Internal Collaboration as a Tool for Gift Card Fraud Mitigation

Insights from an R-CISC Member

R-CISC THE RETAIL ISAC

BACKGROUND

As gift card and e-gift card purchase continue to rise, growing at a rate of 29 percent annually*, so too are gift card fraud attempts. Weak security features make gift cards virtually as valuable to cybercriminals as cash. Common failings to secure gift cards include the mass production of cards with a predictable pattern, limited security, and easily enumerated number sequencing with limited analysis. Even unskilled bad actors can use tools to increment cards, get payouts online, or even re-encode mag strips with valid data for commercial use. As gift card security remains underregulated, negative consequences persist. In fact, Canadian authorities estimate that $5-55B annually* is laundered using gift cards.

In retail organizations, both information security and fraud investigation teams have a stake in detecting, protecting, and thwarting these attacks. As part of the educational effort put forth by the Gift Card Fraud Working Group, one R-CISC member shared what happened when their information security team partnered with fraud investigations. Not only did they see a tremendous overlap in their detection and intelligence collection, but they were they better able to correlate fraud activity and protect their environment.

With collaboration well established, this team shared several takeaways with the group for increasing gift card fraud mitigation.

**statistics source: (CNP, 2016); (Armerding, 2017)*

KEY BENEFITS

- **Watch your API Endpoints** – anywhere that your API is exposed, you should monitor for fraudulent activity. This includes your gift card balance inquiry page, shopping cart, and check-out page.
- **Look for Anomalies** – Fiscal outliers make themselves known quickly as bad actors typically make mass attempts. Predictive analytics help call out suspicious behavior like incrementing card numbers and/or pins.
- **Utilize Mitigation Controls** – Use controls like CAPTCHA on API endpoints, Gee-IP blocking to countries you don't ship to, or rate-limits on card numbers (i.e. don't allow balance inquiries after X attempts). These controls decrease the opportunity for an attacker to brute force pins and puts a dent on attacker productivity.
- **Increase Complexity** – adding another digit to a pin or move to alphanumeric options to exponentially increase the possible combinations attackers can search for, thus, limiting brute force capabilities.

R-CISC THE RETAIL ISAC