



A Strategic Guide for Digital Gift Card Profitability



Gift card sales reached a staggering \$140 billion in 2016, and are projected to reach \$180 billion in 2018. While physical gift cards comprise the majority of sales, digital gift cards are growing at a rate of 200 percent compared to 5 to 6 percent growth for their physical counterpart. While this seems like good news, there are a number of stark realities associated with gift cards, particularly digital gift cards.

Digital gift card fraud is rising dramatically. Radial data shows digital gift card fraud attacks more than doubled from 2015 to 2016 and then quadrupled from 2016 to 2017. The sheer velocity of delivery and instant monetization make digital gift cards an attractive and lucrative target for cyber criminals. Higher risk innately instills increased caution, potentially creating higher false positives and negatively impacting legitimate customers as well as the brand. Finally, more fraud potentially means more chargebacks impinging on accepted thresholds, which could adversely affect a merchant's ability to accept payments not only for digital gift cards, but also across the board. And with false positives and chargebacks comes a hit to a merchant's bottom line. According to Javelin Strategy Research, false positives and chargebacks consumed an average 2.8 percent of digital merchant's total revenue in 2017.

While each of these threats could have dire consequences, eCommerce merchants can counter them with the right digital gift card fraud management strategies. This guide breaks down four actionable strategies that drive digital gift card profitability and mitigate risk especially when implemented holistically.

According to Javelin Strategy Research, false positives and chargebacks consumed an average 2.8 percent of digital merchant's total revenue in 2017.

A photograph of two women sitting at a desk, looking at a laptop screen. The woman on the left is holding a credit card and has a surprised or concerned expression. The woman on the right is looking at the screen with a thoughtful expression. The image is overlaid with a semi-transparent teal color.

Strategy 1: Make digital gift card order conversions a priority.

While this may seem like an obvious strategy, order reject rates for digital gift cards are higher than reject rates for physical goods. On the surface this makes sense since digital goods, by their very nature, pose a higher risk for fraud. However, order conversion is tied to a number of factors that many retailers lack such as big data, advanced fraud management systems, and human expertise. And these inadequacies are amplified for digital goods with order conversions suffering, a higher incidence of false declines and chargebacks, which are up 25 percent and 60 percent respectively over 2016, and a bigger blow to the bottom line.

Big data matters

Digital gift cards are the perfect fast fraud scenario. Fraudsters purchase one or hundreds of digital gift cards using stolen credit cards, synthetic identities, or bots. They sell these cards on marketplaces, to criminal rings globally, or use the cash to purchase goods they resell (doubling down on fraud). Speed is on their side, making it difficult for retailers to stop the fraud before it occurs. This is exacerbated when merchants rely only on their own proprietary transactional data, negative list and limited data elements to screen for fraud. Given the sophistication of today's cyber criminals and their use of malware, VPNs and virtual machines to disguise their location and device, it doesn't take long to find and exploit weaknesses. By the time a merchant realizes it has been victimized, it's too late. The money is long gone.

And what happens when a new and legitimate customer attempts a digital gift card purchase? Will the transaction be automatically flagged as high risk, or worse, systematically rejected because there is no known data in the merchant's database? The simple fact is, any retailer that is conducting digital gift card fraud management using limited data is setting itself up for failure. High-risk transactions require big data, as in billions of records across a multitude of merchants, to establish a deep-seated foundation that can be leveraged in real-time to stop digital card theft in its tracks, while also converting a higher number of orders.

An advanced fraud management system backed by fraud experts is a must

Just as limited data constricts a merchant's ability to accurately screen for fraud and improve conversions, the same is true for the tools deployed to automate the screening process and hold only the riskiest orders for manual review or not at all. Relying on a single tool such as proxy

detection or email verification can easily be circumvented by fraudsters. Even the most widely implemented tools like customer order history and card verification number become vulnerable, especially considering the massive data breaches that occurred in 2017.

Advanced fraud management systems employ a layered approach that addresses each stage of the purchase path, which results in higher order conversions. Equally important, a layered approach makes it more difficult for fraudsters to compromise fraud detection systems, frustrating criminals before they can wreak havoc. Survey findings by LexisNexis show that eCommerce companies that invest in a multi-layered approach, including advanced identity and fraud transaction verification & authentication, experience 65 percent fewer successful fraud attempts.

