Coupon Glittering: Best Practices for Mitigating Coupon Fraud
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.