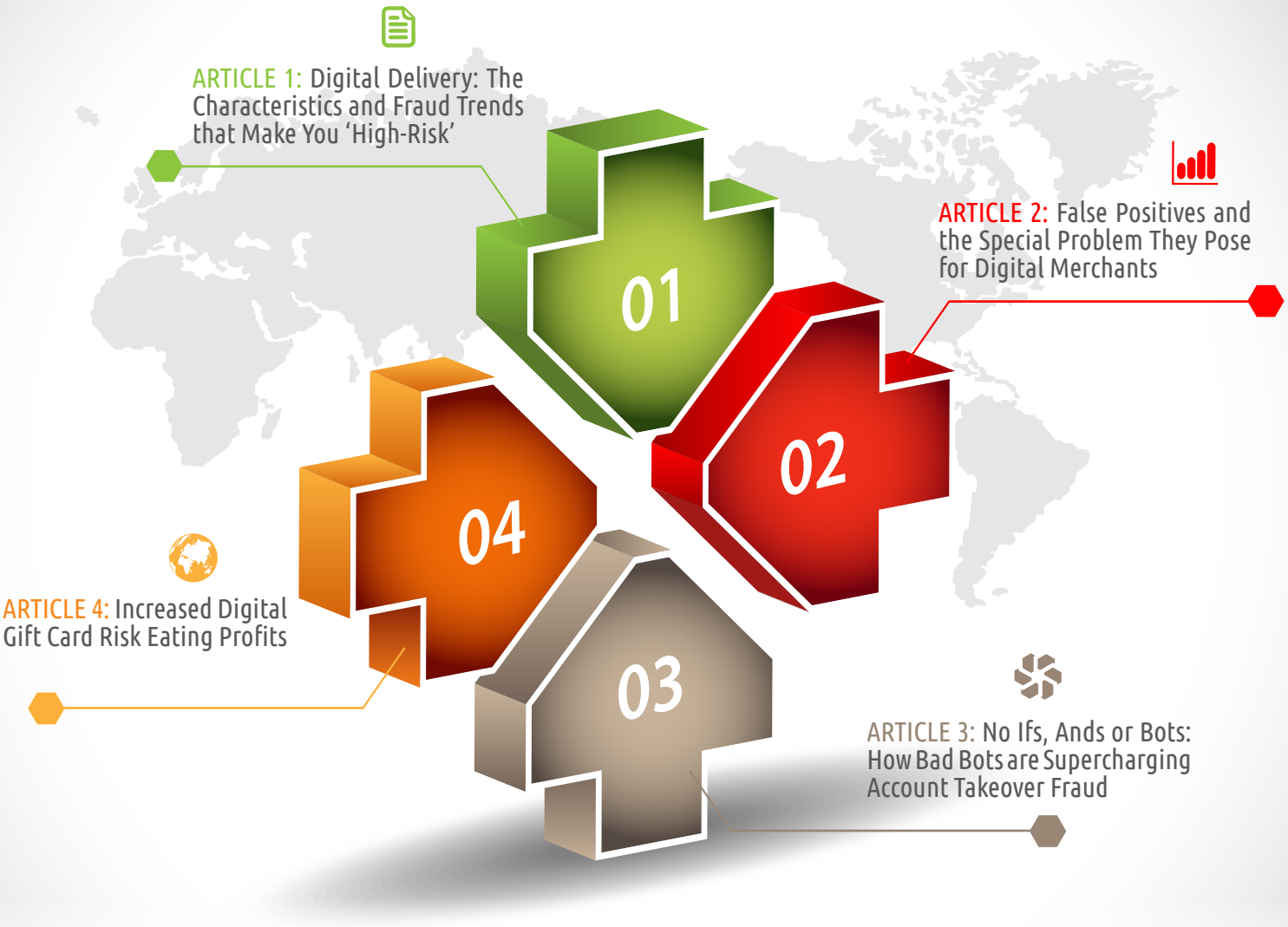
THE CNP REVIEW

Topics, trends, tips and best practices to drive your business forward. | Card Not Present®

Q2 2018: WHY DIGITAL DELIVERY IS SO RISKY



CNP CARD NOT PRESENT®
NEWS, EDUCATION AND EVENTS
DECODING DIGITAL PAYMENTS & FRAUD

Radial


DJ Murphy

At Card Not Present, continuous dialogue with our community has given us a unique perspective on the payments and fraud issues that affect the entire range of online merchants. The CNP Review is a compendium of the most important payments and fraud issues facing merchants today. Each quarter, in cooperation with a partner, we will examine one aspect of our world in four in-depth pieces covering the trends and challenges driving that issue.

