- **Tactics:** Pre-Compromise
- **Schemes:** Gift Card Fraud
- **Description**
  - Fraudster uses an algorithm or brute force to generate gift card numbers that can potentially be legitimate. This can be conducted by predicting or acquiring the algorithm used to generate gift card numbers and creating them. This can be used with Check Gift Card Balance to identify legitimate gift cards with funds for future use.

- **Mitigation**
  - Brute Force Resistant Gift Card Numbers
    - Generate long and complicated gift card numbers that are resistant to prediction.
- **Detection**
  - This technique cannot be easily detected by organizational controls due to it occurring outside of the organization's scope.
- **References**
  - Industry Partner Collaboration

Password Reset FT1006

- **Tactics:** Pre-Compromise, Initial Access
- **Schemes:** Account Takeover
- **Description**
  - Actors abuse the password reset functionality to verify whether or not an account exists on a website. If the website provides feedback that indicates the account does exist, the actor then proceeds to attempt a login for that account using exposed credentials. If the account does not exist, the actor does not submit a login request to avoid expending unnecessary resources on an invalid account.
  - Actors compromise the victim's email account and then submit a password reset request to the targeted site. The actor is able to change the victim's password to one of their choosing, allowing them access to the victim's account.
- **Mitigation**
  - Neutral Feedback
    - Do not provide feedback that notifies an actor if the account exists or does not exist on the website.
  - Customer Notification
    - Notify all available contacts on the account when a password is reset.
- **Detection**
  - Behavioral Attribute
    - Monitor password reset endpoints for abnormal behavior.
  - Velocity Attribute
    - Identify automated attempts to validate a credential list by volume of attempts.
- **References**
  - Industry Partner Collaboration

Proxy Abuse FT1007

- **Tactics:** Pre-Compromise
- **Schemes:** Account Takeover
- **Description**
  - Actors abuse legitimate or illegal proxy services that act as an intermediary for requests from clients seeking resources from other servers, effectively masking the fraudster's IP address or other network attributes. Some examples of this are use of commercial VPN services, proxies through hosting providers, residential proxies, compromised machines such as botnets and malware infected hosts, and TOR services.
- **Mitigation**
  - Behavioral Prevention

        - Block traffic from known proxies, TOR exit nodes and infected machines.
- **Detection**
    - Network Traffic Attributes
        - Aggregate IP addresses to identify the common carriers / autonomous system numbers.
        - Establish normal and abnormal behavior for traffic originating from those networks.
- **References**
    - MITRE ATT&CK

Shoplifting FT1101

- **Tactics:** Initial Access
- **Schemes:** Gift Card Fraud
- **Description**
    - Taking items from a store without paying for them. Shoplifting can range from concealing items in personal clothing or bags to swapping price tags to make items appear cheaper. Items shoplifted to support fraud are typically high value, small in size and easy to resell.
    - Examples of commonly stolen items to support fraud are gift cards, electronics and luxury goods.
- **Mitigation**
    - Bag Control
        - Control the size and type of bags that are permitted inside the store.
    - Structured Loss Prevention Program
        - Implement a structured loss prevention program involving physical security, policies, procedures, resources and systems to prevent, deter and identify merchandise or gift card loss.
    - Anti-Theft Prevention
        - Additional physical protection of products from theft such as locked shelving, containers and vending machines, and storing items behind checkout counter.
- **Detection**
    - Anti-Theft Security Tags
        - Attach a device to items that will cause an alarm if removed from the store without authorization.
    - Security Guards
        - At physical locations, use security guards to identify and deter shoplifting.
    - Video Surveillance Systems
        - Monitor video feeds for suspicious activity around high-value items.
- **References**
    - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

Gift Card Extortion FT1102

- **Tactics:** Initial Access, Control
- **Schemes:** Gift Card Fraud
- **Description**

    - The fraudster obtains gift cards through coercion of a victim. This can involve many forms, including threats of violence, property damage, harm to reputation or unwarranted government action, unlike robbery or theft where property is taken without consent.
    - A fraudster may pretend to be a representative of the government to coerce a victim through a fear response. They may convince a victim that they must purchase gift cards with their own funds and turn the gift card over to the fraudster.
    - Another common extortion scam is a fraudster pretending to be a relative of a victim who is being held against their will, whether by criminals or a foreign government. They then convince the victim to purchase gift cards as restitution or a bribe to release their family member.
    - Fraudsters will also prey on retail organizations, using these tactics against employees, coercing or convincing them to purchase gift cards without taking payment, resulting in register shortage.
- **Mitigation**
    - Primary Gift Card Lock-In
        - When a gift card is purchased, lock the gift card into the identity of the purchaser. Do not allow another person to use the gift card without identify verification or authentication.
    - Login Required
        - Require an account before permitting purchase of or transfer of a gift card.
    - Gift Card Purchase Limit
        - Enforce limits of quantity and/or the value that may be purchased by an interaction or person.
    - Training and Awareness
        - Consumer fraud awareness and education campaigns, signage, pop-ups and other forms of communication.
        - Employee education and awareness to ensure proper payment has been received for gift card transactions.
- **Detection**
    - Velocity Attributes
        - Monitor for the purchase of gift cards by value and quantity from an individual by a predetermined value and/or time frame.
    - Behavioral Attributes
        - Monitor for out-of-character purchases of an individual and their lifestyle.
- **References**
    - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)
    - Avoiding and Reporting Gift Card Scams