While big data and layered fraud management are key to automatically approving the highest percentage of orders and creating a frictionless customer experience, people are also critical. Fraud tools based on machine learning have come a long way in recent years, and that maturity, along with the significant uptick in online fraud, has driven the proliferation and popularity of these tools. However, given the higher risk of digital goods, it isn't enough to rely solely on machine learning. Some level of human intervention will always be needed to manually review the riskiest orders, analyze trends – of which there are many – and adjust rule sets accordingly to thwart future attacks. Without this human touch, order conversions suffer, revenue is thrown away, good customers are insulted, and the opportunity to protect the business from future attacks is lost.

The fraud management tools, staff, and systems all add up to big bucks. That expense, coupled with lower than average conversion rates, should give any merchant pause, which takes us to the next strategy.

Survey findings by LexisNexis show that eCommerce companies that invest in a multi-layered approach, including advanced identity and fraud transaction verification & authentication, experience 65 percent fewer successful fraud attempts.

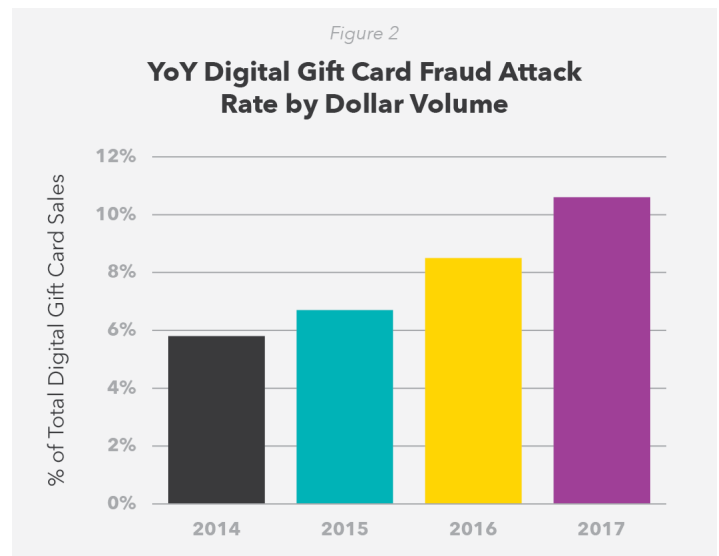
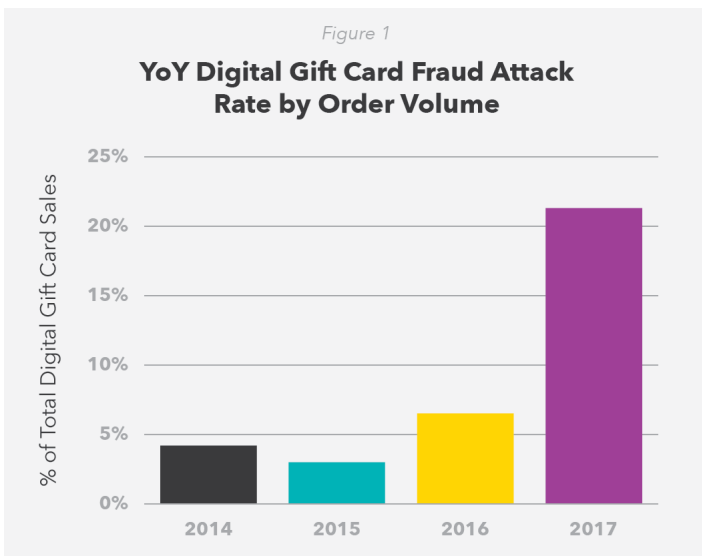


Strategy 2: Invest in a solution that fully indemnifies digital gift card risk.

The goal of digital gift cards is to give customers flexible purchase options that translate into higher eCommerce revenue for merchants. So why would any merchant subject a high-risk transaction to a fraud management partner that does not indemnify for fraud? It's like purchasing an exotic car with no warranty.