Our Q2 2018 edition of the CNP Review looks at the increased risk of digital delivery. In addition to providing a new way to shop, eCommerce created a new way to deliver goods: digitally, via the Internet. Airline tickets, music, gift cards, games, hotel reservations and more can all be purchased online and received in digital form. But the convenience of instant delivery comes at a price: increased risk of fraud. The inaugural CNP Review examines some of the recent issues facing merchants in these verticals and some practical ideas to mitigate those elevated risks.

DJ Murphy
Editor-in-Chief
Card Not Present®

Digital Delivery: The Characteristics and Fraud Trends that Make You 'High-Risk'

All fraud prevention professionals eventually understand that the type of fraud a given company experiences depends on many factors including: price point, target customer, resale value and business model. However, the biggest factor is whether a merchant deals in physical or digital goods. Digital products present challenges for fraud fighters that can put their business at higher risk for several pernicious fraud types.

Delivery of a physical good requires a physical address. In order to monetize fraud in the case of physical goods, a fraudster has to possess the item, which requires shipment to a valid address. A shipping address is one piece of information that can be analyzed to identify a fraudulent transaction—a piece that digital merchants don't get to leverage.

Digital delivery companies also face another challenge: instant fulfillment. They don't have the luxury of two or three days between purchase and delivery. Typically, customers expect items like event tickets, travel arrangements, video game content or e-gift cards instantaneously. Fraudsters also rely on this quick delivery to purchase digital goods with stolen credentials, and then resell the goods to a buyer that is typically lined up in advance.

Because the stakes can be elevated when fraud occurs in these high-risk verticals, it's important to know what types of fraud to watch out for. Here are several that can pose serious problems for merchants active in these industries:

TRIANGULATION

Triangulation is the term used to describe when a fraudster buys something from a company with a stolen credit card and resells it to an unsuspecting consumer. Sometimes goods are purchased up-front and resold on third-party marketplaces or auction sites. In other cases, a fraudster will purchase the item only after a consumer expresses interest. For instance, a fraudster may purchase several e-gift cards to a popular company and resell them for a discounted price. But, for travel bookings, they will post an advertisement for reduced travel and place the order for flight and/or hotel in the consumer's name, but on a stolen credit card. They typically receive payment from the consumer through digital wallets or peer-to-peer money transfer services.

The biggest challenge with triangulation is when merchants suspect fraud and cancel the transaction before the unsuspecting consumer has used the good or service. Often, consumers don't realize they purchased stolen products, expecting fulfillment of the item they purchased. This creates a customer service issue for the merchant when the consumer tries to board the flight, attend the concert or use the gift card. Should merchants fulfill the item anyway, to avoid negative publicity and a negative customer experience, or advise customers that purchases are guaranteed only when they are made directly through your company?

This decision should be made internally, but should factor in the average cost of goods, website messaging and how often this occurs. Having a strong internal strategy for handling these situations, not deviating from them often and working with internal stakeholders are vital. These strategies will help your company avoid chaotic one-off situations, and eventually, consumers will adapt to the policy.

ACCOUNT TAKEOVER

Account takeover used to be a problem mostly for banks, but it has become a top concern for eCommerce fraud professionals in all verticals. As merchants began enabling faster checkout for customers who established an online account and kept a card on file, fraudsters began to see the benefits of hijacking those accounts. As data breaches yielding login/password combinations proliferate, online gaming, event ticketing, content streaming, and other digital-product sellers are at risk of account takeover.

Fraudsters can leverage stolen login credentials to take over an online account and make purchases they can resell or drain the account of any items that have value (e.g., gaming credits or loyalty points). They also can use the account for its legacy value, allowing a fraudster to make a purchase on a stolen credit card on an account that has already been verified.

Similar to triangulation, the victim in this scam is an unsuspecting consumer, whose account has been compromised. If the account is canceled or suspended, the legitimate consumer won't be allowed to make purchases or access the items or content stored on their account. If an account is drained of value or the card on file is used for a fraudulent purchase, merchants need to have a strategy for addressing the situation.