Check Gift Card Balance FT1103

- **Tactics:** Initial Access
- **Schemes:** Gift Card Fraud
- **Sub-Techniques:** Application FT1103.1, Phone Verification FT1103.2
- **Description**
    - The fraudster may abuse legitimate functions to confirm a gift card is active and has funds. To reduce overhead, retailers may have autonomous systems for gift card owners

and recipients to check if their gift card is usable and has value. These systems are generally available to the public for interaction.

- **Mitigation**
  - Login Required
    - Require authentication before displaying gift card status or value.
  - Access Code Required
    - Require an access code that is separate from the gift card number before revealing the status and funds on the gift cards.
  - Online Location Data
    - Some physical locations should not be able to check gift card balance. Some locations may also be the source of repeated fraud attempts. Prevent the ability to check gift card status and funds based on locations.
  - Phone Number
    - Automatically block phone numbers related to VoIP services and phone numbers that have been known to be used to perpetrate fraud.
- **Detection**
  - Network Traffic Attributes
    - Monitor for network traffic attributes such as IP address, DNS name, ASN and other digital location attributes, especially if some of these sources have known fraud activity or have a high risk of fraud activity.
  - Time-Based Attributes
    - Based on the location of your operations, monitor for activities that occur during off hours.
  - Device Attributes
    - Monitor device factors such as device type, user agent string, operating system, cookies.
  - Velocity Attributes
    - Monitor for number of requests based on a predetermined number of requests over a set amount of time.
  - VoIP Attribute
    - Monitor for use of VoIP numbers that are not tied to a physical landline or mobile phone.
- **References**
  - Industry Partner Collaboration

Check Gift Card Balance: Application FT1103.1

- **Tactics:** Initial Access
- **Schemes:** Gift Card Fraud
- **Description**
  - The fraudster may iteratively probe web applications using built-in functions in the applications to confirm the gift card is active and has funds. The fraudster may use gift card numbers that are generated by brute force guessing, purchased from a source or gathered from victims.
  - A fraudster may purchase a large amount of gift card numbers on the dark web. They will use the web application built-in function and in a manual or automated fashion check

to see if the gift card is active and has funds. This information can be used in future operations to convert the gift card into usable funds for the fraudster.

- **Mitigation**
  - Login Required
    - Require authentication before displaying gift card status or value.
  - Access Code Required
    - Require an access code that is separate from the gift card number before revealing the status and funds on the gift cards.
  - Online Location Data
    - Some physical locations should not be able to check gift card balance. Some locations may also be the source of repeated fraud attempts. Prevent the ability to check gift card status and funds based on locations.
- **Detection**
  - Network Traffic Attributes
    - Monitor for network traffic attributes such as IP address, DNS name, ASN and other digital location attributes, especially if some of these sources have known fraud activity or have a high risk of fraud activity.
  - Time-Based Attributes
    - Based on the location of your operations, monitor for activities that occur during off hours.
  - Device Attributes
    - Monitor device factors such as device type, user agent string, operating system, cookies.
  - Velocity Attributes
    - Monitor for number of requests based on a predetermined number of requests over a set amount of time.
- **References**
  - Industry Partner Collaboration

Check Gift Card Balance: Phone Verification FT1103.2

- **Tactics:** Initial Access
- **Schemes:** Gift Card Fraud
- **Description**
  - The fraudster may use a retailer-provided phone service to confirm a gift card is active and has funds. The fraudster may use gift card numbers that are generated by brute force guessing, purchased from a source or gathered from victims.
- **Mitigation**
  - Access Code Required
    - Require an access code that is separate from the gift card number before revealing the status and funds on the gift cards.
  - Behavior Prevention
    - Automatically block phone numbers related to VoIP services and phone numbers that have been known to be used to perpetrate fraud.
- **Detection**
  - Time Based Attributes

        - Based on the location of your operations, monitor for activities that occur during off hours.
    - VoIP Attribute
        - Monitor for use of VoIP numbers that are not tied to a physical landline or mobile phone.
- **References**
    - Industry Partner Collaboration

