CNP WHITE PAPER

CHARGEBACKS AND GIFT CARDS PART 1

Understanding and Avoiding E-Gift Card Fraud

CNP CardNotPresent.com®

THE INDEPENDENT SOURCE FOR ORIGINAL CNP NEWS

Chargeback

CHARGEBACKS AND GIFT CARDS PART 1

Understanding and Avoiding E-Gift Card Fraud

Last year consumers spent $127 billion on gift cards. That's an increase of nearly 400 percent since 2001 with analysts predicting continued escalation to $160 billion in sales by 2018. One of the biggest drivers of this growth is accessibility. Retailers and restaurants have made gift cards available in various channels from retail stores, grocery stores and convenience stores, to post offices, mobile devices and dedicated online sites. Along with the proliferation of sales outlets from which they are available, the anonymity of gift cards and the ease of redemption have attracted fraudsters in droves.

The most prevalent way fraudsters obtain gift cards is to purchase them with stolen credit cards, which results in chargebacks to merchants. Fraudsters also like to purchase gift cards with fabricated EMV credit cards from merchants that are not EMV compliant, which also results in chargebacks that are not fightable by the merchant. As of October 2015, card-present merchants that do not yet accept EMV chip-enabled credit cards are exposed when an EMV card is presented but not read with a chip reader.

When a chargeback is issued on a gift card that has already been redeemed, the merchant experiences the loss of the transaction amount by the cardholder (via the chargeback) as well as the loss of the cost of goods or services that were purchased. In addition, there are ancillary costs—those associated with distribution, customer acquisition and credit-card processing fees—that the merchant also loses.

Due to the high volume of fraud-related chargebacks surrounding the purchase of gift cards, Chargeback.com, Inc. (Chargeback) has commissioned a two-part whitepaper series to explore the various gift-card fraud related schemes and understand the best practices merchants should employ to prevent future financial losses. This first paper will focus on e-gift card fraud in card-not-present channels. The follow-up paper will discuss common fraud schemes with physical gift cards both in the card-not-present and card-present channels.

Open Loop vs. Closed Loop

There are two different kinds of gift cards in the market. Open-loop gift cards are those that carry a network brand—Visa, MasterCard or American Express—and can be used at any merchant location that accepts that card brand. Closed-loop gift cards refer to gift cards issued by specific retailers or restaurants that only can be redeemed by that merchant.

Closed-loop gift cards account for the majority of merchants' financial losses due to fraud. Unlike open-loop cards, closed-loop gift cards were not created as a form of currency. Also, they have multiple platforms, unlike bank-issued gift cards that were created with risk in mind, according to Khalid El-Awady, president at Chargeback.

Understanding the Scope of E-Gift Card Fraud

According to Giftcards.com, electronic digital gift cards are the fastest growing segment of the gift card industry growing at a rate of 29 percent annually. They are expected to make up 7 percent of the overall gift-card market by the end of 2016, accounting for more than $10 billion in sales, according to CEB/Tower Group. Because digital gift cards can be stored and used on mobile devices and sent almost immediately, they make perfect last-minute gifts.

While gift cards, in general, appeal to fraudsters, digital gift cards are even more popular with their near immediate delivery, no physical address requirements, and high consumer adoption rates have created a perfect storm that retailers must be prepared for. According to a recent report by payments processor ACI Worldwide, across hundreds of millions of transactions, electronic gift cards have the highest fraud attempt rates of all products sold by their merchants. Between Black Friday (the Friday following the Thanksgiving holiday in the U.S.) and Christmas in 2015, 9.5 percent of all online fraud attempts were on downloadable e-gift cards.

Considering the $10 billion e-gift card market cited by CEB/Tower Group and ACI's 9.5 percent fraud rate, an estimated $950 million was lost to e-gift card fraud this year. Given that the 2015 LexisNexis True Cost of Fraud Survey recently estimated that every $1 lost to fraud actually costs merchants $2.27 for e-commerce transactions and $2.89 in mobile channels, e-gift card fraud alone will cost CNP merchants an estimated $2.16 billion this year.

The Impact of Secondary Markets

One of the biggest contributing factors to gift card fraud in general, and especially e-gift cards, is the abundance of online marketplaces allowing consumers to sell unused gift cards online. Some buy cards directly from consumers and resell them. Others take the form of online classifieds or auctions. Most gift cards sold on these sites are available for less than the value of the gift card, depending on the popularity of the brand. Reseller sites pay sellers and charge buyers set rates for each brand they sell. Online classified and auction sites allow sellers to set their own price which can carry deep discounts.

> *"It used to be that a $100 gift card to a popular chain restaurant was only worth two dinners and a couple drinks. Now, it can be worth up to $90 of liquid funds (cash) on a secondary site"*

While the majority of gift cards sold on such sites are purchased legitimately, the opportunity to turn gift cards into cash is attractive to many fraudsters. Merchants, therefore, need to shift the way they view the sales of these products on secondary markets.