To create the best prevention and management strategy, it's important to identify how accounts are being taken over and what they are being used for. Consider verification products to better validate users beyond passwords. Stronger authentication, deploying device ID technology, or requiring additional information when a new card is added or a new device is attempting to make a purchase or log in to an existing account can all be helpful in controlling account takeover fraud.

CARD TESTING

Card testing fraud is common for companies that have a lot of low-dollar (below $20) transactions. Content streaming, video games with in-app purchases, inexpensive subscription services and online domain services are all common targets of this fraud method.

Typically, the entity or person who obtains fraudulent payment information is not the same person or entity making fraudulent purchases. Sellers of stolen payment cards can make more money if they are still active (i.e., not canceled by the consumer or issuer). They verify that by using the card in a low-dollar transaction prior to selling it. They aren't interested in the fulfillment of a product, but instead just need a positive authorization—usually for thousands of stolen card numbers. These purchases can quickly add up, resulting in a spike in chargebacks or in fraud reports that reflect negatively on the merchants and could eventually lead to fines or suspension of a merchant account if not controlled. Susceptibility to card testing is one reason sellers of digital products could be deemed "high risk."

A large volume of low-dollar transactions for memberships or inexpensive digital items can indicate a business is being attacked by card testing. Placing velocity limits on e-mail addresses, IP addresses, device IDs or phone numbers and the time between orders can help control this issue. Most bulk card testing is done using bots running on a script. Disrupting this process by randomly moving the placement of the checkout button or other fields will essentially "break" the script, but won't impact a legitimate customer.

CONCLUSION

By identifying the type of fraud you are most commonly seeing on your platform, you can establish a strong fraud prevention strategy. For digital delivery companies, the speed of the decision and action is important. Companies that are able to cancel fraudulent orders prior to fulfilling them take away the incentive for fraudsters to continually target the business.

Layering automated tools and processes to verify or cancel suspicious orders will help reduce the likelihood of all these fraud types. Even with prevention mechanisms in place, however, fraudsters will test them to see if they are easily overcome, so it is important to continually measure and study the methods they are using.

Internal fraud prevention should be a continual battle, not implementing technology and waiting for it to thwart bad guys. As companies implement strategies and technologies that make it more difficult to defraud them in these ways and remain vigilant, the fraud attempts should start to decrease, making these issues more manageable.

False Positives and the Special Problem They Pose for Digital Merchants

Fraud prevention is often compared to a game of whack-a-mole: You stop one fraudster only to have another pop up in a different place. You have to be on your toes at all times, mallet at the ready. Merchants hope to become proficient enough at the game to stop most of the fraudsters and mitigate their losses.

But this portrayal of fraud prevention leaves out a key factor: false positives. A more accurate picture of fraud prevention is that of a more nuanced game of whack-a-mole, one where many of the pop-ups are not really "moles" at all, but legitimate customers trying to make a purchase. Merchants know it's a problem: Nearly 70 percent of merchants say they are concerned about their fraud prevention incorrectly targeting legitimate customers[1]. And, they know that delaying, declining or canceling an order can result in the immediate loss of the sale in question and, more importantly, subsequent sales to a customer who, out of frustration, turns to a competitor—maybe for life.

Merchants have only a small window of time to figure out whether this is a fraudster or a customer and act accordingly. Some merchants, however, are at a distinct disadvantage in this arena.

DIGITAL VS. PHYSICAL: WHICH IS MORE AT RISK?

A physical-goods merchant often can verify a purchase in the time between the placement of the order and its shipment (up to several days, in some cases). Digital-goods merchants, on the other hand, don't have the luxury of that extra time; their customers expect immediate delivery of their product. What's worse, due to the nature of their products, they have fewer data points to determine if a transaction is legitimate. And of course, their customers don't differentiate between digital and physical goods. Regardless of the product, that transactions go through quickly and without interruption are table stakes to consumers. They assume those things will happen every time they purchase something online and only notice when they don't.

As a result, it comes as no surprise that digital goods merchants run a significantly higher risk of declining a legitimate transaction. A 2017 study shows that while an average of 17 percent of declined transactions by physical goods-only merchants are false positives, that number jumps to 22 percent for eCommerce merchants that sell digital goods.[2]

What that number does not measure could be even more important. The effect declines have on the lifetime value of a customer can be significant.

A 2018 analysis by Radial of customers who returned to a merchant's site after being declined due to a false positive found that the customer not only shopped less frequently, but also spent less per order. The result was a 68 percent lower lifetime value per year, per customer. And that's for the customers who came back; many simply didn't return. It also says nothing of the impact of word of mouth when a rejected customer shares their experience with family and friends or on social media.