Check Gift Card Balance: In-Store Gift Card Verification FT1103.3

- **Tactics:** Initial Access
- **Schemes:** Gift Card Fraud
- **Description**
    - The fraudster uses legitimate functions inside a bricks-and-mortar store to verify status of gift cards. The fraudster may use kiosks, checkout or customer service to verify legitimacy of a gift card.
- **Mitigation**
    - Access Code Required
        - Require an access code that is separate from the gift card number before revealing the status and funds on the gift cards.
- **Detection**
    - Velocity Attributes
        - Monitor for gift cards a person is attempting to verify.
- **References**
    - Industry Partner Collaboration

Valid Accounts FT1104

- **Tactics:** Initial Access
- **Schemes:** Gift Card Fraud, Account Takeover
- **Description**
    - The fraudster may obtain, create and abuse accounts to gain access, elevate access or control a resource. Since these credentials are generally legitimate, they may be used to bypass access controls in place to protect resources. This can also be used to achieve persistence in a system.
    - One example of this is if a fraudster gains control over a loyalty account. The fraudster can control the spending of loyalty points to buy items to support monetization. If gift cards are tied to the accounts, this may also be a method to control gift card use.
- **Mitigation**
    - Multi-Factor Authentication
        - Use multiple forms of authentication such as username and password paired with a one-time passcode before permitting access.
        - Require identity verification upon detection of access requests that are significantly different than what is expected for the individual.
    - Password Policy

        - Encourage using strong passwords with sufficient length and complexity. Discourage reusing passwords.
- **Detection**
    - Network Traffic Attributes
        - Monitor for network traffic attributes such as IP address, DNS name, ASN and other digital location attributes, especially if some of these sources have known fraud activity or have a high risk of fraud activity.
    - Time-Based Attributes
        - Based on the location of your operations, monitor for activities that occur during off hours.
    - Device Attributes
        - Monitor device factors such as device type, user agent string, operating system, cookies.
    - Behavioral Attributes
        - Monitor for access attempts and purchases that are significantly different from known good behavior for each customer.
- **References**
    - MITRE ATT&CK
    - Top 10 Digital Commerce Account Risks & How to Mitigate Them by Gunnar Peterson
    - Authentication and Access to Financial Institution Services and Systems
    - NIST Digital Identity Guidelines 800-63

Valid Accounts: Fraudulent Account FT1104.001

- **Tactics:** Pre-Compromise, Initial Access
- **Schemes:** Gift Card Fraud, Account Takeover
- **Description**
    - The fraudster uses a legitimate resource to create an account for malicious usage. These accounts may be used for reconnaissance and to probe the defenses of the victim's applications.
    - One example of this is if a fraudster creates an account with fake information. Using this as a foothold the fraudster may gather information on the application itself such as naming convention, loyalty points and other information that may be used to monetize the account.
- **Mitigation**
    - Multi-Factor Authentication
        - Before permitting account changes, use multiple forms of authentication such as username and password paired with a one-time passcode before permitting access.
        - If relevant, send confirmatory message to the original contact fields (e.g., original email address, phone number, street address).
- **Detection**
    - Network Traffic Attributes
        - Monitor for network traffic attributes such as IP address, DNS name, ASN and other digital location attributes, especially if some of these sources have known fraud activity or have a high risk of fraud activity.
    - Time-Based Attributes

        - Based on the location of your operations, monitor for activities that occur during off hours.
    - Device Attributes
        - Monitor device factors such as device type, user agent string, operating system, cookies.
    - Velocity Attributes
        - Monitor for accounts that are created quickly in succession from the same location or with similar features.
- **References**
    - Top 10 Digital Commerce Account Risks & How to Mitigate Them by Gunnar Peterson

Valid Accounts: Fraudulent Account Update FT1104.002

- **Tactics:** Pre-Compromise, Initial Access
- **Schemes:** Gift Card Fraud, Account Takeover
- **Description**
    - The fraudster uses and makes changes to an account without the knowledge of the account holder.
    - One example of this is if a fraudster convinces a helpdesk to update the phone number of a legitimate account to one they control. The fraudster can then use this to reset the password or otherwise authenticate to control the victim's account.
- **Mitigation**
    - Multi-Factor Authentication
        - Use multiple forms of authentication such as username and password paired with a one-time passcode before permitting access.
        - Require identity verification upon detection of access requests that are significantly different than what is expected for the individual.
        - Send confirmatory message to the original contact fields (e.g., original email address, phone number, street address).
- **Detection**
    - Network Traffic Attributes
        - Monitor for network traffic attributes such as IP address, DNS name, ASN and other digital location attributes, especially if some of these sources have known fraud activity or have a high risk of fraud activity.
    - Time-Based Attributes
        - Based on the location of your operations, monitor for activities that occur during off hours.
    - Device Attributes
        - Monitor device factors such as device type, user agent string, operating system, cookies.
    - Velocity Attributes
        - Monitor for accounts that are created quickly in succession from the same location or with similar features.
    - Online Identities
        - Monitor for account creations with suspicious names that do not appear legitimate. Some examples are ABCD, AAA, QAZ, etc.
- **References**