"It used to be that a $100 gift card to a popular chain restaurant was only worth two dinners and a couple drinks. Now, it can be worth up to $90 of liquid funds (cash) on a secondary site," says El-Awady. "Most merchants are learning this the hard way when they receive fraud chargebacks for gift cards purchased with stolen credit cards. Most did not consider risk prevention when they created their online gift-card program or the platform used for purchasing these products."

Usually, when merchants receive a chargeback or report of confirmed fraud on a gift card, they retract the remaining funds on the card to lessen the loss from the chargeback. When consumers purchase cards from a secondary-market site (which becomes the merchant of record), many still believe it's the merchant's duty to guarantee the funds on the card. Many merchants are reporting this has become a problem and different merchants handle it in different ways. According to the CBRR, only the merchant of record is required to repay the consumer for the purchase of a gift card that has been frozen.

Some reseller sites have a 60-day guarantee on gift card funds. In these cases, they may issue refunds once they research the situation. If the site does not offer a guarantee, consumers can attempt to obtain their funds via a chargeback to the merchant. If a consumer purchased a gift card directly from a fraudster via a classified ad or online auction site those funds most likely cannot be recouped. Regardless of the legal liability, consumers will place the blame on the merchant that issued the gift card. So, while merchants are not required to re-issue funds on cards sold by a secondary source, it may be necessary to preserve the perception of a brand, especially if a cardholder threatens to post their complaint on social media.

Identifying Popular E-Gift Card Fraud Schemes

Understanding the methods used to perpetrate gift card fraud is the first step in identifying fraudulent gift card purchases on your own website. The most common is creating a new account or logging in as a guest and making a single purchase using a stolen credit card number. While the information provided by gift-card buyers is minimal, some indicators of this “straight across” fraud are:

- New or invalid e-mail addresses or e-mail domains
- Nonsensical purchaser and/or recipient names (e.g., “hjgewte qojkjdahds”)
- Purchaser and recipient have the same name and/or e-mail address
- Generic or standard gift message that hasn’t been personalized
- Gift message that does not make sense (e.g., “Happy Valentine’s Day” in June)
- Several credit cards were used and declined prior to a successful purchase
- Same IP or device ID used to buy several gift cards in one day

Another common fraud tactic used to purchase e-gift cards is account takeover. Typically, fraudsters use login credentials stolen in a data breach from another source. Based on the fact that most people use the same password and username over and over again, that usually gives them access to multiple retailer accounts. This enables them to bypass most standard fraud tools that only look at new accounts making gift card purchases. Once logged into an account, fraudsters will either use the credit card on file or a stolen card to create a purchase making the order appear legitimate to many fraud systems.

Merchants that have stored value cards attached to customer accounts are especially susceptible because fraudsters can transfer that value to an account created by the fraudster or simply change the email address and send themselves the value in an e-gift card. In May 2015, a journalist uncovered this very situation occurring on the Starbucks mobile app.

Some indicators of account takeover for gift card fraud are:

- Multiple login attempts on user accounts
- Login and purchase activity happening too fast to be accomplished by a human
- Purchaser e-mail is changed when purchasing an e-gift card
- Larger purchases inconsistent with previous user history
- Logins performed from location and/or device inconsistent with previous user history

E-Gift Card Fraud Prevention Doesn't Have to Mean Sales Prevention

Fraud targeting e-gift cards has grown significantly in just the last few years, so many companies are finding themselves in a reactive position. Some e-commerce companies have set restrictions on e-gift card sales to prevent fraud, but that also hinders legitimate purchases. A few of these restrictions include:

- Placing limits on the gift card value (e.g., not allowing e-gift card purchases in excess of $50 each via their website)
  - Downside: In these cases, fraudsters simply adapt their behavior, purchasing four $50 e-gift cards, instead of one $200 e-gift card. In addition to these fraudulent sales now blending in with legitimate sales, this also can result in lost sales of legitimate gift cards
- Not allowing e-gift cards to be delivered through social media websites
  - Downside: When a purchaser provides a social media address or handle for the recipient, this actually provides more information to be used to determine the legitimacy of a transaction. With the increased use of social media and less reliance on e-mail by millennials, choking off this channel could deter a sale, causing the purchaser to go to another retailer that does offer this solution.

- Require manual reviews performed on all e-gift card orders over a certain dollar value
  - Downside: Fraudsters are constantly testing the system to figure out specific risk thresholds of each merchant. It won't take long before they figure out that they need to place an order under a certain amount to avoid manual review. Additionally, one of the appealing qualities of e-gift cards is the ability to send a gift almost immediately. Whether it's a last minute birthday gift or an employee incentive to be rewarded for daily performance, consumers expect e-gift cards to be delivered within a short period—not to be tied up for days.

Best Practices and Strategies for Preventing E-Gift Card Fraud

Not all prevention strategies are able to reduce fraud without negatively impacting legitimate sales of e-gift cards but merchants have found ways to reduce loss from e-gift card fraud.

