Gift Card Crimes: HB1074

MRA

Maryland Retailers Alliance

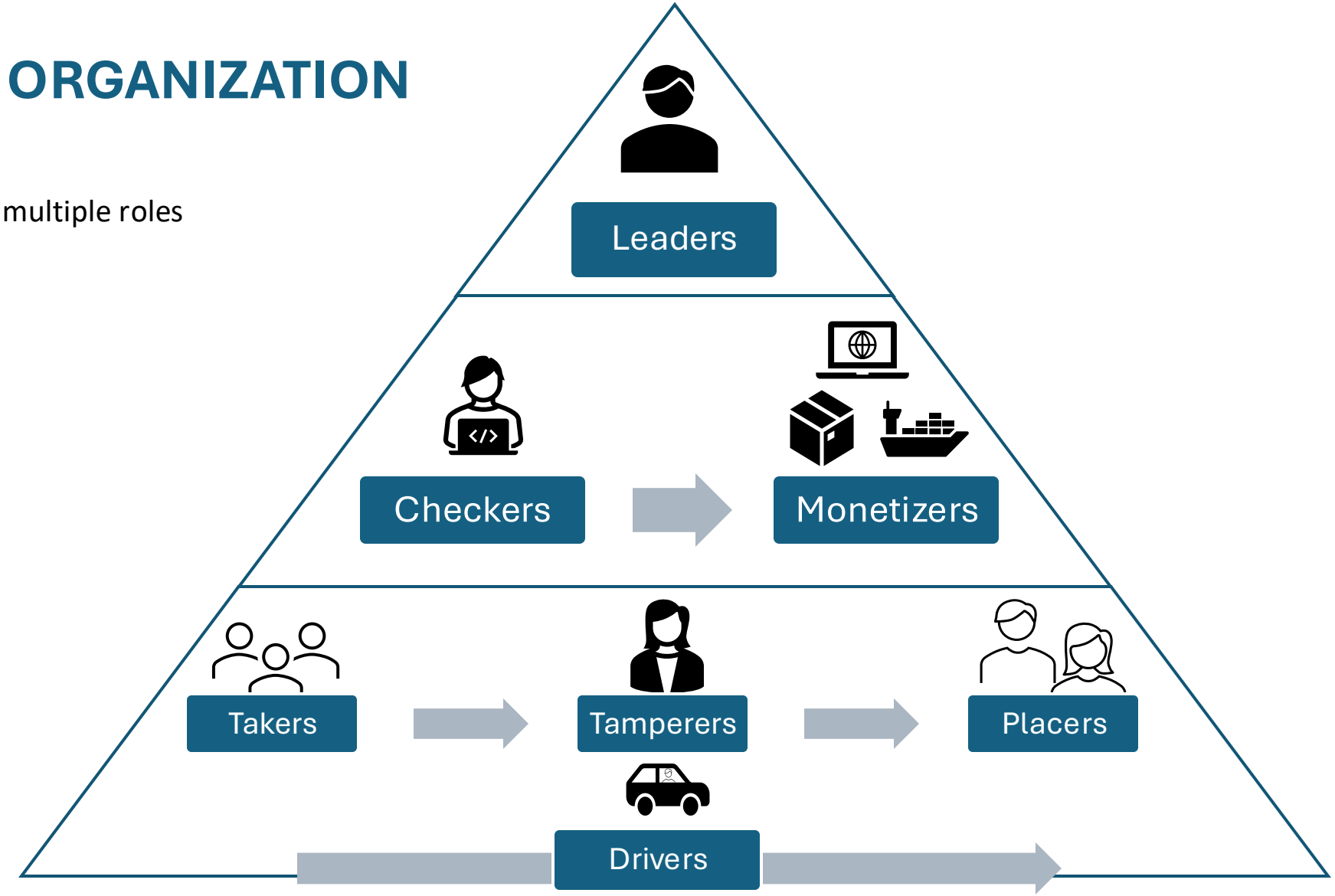
OVERVIEW: Gift Card Tampering

- Consumers purchase prepaid financial instrument cards from retailers which are stored on an open sales floor, and which contain various security features to protect the cards unique, specific and private financial information like the card number and pin.
- Perpetrators of theft commonly work together with others to act in specific roles, and sometimes perform multiple roles individually, to steal funds after a consumer makes the purchase of a gift card.
- Bad actors are focusing on brands that can be exchanged for hardware or other goods that can be sold on online marketplaces.
- Major retailers with numerous outlets are the main targets. Cards are usually stolen from smaller stores and moved to high-traffic areas where inventory sells quickly.
- There is a noticeable concentration in certain states, particularly those along major highways like Interstate 95.
- Retailers that are implementing preventive measures are experiencing significant decreases in tampering incidents.