- Top 10 Digital Commerce Account Risks & How to Mitigate Them by Gunnar Peterson

Credential Stuffing FT1105

- **Tactics:** Initial Access
- **Schemes:** Account Takeover
- **Description**
  - Fraudsters abuse a variety of web automation tools to automate login attempts using credential lists known as “combolists.” Web automation serves a legitimate purpose in web application development and testing, but commercial projects can be abused by threat actors for illicit activity.
  - Fraudsters develop custom credential stuffing tools to automate login attempts. These tools can be site-specific or configurable via files known as “configs” which are then either sold or shared in underground communities. These tools range from simple scripts where technical details for the transaction are coded into the script itself, to fully configurable tools where actors can insert their own variables and other parameters into the automation.
- **Mitigation**
  - Behavioral Prevention
    - Many commercial services provide bot detection and mitigation, often incorporated into content delivery networks and other management packages.
    - Commonly available tooling includes default technical indicators which should be mitigated at the edge and automatically denied.
- **Detection**
  - Velocity Attribute
    - Monitor for surges in login attempts and other anomalous activity.
    - Monitor the response to login attempts where a surge in attempts to access accounts that do not exist at the target organization is a strong indicator of automated credential stuffing.
  - Behavioral Attributes
    - Monitor for repeated patterns of activity post-login, which is an indicator that the activity is automated.
- **References**
  - MITRE ATT&CK
  - Top 10 Digital Commerce Account Risks & How to Mitigate Them by Gunnar Peterson

Gift Card Return FT1201

- **Tactics:** Control
- **Schemes:** Gift Card Fraud
- **Description**
  - The fraudster converts an illicitly acquired or invalid gift card into a legitimate gift card.
  - For example, a fraudster illicitly obtains a gift card. Through social engineering or taking advantage of a retailer’s legitimate system, they transfer the value from the illicitly obtained gift card to a new gift card that the fraudster legitimately owns.
- **Mitigation**
  - Return Limits
    - Do not exchange gift cards over a pre-determined value.

- **Detection**
  - Transaction Data
    - Identify suspicious purchases and returns by gift card numbers.
- **References**
  - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

Gift Card Merge FT1202

- **Tactics:** Control
- **Schemes:** Gift Card Fraud
- **Description**
  - The fraudster obtains a gift card through legitimate means. Using a retailer-provided method they transfer value from an illicitly obtained gift card to legitimate gift cards.
  - For example, a fraudster purchases a legitimate gift card with a value of $5. They illicitly obtain multiple gift cards with values of $100 and $150. Using a legitimate retailer feature they combine gift cards. The values of the illicitly obtained gift cards are added to the legitimate one. The fraudster added $250 to their $5 gift card. They now have $255 on their legitimate gift card.
- **Mitigation**
  - Behavior Prevention
    - Do not permit merging of gift cards.
  - Login Required
    - Require authentication before permitting transfer of gift card value.
  - Access Code Required
    - Require an access code before permitting transfer of gift card value.
- **Detection**
  - Transaction Data
    - Identify suspicious transfer of value from gift cards to other gift cards.
  - Velocity Attributes
    - Identify suspicious transfers from many gift cards to one gift card, for example, if 20 gift cards with value of $5 are added to a single gift card.
- **References**
  - Industry Partner Collaboration

Gift Card Tampering FT1203

- **Tactics:** Control
- **Schemes:** Gift Card Fraud
- **Description**
  - Fraudster takes physical possession of an unactivated gift card and takes the information that allows them to control the gift card when it is funded and activated.
  - An example is if a fraudster steals gift cards from a store. They copy down the pertinent information needed to control the gift card and verify funds such as gift card number and security PIN. The fraudster then repackages the gift card and returns it to the store. When a victim purchases the gift card and loads value, the fraudster can spend the funds on the gift card without the victim's awareness.
- **Mitigation**

    - Primary Gift Card Lock-In
        - For gift cards, lock the gift card into the identity of the purchaser. Do not allow another person to use the gift card without identify verification or authentication.
    - Login Required
        - For gift cards, require an account before permitting purchase of or transfer.
    - Gift Card Location
        - Store gift cards behind checkout counter to limit theft.
    - Video Surveillance System
        - For in-store gift card displays, consider the placement of a video security camera (CCTV) to monitor the area. Utilize signage to inform customers of CCTV use.
- **Detection**
    - Security Guard
        - At physical locations, use security guards and/or other store employees to identify instances of fraudsters stealing gift cards and/or returning tampered gift cards.
    - Video Surveillance Systems
        - At physical locations, use video surveillance to identify instances of fraudsters stealing gift cards and/or returning tampered gift cards.
- **References**
    - Industry Partner Collaboration
    - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

