TLP: White

05.15.2018

Coupon Glittering: Best Practices for Mitigating Coupon Fraud

R-CISC
THE RETAIL ISAC

R-CISC EXECUTIVE INTELLEGENCE Recipients may share TLP: WHITE information. This rosource may be distributed without restriction.

Background

Cost-conscious customers continue to drive demand for digital solutions that save money while shopping. To meet this need, retailers developed digital coupons and customer rewards programs, which ultimately increase the company's exposure to risk of fraud.

Coupon Glittering, or Coupon Glitching, describes when a criminal exploits business process flaws, hacks, or coupon barcoding to commit fraud. Threat actors then "cash out" on coupon overages by loading the dollar amounts onto gift cards, re-selling products purchased at heavy discounts, or reselling the coupons themselves. In fact, this type of abuse is so rampant that a quick search of social media sites reveals many groups dedicated to sharing coupon glittering hacks.

Coupon authentication methods are limited, and as a result, cashiers may be put in a difficult situation by questioning the authenticity of a customer-presented coupons. Rather than running the risk of upsetting a customer or initiating a scenario that results in negative publicity, cashiers are forced to potentially side with the fraudster.

Exploits

Common exploits associated with coupon fraud include:

- Business process flaws or hacks
- Exploiting the coupon (including with photoshop, barcode manipulation, counterfeit coupons)

Fraud schemes may include:

- Printing multiples of the same coupon for use at different stores
- Manipulating digital and physical coupons to award large discounts off of any merchandise (instead of limited merchandise as intended)
- Selling counterfeit coupons that do not work and cause reputational damage
- Creating fraudulent barcoding structures that can manipulate point of sale (POS) terminals to award 100 percent off of merchandise

Business process exploit example: High-dollar coupons are generated with a unique barcode that, when used, validates against a database by the POS system.

Database updates are completed in batches, leaving a window for fraudsters to exploit single-use coupons at multiple different stores.

Strategies for Mitigating Coupon Fraud

- Cap the maximum dollar value that cashiers can override for un-scannable and high-value coupons
- Thoroughly test eCommerce websites and business processes to identify flaws and unintended consequences that could be exploited
- Monitor social media to stay informed on glitching trends and to listen for chatter related to your brands
- Isolate the coupon to specific products, pricing, promotions, and time durations
- Implement technology solutions that allow you to define specific usage rules for digital coupons
- Incorporate countdown clocks or other animated graphics into digital coupon design to help cashiers more easily distinguish legitimate coupons from fraudulent coupons
- Educate your front-line employees to recognize abnormal behavior
- Monitor cashier overrides and leverage surveillance cameras for possible employee theft of coupons

The R-CISC would like to thank its members and trusted sharing partners, including Kristopher Russo of ITS Partners, for contributing to the development of this resource.

For more information on the R-CISC membership or the Fraud Working Group, reach out to information@r-cisc.org.