However, if that partner is simply providing a tool that a merchant manages itself, then not indemnifying makes sense – at least for the partner. It wouldn't be in the partner's best financial interest to indemnify something they don't have direct control over. On the flip side, shouldn't a fraud tool partner provide some level of guarantee regarding the robustness of their tool as it pertains to digital goods? It's a conundrum. Merchants that elect to handle fraud management for their digital gift card program on their own are not only exposing themselves to elevated risk, they are also relinquishing the opportunity to transfer that risk and financial burden to a third party.


And the elevated risk is real. Figures 1 and 2 show year-over-year fraud attack rates as a percentage of total digital gift card sales by order and dollar volume respectively. Clearly attacks are on the rise.



EMV was mandated in October 2015, but adoption was slow as merchants struggled with compliance costs and the complexity of adoption. In fact, the fraud attack rate on order volume actually dropped in 2015 as fraudsters continued to focus on card-present transactions before the EMV October deadline. Despite the slow adoption rate, fraudsters felt the card-present squeeze in 2016 and shifted their attention online. As a result, digital gift card fraud attacks increased significantly with 2016 attacks by order volume more than doubling (3.0 percent in 2015 compared to 6.6 percent in 2016). The dollar attack rate also increased but not as dramatically as the order volume attack rate, largely due to a 35.8 percent decrease in the average order value (AOV) of the 2016 attacks—\$120.00 compared to 2015's attack AOV of \$187.00.

By 2017 however, the EMV roll out had taken hold with CPI Card Group reporting 85 percent of consumer credit cards had been issued with a smart chip, dramatically impinging on fraudsters' ability to commit counterfeit card-present fraud. This dramatic shift in EMV adoption is reflected in the significant increase in digital gift card fraud from 2016 to 2017. Attacks by order volume grew a stunning 222.7 percent as fraudsters pounded the digital world with high-velocity automated attacks using stolen data fueled by massive data breaches. Dollar fraud attacks also rose, but continued the 2016 trend of lower transaction values with attack AOV dropping 120 percent to a four-year low of \$59.

For merchants, this data should be a wake-up call. The sophisticated techniques and the velocity of attacks and monetization make it far too risky for merchants to manage fraud on their own. Every merchant that offers digital gift cards should be looking for a fraud management partner willing to take on fraud liability. That willingness to indemnify is a strong indicator the solution provider has the technology, people and expertise to make a digital gift card program profitable for both parties.

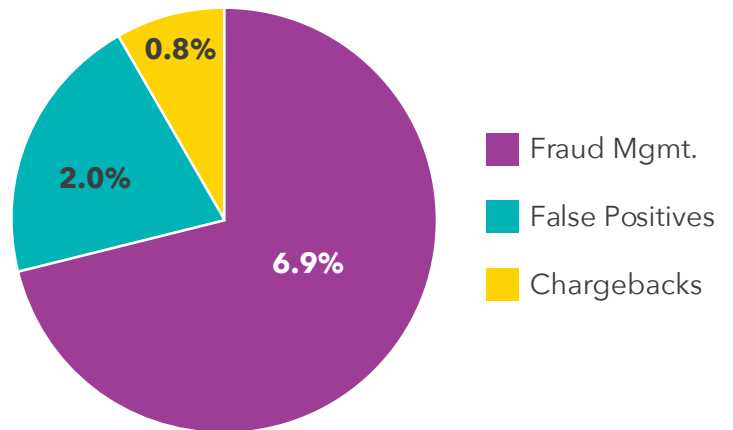


Strategy 3: Lower your fraud management operational costs.

Fraud management, chargeback losses, and false positives are all negatively impacting a merchant's bottom line and the impact is growing.


According to Javelin Strategy Research, digital goods merchants lost 9.7 percent of revenue on average to fraud, an increase of 13 percent from 2016. Of the 9.7 percent revenue loss, 6.9 percent is attributed to fraud management with false positives and chargebacks eating the remaining 2.0 percent and 0.8 percent respectively. In addition to eroding the largest share of revenue, fraud management – investments in technology and personnel – consumes 25 percent of a digital merchant's operational budget and 75 percent of total fraud costs, triple the actual fraud losses themselves.