Gift Card Redemption FT1204

- **Tactics:** Control
- **Schemes:** Gift Card Fraud
- **Description**
    - The fraudster obtains a gift card through illegitimate or illicit means and purchases an item.
    - One example of this is if a fraudster uses a fraudulently obtained gift card to purchase a high-value easy-to-sell item such as jewelry or electronics. The fraudster then can monetize these items through various strategies such as resale or drop shipping.
- **Mitigation**
    - Primary Gift Card Lock-In
        - For gift cards, lock the gift card into the identity of the purchaser. Do not allow another person to use the gift card without identify verification or authentication.
    - Login Required
        - For gift cards, require an account before permitting purchase of or transfer.
- **Detection**
    - Transaction Data
        - Identify suspicious purchases of commonly resold items with potentially illicitly obtained gift cards.
- **References**
    - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

Loyalty Points Abuse FT1205

- **Tactics:** Control
- **Schemes:** Account Takeover
- **Description**
  - The fraudster converts loyalty points into items or gift cards that can be used from monetization.
  - One example of this is if a fraudster successfully compromises a victim's account through means such as Social Engineering. They can convert the victim's loyalty points into a gift card that the fraudster controls. This gift card can be further used for monetization.
- **Mitigation**
  - Multi-Factor Authentication
    - Use multiple forms of authentication such as username and password paired with a one-time passcode before permitting access.
    - Require identity verification upon detection of access requests that are significantly different than what is expected for the individual.
  - Password Policy
    - Encourage using strong passwords with sufficient length and complexity. Discourage reusing passwords.
- **Detection**
  - Network Traffic Attributes
    - Monitor for network traffic attributes such as IP address, DNS name, ASN and other digital location attributes, especially if some of these sources have known fraud activity or have a high risk of fraud activity.
  - Time-Based Attributes
    - Based on the location of your operations, monitor for activities that occur during off hours.
  - Device Attributes
    - Monitor device factors such as device type, user agent string, operating system, cookies.
  - Behavioral Attributes
    - Monitor for access attempts and purchases that are significantly different from known good behavior for each customer.
- **References**
  - Industry Partner Collaboration

Resale FT1301

- **Tactics:** Monetization
- **Schemes:** Gift Card Fraud
- **Sub-Techniques:** Drop Shipping FT1301.1, Unwitting Buyer FT1301.2
- **Description**
  - The fraudster exchanges the illicitly obtained items or gift cards with another person or organization in exchange for liquid funds.

    - For example, a fraudster may steal jewelry worth $100. Using a third-party market such as Facebook Marketplace, they sell the illicitly obtained jewelry for $80, converting the item to currency the fraudster controls.
- **Mitigation**
    - Primary Gift Card Lock-In
        - For gift cards, lock the gift card into the identity of the purchaser. Do not allow another person to use the gift card without identify verification or authentication.
    - Login Required
        - For gift cards, require an account before permitting purchase of or transfer.
- **Detection**
    - Transaction data
        - Monitor for anomalous purchases of easily monetized items such as electronics and luxury goods.
- **References**
    - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

Resale: Drop Shipping FT1301.1

- **Tactics:** Monetization
- **Schemes:** Gift Card Fraud
- **Description**
    - The fraudster will use a third party to ship directly to a customer.
    - For example, to obfuscate the legitimacy of the gift card, the fraudster will store gift cards with a third-party partner who will list and manage their gift cards. A buyer will purchase the gift card from the third party. The buyer will receive illegally obtained gift cards.
- **Mitigation**
    - Primary Gift Card Lock-In
        - For gift cards, lock the gift card into the identity of the purchaser. Do not allow another person to use the gift card without identify verification or authentication.
    - Login Required
        - For gift cards, require an account before permitting purchase of or transfer.
- **Detection**
    - Transaction data
        - Monitor for anomalous purchases of easily monetized items such as electronics and luxury goods.
- **References**
    - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

Resale: Unwitting Buyer FT1301.2

- **Tactics:** Monetization
- **Schemes:** All
- **Description**
    - The fraudster sells the illicitly obtained goods or resources to an unwitting buyer.
- **Mitigation**
    - Primary Gift Card Lock-In

        - For gift cards, lock the gift card into the identity of the purchaser. Do not allow another person to use the gift card without identify verification or authentication.
    - Login Required
        - For gift cards, require an account before permitting purchase of or transfer.
- **Detection**
    - Market Resale Data
        - Monitor for anomalous sales of serialized items and gift cards in third-party locations and other repositories.
- **References**
    - Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