Method of Operation

ROLES OF THE ORGANIZATION

*Subjects may play single or multiple roles



1. STEAL THE GIFT CARDS

Subject (“takers”) obtains prepaid financial instrument cards (gift cards) from a retail establishment’s sales floor fixtures and remove the cards from the store without payment.

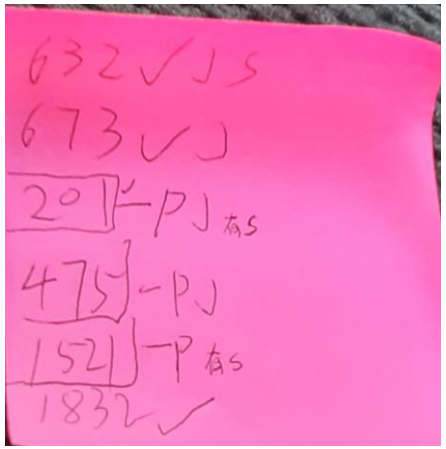
Subjects will act as or have a vehicle “driver” and may have a, or multiple, “lookouts” within the store.

2. PROCESS THE CARDS

Subjects then take said cards offsite where the "tamperers" carefully and skillfully remove the cards' security features (security stickers and/or packaging).

They then re-package the cards in a way that makes it difficult to tell that the packaging has been compromised.

**Subjects often track where cards are taken from, so they may replace the cards after they're taken at the same store, to circumvent retailers' technological fraud prevention systems*



Sample of tracking, based on addresses

3. GAIN CARD'S SENSITIVE INFORMATION

Subjects will obtain the cards' unique and private financial information (card numbers and pins) making them "compromised cards."

Subjects then have the compromised cards' **security features either replaced or recreated**, to make the compromised cards/packaging appear *untampered*, to preserve the confidence of the consumer and concealing the fact the compromised cards' private information was compromised.

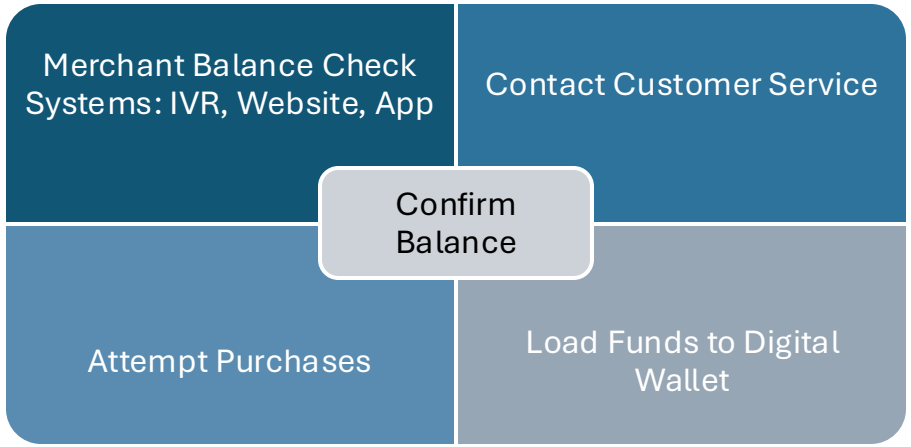
4. REPLACE THE CARDS BACK AT THE STORE

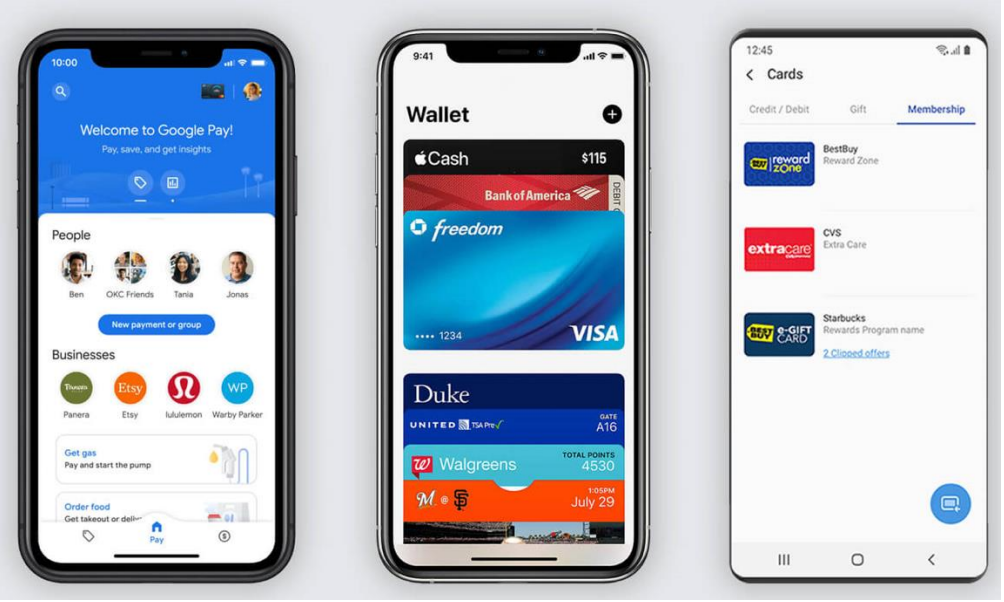
Subjects then **replace** the compromised cards **on store's fixture**, being either the same or different store, to pose the cards as uncompromised and available for **purchase by a consumer**.