Fraud Costs as a % of Revenue



With fraud management costs and revenue losses rising year over year, merchants need to weigh the pros and cons of in-house fraud management versus outsourcing all, or at the very least, the high-risk transactions. And the reasons are straight forward. Digital transactions are more complex, higher velocity and instantly monetized – traits that dictate a more comprehensive range of risk mitigation tools and processes as well as a greater number of highly skilled fraud management specialists.

Bottom line: a digital merchant with \$400 million in annual revenue is losing \$38.8 million to fraud costs. This could be slashed by outsourcing with a third-party that replaces the fraud costs with a transaction fee for approved orders only, converts more orders as a result of big data and sophisticated tools, performs manual reviews on only the riskiest orders, and also indemnifies fraud.



Strategy 4: Increase revenue share of every digital gift card sold.

Don't be resigned to paying premium rates for digital gift card fraud management. While there may be an expectation to pay more for high-risk opportunities, if a merchant partners with a fraud provider that is experienced in high-risk markets, then that provider should not put the full burden of financial risk on the merchant by charging premium rates in addition to not indemnifying fraud. That's just eating into profits. Therefore, it's important for merchants to assess options in the market by asking fraud providers the right questions because the responses to these questions are explicitly linked to the profitability of every transaction.

What is the fraud provider's average conversion rate for digital gift cards?

Part of this conversation should cover data, systems, processes, and people. Does the provider use a consortium of data? Do they have comprehensive tools to confirm the legitimacy of a transaction? Can their rule sets be changed in real time? Are they staffed with data scientists, manual review and trend analysts? All of these factors drive higher conversions. Keep in mind approval rates can fluctuate so it's important to look at the big picture – approval rates and attack rates. However, the average annual order approval rate will be a good indicator of a provider's digital gift card prowess. Merchants should partner with an experienced provider rather than be part of the provider's digital gift card learning curve.

Do they indemnify fraud?


Unless a merchant is an expert in digital gift card fraud, or is under the misconception fraud and false positives aren't a problem for the business, indemnification is essential for high-risk transactions. If a merchant is engaged with a fraud partner that doesn't assume the fraud liability for digital gift cards, at the very least, the merchant should consider fraud screening alternatives for its high-risk transactions. Quite simply, making indemnification a priority delivers an instant lift to digital gift card profitability.

Is their fee structure the same for physical goods and digital goods?

This question is tricky. Everyone needs to make a profit, so a provider may charge more for high-risk transactions particularly if they are indemnifying fraud. If they aren't indemnifying, the rate should be standard across physical and digital goods – even if they are managing fraud for a merchant, and definitely if they are just providing a tool the merchant manages itself. Merchants should also understand if they are paying for every transaction or only the orders that are successfully converted. Given the higher order reject rate for digital goods, this is a very important consideration. If a merchant is paying for every transaction and 25 percent of the orders are rejected, the converted orders just became less profitable. Merchants should also compare fee structures across multiple providers and look for hidden fees or caveats that protect the provider and not the merchant. A gap in basis points should not be the only consideration.

What is the integration process and how long does it take?

Finally, merchants need to think about the ease of integration, how long it takes, and the time and resource allocation needed to support the integration. A long and complex integration eats away time to revenue and overall return on investment. Look for simple APIs and pre-launch test sand boxes to cut time to market.



Bottom line, fraud management may not be a one size fits all. While some tools and providers may be very good at general eCommerce transactions, high-risk transactions are more challenging and it's the merchant who ultimately pays the price. With the popularity of digital gift cards and the associated fraud steeply on the rise, it's time to give digital gift card fraud protection the due diligence it warrants. Every merchant that offers digital gift cards should be looking for ways to increase conversions, shift fraud liability, lower operational costs, and improve the profitability of every transaction. The results will be profound.

About Radial Fraud Protection

Radial brings more than 15 years of experience and 24x7x365 resources that work in concert and adjust in real time to ensure cyber criminals don't get the upper hand. We are committed to our clients' success including indemnifying fraud – even for high-risk markets – and only charging for approved orders. Flexible options allow merchants to leverage the solutions that best meet the needs of their organization whether it's for complete fraud management for all orders, fraud management for high-risk orders only, or a risk rating to supplement a merchant's existing tool set. We are obsessed with fraud so merchants don't have to be.

Contact us:

sales@radial.com

1-877-255-2857