Checkout FT1303

- **Tactics:** Monetization
- **Schemes:** All
- **Sub-Techniques:** Point of Sale FT1303.1, Guest Services FT1303.2, Online Web/Mobile FT1303.3
- **Description**
    - The fraudster uses legitimate checkout to redeem or otherwise convert illicit resources into liquid funds.
- **Mitigation**
    - Access Code Required
        - Require an access code that is separate from the gift card before refunding gift card value.
    - Behavior Prevention
        - Identify potentially fraudulent returns and do not refund money if fraud is detected.
    - Restocking Fees
        - Require a fee for potentially fraudulent returns.
    - Delayed Reimbursement
        - Postpone refund by a predetermined amount of time for items that are commonly related to fraud.
- **Detection**
    - Transaction Data
        - Monitor for returns of items commonly related to fraud such as gift cards, luxury items and electronics for fraudulent activity.
- **References**
    - Industry Partner Collaboration

Checkout: Point of Sale FT1303.1

- **Tactics:** Monetization
- **Schemes:** All
- **Description**
    - The fraudster uses the checkout in-store to convert illicit resources into liquid funds.
- **Mitigation**
    - Access Code Required

        - Require an access code that is separate from the gift card before refunding gift card value.
    - Behavior Prevention
        - Identify potentially fraudulent returns and do not refund money if fraud is detected.
    - Restocking Fees
        - Require a fee for potentially fraudulent returns.
    - Delayed Reimbursement
        - Postpone refund by a predetermined amount of time for items that are commonly related to fraud.
- **Detection**
    - Transaction data
        - Monitor and record product serial number of items that are commonly related to fraud.
    - Velocity Attributes
        - Monitor returns for total amount and total value of items returned.
- **References**
    - Industry Partner Collaboration

Checkout: Guest Services FT1303.2

- **Tactics:** Monetization
- **Schemes:** All
- **Description**
    - The fraudster uses the guest services in-store to convert illicit resources into liquid funds.
- **Mitigation**
    - Access Code Required
        - Require an access code that is separate from the gift card before refunding gift card value.
    - Behavior Prevention
        - Identify potentially fraudulent returns and do not refund money if fraud is detected.
    - Restocking Fees
        - Require a fee for potentially fraudulent returns.
    - Delayed Reimbursement
        - Postpone refund by a predetermined amount of time for items that are commonly related to fraud.
    - Training and Awareness
        - Train customer service representatives to identify potential fraud situations and deny refund.
- **Detection**
    - Transaction data
        - Monitor and record product serial number of items that are commonly related to fraud.
    - Velocity Attributes
        - Monitor returns for total amount and total value of items returned.

- **References**
  - Industry Partner Collaboration

Checkout: Online/Web Mobile FT1303.3

- **Tactics:** Monetization
- **Schemes:** All
- **Description**
  - The fraudster uses digital resources to convert illicit resources into liquid funds.
- **Mitigation**
  - Online Location Data
    - Some physical locations should not be able to return items. Some locations may also be the source of repeated fraud attempts. Prevent the ability to return items for funds based on locations.
- **Detection**
  - Transaction data
    - Monitor and record product serial number of items that are commonly related to fraud.
  - Network Traffic Attributes
    - Monitor for network traffic attributes such as IP address, DNS name, ASN and other digital location attributes, especially if some of these sources have known fraud activity or have a high risk of fraud activity.
  - Time-Based Attributes
    - Based on the location of your operations, monitor for activities that occur during off hours.
  - Device Attributes
    - Monitor device factors such as device type, user agent string, operating system, cookies.
  - Velocity Attributes
    - Monitor for number of requests based on a predetermined number of requests over a set amount of time.
- **References**
  - Industry Partner Collaboration

Mitigations

Security concepts and technologies that can be used to prevent or disrupt a technique from being successfully executed.

Primary Gift Card Lock-In FM1001

- **Description**
  - Ensure the purchaser is the only person that can monetize the gift card.
- **Technique(s) Mitigated**
  - Gift Card Extortion
  - Gift Card Control
  - Resale
  - Drop Shipping

- Unwitting Buyer
- Gift Card Purchase

Login Required FM1002

- **Description**
  - Ensure a resource is tied to an authentication source before allowing activation, use or transfer.
- **Technique(s) Mitigated**
  - Gift Card Extortion
  - Check Gift Card Balance
  - Check Gift Card Balance: Application
  - Gift Card Control
  - Gift Card Merge
  - Resale
  - Drop Shipping
  - Gift Card Purchase

Access Code Required FM1003

- **Description**
  - Require an access code before permitting access to resource.
- **Technique(s) Mitigated**
  - Gift Card Extortion
  - Check Gift Card Balance
  - Check Gift Card Balance: Application
  - Check Gift Card Balance: Phone Verification
  - Check Gift Card Balance: In-Store Gift Card Verification
  - Gift Card Merge
  - Checkout
  - Checkout: Point of Sale Checkout
  - Checkout: Guest Service

