Gift Card Fraud
CASE STUDY

PURPOSE: Over the past several years, FIS™ has worked with many merchants and financial institutions on different variations of fraud. Sharing the information from one merchant case will provide the outline of their internal fraud and key factors of potential monetary loss to merchants when they become the victim of a fraud event.

BACKGROUND: A merchant participated in a Gift Card loyalty program for many years. Customers would purchase gift cards from the merchant that were redeemable at all of their store locations. As the number of locations grew, the merchant would add the gift card product to each store.

A gift card loyalty program is a merchant program that may utilize a standalone terminal, or can be incorporated into the existing merchant Point of Sale (POS) device/system. These programs build new and repeat customer bases for merchants. Merchants track the dollar value of cards sold and reduce their outstanding balance when cards are redeemed. This allows merchants to know their outstanding liability for the program and also allows them to balance their registers for this transactional activity.

BREACH #1 DETAILS

Timeline

- February 2014 - Merchant ABC deployed and continued to grow a successful gift card program.
- August 2017 – The owner at the merchant store submitted an Add Location form to add a new location, including virtual terminal for processing until the POS system was installed.
- August 2017 - November 2017 – Transactions were processed as normalon the virtual terminal.

This case study outlines a specific instance of a merchant's preventable internal fraud and the subsequent monetary loss.

Timeline, contunued

- November 2017 – The merchant installed their Point of Sale system at the location and the virtual terminal was no longer utilized.
- Early May 2018 – The location's General Manager is terminated from the company. Unbeknownst to the owner:
    - He took the virtual terminal URL
    - He took a stock of gift cards
    - He took the user name and password for the virtual terminal site
- May 2018 – September 2018 – Numerous transactions <$2,000 were processed multiple days and times on the virtual terminal totaling just under $100,000 in false gift card loads.
- September 2018 – The merchant realized that his books did not balance and contacted FIS and law enforcement for assistance.
- September 2018 – FIS deactivated all gift cards so the cards could no longer be used, and the merchant implemented a $100 activation (or add value limit) per gift card on their POS system.

Authorized User status for the General Manager was never revoked upon his termination.

Security Deficiencies

- Authorized User status for the General Manager was never revoked upon his termination.
- Funding limits were not placed on the cards and up to $2,000 was allowed to be added to the cards.
- The merchant and/or location was not monitoring daily gift card activity reports to see the odd activity.
- The merchant and/or location was not balancing their register with the gift card program activity.
- A common user name and password was utilized and stored by the internet browser on the location computer.

Financial Impact to the Merchant

- Merchant lost over $18,000 in redeemed gift cards that were never funded with real money.
- Merchant incurred all legal fees to pursue the former employee.
- Merchant incurred fees to implement security measures on POS system.
- Merchant lost numerous hours of productivity to detect the issue, identify and deactivate the gift cards, explain and fill out paperwork with law enforcement, implement new security measures with the POS system and all store locations, and file insurance loss.