5. BALANCE CHECK

The numbers and pins previously obtained from the card are then “**balance checked**” frequently so the subjects’, or those within their organization, are made aware when funds are placed on the compromised cards’ by a consumer.

Said balance checks may be in manual form (like via the phone) or via advanced electronic programs designed to provide easier and more frequent balance checks.





6. USE THE FUNDS FROM THE CARD

Upon the balance check of the compromised cards showing a balance, **subjects use the balance** removing it from the card without the cards' purchaser or owner being aware.

Fraudsters frequently utilize gift cards to purchase electronics, luxury items, tools, and more, often in tax-free states. These products are then shipped internationally to countries such as China, Russia, and select nations in the Middle East, where they are resold.

https://www.dhs.gov/hsi/insider/recognize-respond-gift-card-fraud-retail

WHAT IS PROJECT RED HOOK?

Project Red Hook was spearheaded under the auspices of Operation Boiling Point:

– This initiative was created to take a 30,000 ft view of the gift card fraud that is occurring transnationally and associated with international Organized Retail Crime (ORC) rings.

Immediate Goals and Priorities:

– Collect data at: GCFraud@hsi.dhs.gov or HSI Tip Line at 1-866-347-2423.

– Coordinate nationwide & eventually transnational investigative efforts to disrupt and dismantle these ORCs.

PROJECT RED HOOK

WORKING TOGETHER TO PROSECUTE GIFT CARD TAMPERING CRIMINALS

One of the challenges we are currently facing is a consistent and clear path to the prosecution of Card Tampering criminals, largely due to two key factors:

- Not having a strong partnership with law enforcement to educate regarding Card Tampering and potential tie to broader Organized Retail Crime rings.
- Because cards have no value throughout most of the “act of card tampering,” there has been a lack of clarity on what criminals could and should be charged with when they are caught in the act.

The Plan:

- HSI is urgently trying to increase national awareness regarding card tampering fraud across all Law Enforcement agencies at the Federal, State, and Local levels.
- HSI has documented a set of U.S. statutes immediately applicable to card tampering cases.
- Brands are updating their Terms & Conditions on both gift card products and card holder sites (i.e. balance inquiry) that will facilitate successful prosecution.
- HSI is engaging and educating brands regarding how to work with law enforcement to ensure arrests take place.

The following federal statutes are typically being used to prosecute gift card fraud:

Fraud and related activity in connection with access devices

- 18 U.S.C. § 1029(a)(6) prohibits anyone, when acting "knowingly and with intent to defraud," from soliciting a person for the purpose of "offering an access device," or "selling information regarding . . . an access device," "without the authorization of the issuer."
- 18 U.S.C. § 1029(a)(3) prohibits anyone, when acting "knowingly and with intent to defraud," from "possess[ing] fifteen or more devices which are counterfeit or unauthorized access devices." 18 U.S.C. § 1029(e)(3) defines the term "counterfeit access device" to mean "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud."

Fraud and related activity in connection with computers

- 18 U.S.C. § 1030(a) prohibits a wide variety of computer-related fraud. Section 1030(a)(2)(C), for instance, prohibits anyone from accessing a "protected computer . . . without authorization or exceeding authorized access," and "obtaining information." Section 1030(a)(4) prohibits accessing a "protective computer . . . knowingly and with intent to defraud" and obtaining "anything of value."

Mail fraud and other fraud offenses

- 18 U.S.C. § 1341 – Elements of Mail Fraud

HSI Contacts:

- GCFraud@hsi.dhs.gov
- 1-866-347-2423

- **Project Red Hook**
- Adam Parks, Assistant Special Agent in Charge
- Adam.K.Parks@hsi.dhs.gov

What can Maryland do?

- HB1074 is a much needed statutory tool for law enforcement, prosecutors and retailers.
- At this time, gift card crimes cannot be adequately prosecuted.
- We urge the committee to address this ever-growing criminal enterprise.