Multi-Factor Authentication FM1004

- **Description**
  - This involves requiring two forms of identification, such as a password and a fingerprint or a password and a one-time code sent to a mobile device.
- **Technique(s) Mitigated**
  - Valid Accounts
  - Valid Accounts: Fraudulent Account
  - Gift Card Extortion

Anti-Theft Prevention FM1005

- **Description**
  - Additional physical protection of products from theft (e.g., locked shelving, containers, vending machines, storing items behind checkout counter, etc.).
- **Technique(s) Mitigated**
  - Shoplifting
  - Gift Card Tampering

Training and Awareness FM1006

- **Description**
  - The fraudster uses digital resources to convert illicit resources into liquid funds.
- **Technique(s) Mitigated**
  - Reconnaissance
  - Social Engineering
  - Gift Card Extortion
  - Checkout: Guest Services

Website takedown requests FM1007

- **Description**
  - A formal request to a website owner, service provider or domain registrar to remove an offending website.
- **Technique(s) Mitigated**
  - Fake Pages

Behavior Prevention FM1008

- **Description**
  - Use capabilities to prevent suspicious behavior patterns from occurring on various systems.
- **Technique(s) Mitigated**
  - Check Gift Card Balance: Phone Verification
  - Gift Card Merge
  - Checkout
  - Checkout: Lane Checkout
  - Checkout: Guest Services
  - Checkout: Guest Services
  - Proxy Abuse

Restocking fees FM1009

- **Description**
  - Impose a fee for product returns.
- **Technique(s) Mitigated**
  - Checkout
  - Checkout: Lane Checkout
  - Checkout: Guest Services

Delayed Reimbursement FM1010

- **Description**
  - Delay return reimbursement for a predetermined amount of time.
- **Technique(s) Mitigated**
  - Checkout
  - Checkout: Lane Checkout
  - Checkout: Guest Services

Brute Force Resistant Gift Card Numbers FM1011

- **Description**
  - Use algorithms to generate long and complicated gift card numbers that are resistant to prediction.
- **Technique(s) Mitigated**
  - Gift Card Number Generation

Gift Card Purchase Limit FM1012

- **Description**
  - Enforce limits of quantity and/or the value that may be purchased by an interaction or person.
- **Technique(s) Mitigated**
  - Gift Card Extortion

DNS Registration FM1013

- **Description**
  - Identify potential URLs that may be used to fool individuals and register them to your organization.
- **Technique(s) Mitigated**
  - Fake Pages

Password Policy FM1014

- **Description**
  - Enforce strong passwords with length and complexity requirements.
- **Technique(s) Mitigated**
  - Acquire Database
  - Valid Accounts
  - Loyalty Points Abuse

Return Limits FM1015

- **Description**
  - Do not allow returns over a specified amount.
- **Technique(s) Mitigated**
  - Gift Card Return

Security Guard FM1016

- **Description**
  - A person charged with safeguarding the premises, protecting assets, preventing theft and ensuring the safety of both customers and staff. Their duties typically include monitoring surveillance equipment, patrolling the retail space, managing access points, responding to emergencies and sometimes assisting in loss prevention strategies. Security guards help deter shoplifting and vandalism, maintain order within the store, and contribute to creating a secure shopping environment. They may also be involved in checking receipts, managing crowd control during peak times or special events, and coordinating with law enforcement when necessary.
- **Technique(s) Mitigated**

  - Shoplifting
  - Reconnaissance

Bag Control FM1017

- **Description**
  - Control the admittance or size of bag allowed at the location.
- **Technique(s) Mitigated**
  - Shoplifting

Software Configuration FM1018

- **Description**
  - Harden devices with configurations that can mitigate techniques or harden attack surface.
- **Technique(s) Mitigated**
  - Social engineering

Neutral Feedback FM1019

- **Description**
  - Adversaries will use return codes from public applications to gather information. When providing automatic feedback for failed requests such as accounts, gift cards, password resets, etc., provide an abstract response that does not confirm or deny that the resource exists.
  - For example, if a user requests a password reset, instead of stating that the account exists and an email was sent to the email address on file, instead return "**If** the account exists, an email will be sent to the address on file."
- **Technique(s) Mitigated**
  - Password Reset

Customer Notification FM1020

- **Description**
  - Send a notification to the original contacts listed on an account or resource when changes are made to the account or resources.
  - For example, if an address is updated for an account, send an update notification to the email and phone number listed for the resource.
- **Technique(s) Mitigated**
  - Password Reset
  - Valid Accounts: Fraudulent Account Update

Detection Sources

Telemetry that can be collected to detect fraud that is in progress or has occurred in the past.