- Most importantly, e-gift card purchases should go through the same fraud checks as all other orders. However, they should go into a separate queue with rules specific to e-gift card purchases and behavior.
- The rules engine and/or fraud prevention tool used to assess the risk of each transaction should apply to all payment methods, in all markets and on all channels, including mobile. If there is a way to get around risk assessment, fraudsters will find it.
- Rely primarily on automated fraud systems to enable fast delivery of e-gift cards. Should manual review be needed, however, do not send e-gift card information to the recipient until a transaction is approved.
- Place more senior review analysts, who have strong knowledge of both good and bad customer behavior, in the e-gift card queue. Keep the same group of analysts responsible for this queue so they become experts in this type of fraud. Expect to have these analysts focused only on gift cards in the days leading up to major gift-giving holidays.
- When reviewing e-gift card orders, think of the recipient's e-mail address as the shipping address and consider using an e-mail address verification tool to determine if it has been used for a long time, or was just created for the purpose of ordering gift cards.

- Look for consistent patterns of behavior across gift card purchases that are either confirmed fraud at the time of purchase or result in chargebacks. Ensure that the behavior is applied to the fraud rules engine to keep the fraud prevention process automated, decreasing the manual review volume.
- Work with the customer service department to have a consistent policy and standard messaging when communicating with these consumers. It also may be deemed necessary to have messaging on your website specifically stating your company will only guarantee the funds of gift cards purchased directly through your company or any licensed distributors. This will not only serve as a deterrent, but also provide a point of reference for your customer service to provide the consumer when explaining policies.

It is important to prevent this type of fraud before the e-gift card is ever issued. If that is not possible, catching the fraud before it is redeemed should be your fraud team's next priority. If you are unable to prevent e-gift card fraud prior to the transaction being finalized, it is still important to attempt to identify the fraud and cancel the gift card. Unlike fraud on hard goods, if funds on a gift card are recovered, the loss to the company can be greatly reduced. If a gift card is purchased for $100 and goes through, but an analyst confirms the fraud before the funds are spent, that entire $100 can be recovered, making the chargeback similar to a refund to the cardholder, without the additional loss of the cost of goods or services.

This can become a cat-and-mouse game as fraudsters attempt to transfer funds on gift cards quickly, and often have buyers of gift cards lined up even before they purchase the item on a stolen credit card. Merchants have reported that having this process as a second level of fraud prevention, however, has been successful in recovering funds. Merchants speculate that fraudsters have so much volume in e-gift cards that they just don't have enough time to drain the funds on all cards in a timely manner. But also, if the fraudulently purchased e-gift card is sold on the secondary market, the funds most likely will remain on the card for some time because some sites confirm the funds are on the card before buying them. If a merchant is able to recover the funds during this time, the chargeback will not result in a loss as the funds being disputed will have been recovered.

Conclusion

The e-gift card market has grown at a rate of 175 percent over the last three years and is showing no signs of slowing down. It is imperative that merchants selling them have a comprehensive risk strategy in place that does not hinder legitimate purchases. The incentive to prevent the fraudulent purchase of these cards and to recover the funds on the gift card before they are redeemed is high: each fraudulent transaction will cost the company at least $2.27 for every dollar lost. Additionally, if your company's chargeback rate threatens to exceed one percent, not stopping these chargebacks before they occur can lead to fines from the card brands.

The tools you need to combat e-gift card fraud already exist—perhaps you employ them for other types of CNP fraud, however specific focus and balance of dedicated personnel are required to control this treacherous type of fraud while still reaping the benefits of a comprehensive gift card program that takes advantage of all sales channels.

About Chargeback.com

Chargeback is an industry leader in Chargeback Monitoring, Responses and Alerts. Their solution offers the only chargeback dashboard and reporting tool that's already integrated with ecommerce platforms and payment gateways. The solution enables automated and comprehensive Responses that recover lost revenue from chargeback fraud as well as Alerts from issuing banks to protect merchant accounts from a high chargeback ratio. For more details about Chargeback, visit https://chargeback.com, follow the company on LinkedIn and Twitter or call +1-888-808-8447.

About CardNotPresent.com

CardNotPresent.com, part of the RELX Group, is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. The company's media platforms include the CardNotPresent.com portal, the hub for news, information and analysis about the payments issues that most affect merchants operating in the space; the CNP Report, an e-newsletter delivering that focused information directly to your email inbox twice a week with no extraneous clutter; the CNP Expo, an annual gathering of the leading companies in the space from the smallest e-commerce Websites and technology providers to global retailers and payment processors; and the CNP Awards, an annual event honoring the products and solutions CNP merchants rely on most to increase sales. For more information, visit www.CardNotPresent.com.

This document was produced as a joint effort between CardNotpresent.com and Chargeback.com.

CNP CardNotPresent.com®
THE INDEPENDENT SOURCE FOR ORIGINAL CNP NEWS

Chargeback