Anti-Theft Security Tags FD1001

- **Description**

    - A tag or similar device that is attached to an item that will cause an alarm or otherwise alert security personnel when they are removed without authorization.
- **Technique(s) Detected**
    - Shoplifting

Video Surveillance Systems FD1002

- **Description**
    - Cameras and related equipment used for monitoring activities in various settings to enhance security, deter crime and gather evidence when necessary.
- **Technique(s) Detected**
    - Shoplifting
    - Reconnaissance

Behavioral Attributes FD1003

- **Description**
    - Information involving user's behavior and habits. For example, a system might use a user's typing pattern, mouse movements, preferred language or how they navigate an application, etc., to look for deviations from normal or compare similarity to known abuse or fraud patterns.
- **Technique(s) Detected**
    - Gift Card Extortion
    - Valid Accounts
    - Credential Stuffing
    - Password Reset
    - Loyalty Points Abuse

Time Based Attribute FD1004

- **Description**
    - Time an action occurred that can be compared against a baseline of activity.
- **Technique(s) Detected**
    - Check Gift Card Balance
    - Check Gift Card Balance: Application,
    - Check Gift Card Balance: Phone Verification
    - Valid Accounts
    - Checkout: Online/Web Mobile
    - Loyalty Points Abuse

Device Attributes FD1005

- **Description**
    - Data related to a user's device, such as a smartphone or laptop, as indicators that identify what type of device and software they are using. For example, a system might require a specific cookie or device identifier, expect a consistent device profile to include screen resolution, memory, operating system, time zone, installed plug-ins or other data that may be used to measure device similarity.
- **Technique(s) Detected**
    - Check Gift Card Balance
    - Check Gift Card Balance: Application

- Check Gift Card Balance: Phone Verification
- Valid Accounts
- Checkout: Online/Web Mobile
- Loyalty Points Abuse

Velocity Attributes FD1006

- **Description**
  - Frequency or unusual velocity of an action compared to baseline by some aggregation value. An action might be gift card balance checks. An aggregation value might be a device identifier, IP address, user account ID, or other value. Optionally there can be a metric aggregation like count, sum, distinct count, average, standard deviation, etc. A concrete example might be looking for a large volume of orders in a short period of time for an account.
- **Technique(s) Detected**
  - Gift Card Extortion
  - Check Gift Card Balance
  - Check Gift Card Balance: Application
  - Check Gift Card Balance: In-Store Gift Card Verification
  - Valid Accounts, Gift Card Merge
  - Checkout: Point of Sale Checkout, Checkout: Guest Services
  - Checkout: Online/Web Mobile
  - Credential Stuffing
  - Password Reset

Network Traffic Attributes FD1007

- **Description**
  - Metadata about an IP address like whether it is a hosting provider, VPN or proxy service, residential network, cellular provider or residential ISP. This information may also be associated with user accounts or devices to baseline them over time and look for deviations from the usual access patterns.
- **Technique(s) Detected**
  - Fake Pages
  - Check Gift Card Balance
  - Check Gift Card Balance: Application
  - Valid Accounts
  - Checkout: Online/Web Mobile
  - Proxy Abuse
  - Loyalty Points Abuse

VoIP Attribute FD1008

- **Description**
  - A VoIP (Voice over Internet Protocol) number is a virtual phone number that is not tied to a physical telephone or mobile phone. These numbers are highly portable and may be swapped and reused.
- **Technique(s) Detected**
  - Check Gift Card Balance
  - Check Gift Card Balance: Phone Verification

- Social Engineering

Online Identities FD1009

- **Description**
  - Email addresses, Telegram usernames, social media handles, accounts, etc., that have been the source of fraudulent activities.
- **Technique(s) Detected**
  - Reconnaissance
  - Acquire Database
  - Valid Accounts
  - Password Reset

Transaction data FD1010

- **Description**
  - Records that are related to transactions in-store or online.
- **Technique(s) Detected**
  - Resale
  - Gift Card Return
  - Gift Card Merge
  - Gift Card Purchase
  - Drop Shipping
  - Checkout, Checkout: Point of Sale Checkout
  - Checkout: Guest Services
  - Checkout: Online/Web Mobile

Market Resale Data FD1011

- **Description**
  - Monitor sales of items through third-party market monitoring and other resale data.
- **Technique(s) Detected**
  - Resale: Unwitting Buyer

References

- Authentication and Access to Financial Institution Services and Systems
- Authentication and Lifecycle Management SP 800-63B
- Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)
- MITRE ATT&CK
- Top 10 Digital Commerce Account Risks & How to Mitigate Them by Gunnar Peterson
- Avoiding and Reporting Gift Card Scams
- Industry Partner Collaboration
  - Source not listed to obfuscate partner defenses