POWER OF PARTNERSHIP

How, then, can digital goods merchants both reduce fraud and prevent false positives?

For many companies, it's difficult to achieve on their own—but they can partner with someone who can. This is the recommendation of Al Pascual, Senior Vice President of Research and Head of Fraud and Security at Javelin Research and Strategy. According to Pascual, "for merchants generally, unless you're among the largest, this is not only a distraction, it's an almost impossible challenge. Seeking out security vendors to manage some of this is really going be the most effective way for merchants to navigate the problem."

Pascual notes that many of the fraud tactics merchants have been battling in the past year or two—for instance, automated credential stuffing attacks leading to account takeover fraud—have plagued the banking industry for years.

"The catch for merchants [is], they're not banks," he says. "Banks are going to have much more experience with security, technology, and managing fraud risk, [and] they're going to have larger budgets dedicated to this."

The security vendors who have been working with banks to find solutions are now offering those solutions to merchants, and it could be their lifeline. Pascual also recommends that merchants look seriously at security vendors who offer a guarantee.

"It's a simple way for merchants to deal with the problem: [The vendor] makes the decisions, and you're isolated from the fraud risk."

With credential stuffing and other automated attacks, the sheer volume of traffic—typically thousands of fraudulent attempts per month—makes false positives inevitable for a digital-goods merchant. Fraud management vendors experienced with these automated attacks know the signs. It's their full-time job to track emerging fraud trends and quickly and accurately adjust the sensitivity of their rules, identifying and isolating fraudsters in real time while minimizing false positives.

Techniques such as identifying the IP addresses of potential fraudsters and screening user behavior via embedded Javascript on the merchant's page can be used to isolate fraud. Users who are from a particular IP address or range of addresses, and who are exhibiting known automated styles of behavior, like lots of tabbing and very quick entry of usernames and passwords, can be flagged and sink-holed. "Sink-holing" refers to the redirecting of suspected fraudulent traffic to an unused server, or a server that is not meant for legitimate customers. With the threat isolated, legitimate customers can make their purchases, never having encountered extra friction or onerous security measures, and merchants can focus on improving and growing their business knowing their customers' data is secure.

Of course, credential stuffing is just one example of what merchants are dealing with, and this is where the technology behind a provider's platform comes into play. In addition to knowing what to look for, vendors have advanced technology to keep their antifraud tactics current. This, Pascual says, is key for digital goods merchants in particular:

"When you start talking about transactions at scale, with less data than you get in physical goods, then having a machine make those decisions allows you to adapt more quickly than a person," he explains. "You need some way to deal with transactions that are happening very fast, products delivered very quickly, and fraud schemes that can also change very quickly. So a lot of the vendors that are successful in the space have a machine-learning capability, and you're going to see more of that [going forward]."

So for digital goods merchants, the best way to win at the fraud prevention whack-a-mole game may be simply to hand the mallet to someone else.

1. The 2018 Global Fraud and Identity Report, Experian
2. 2017 LexisNexis® True Cost of Fraud Study, LexisNexis Risk Solutions

No Ifs, Ands or Bots: How Bad Bots are Supercharging Account Takeover Fraud

The role bots play in online fraud has expanded significantly during the past year. One study[1] called 2017 the "year bad bots went mainstream." In and of themselves, however, bots are neither good nor bad. They are simply tools their operators use to automate repetitive tasks on the Internet. But, several of those repetitive tasks enable some very pernicious fraud types and, once programmed, the bots are exceptionally easy to operate. Merchants in the last year—especially those in travel, online gambling and some retail sectors—have seen how bad bots can significantly contribute to credential stuffing, resulting in account takeover fraud.

Why have bots become part of the story of eCommerce fraud? It begins with the thousands of data breaches that have compromised the payment and/or personal information of billions of consumers worldwide. Hackers have made oceans of stolen information available for sale to anyone with the inclination and moral flexibility to take advantage of it. There is *so* much information yielded in breaches, however, that a means to winnow it down to the most valuable pieces became necessary.

JUST A LINK IN THE FRAUD VALUE CHAIN

As perpetrating fraud has become more lucrative, it has taken on many of the characteristics of legitimate business, including industrialization and specialization. Hackers no longer steal information and use it to commit fraud themselves. They don't even sell it to the end users. Many links in a fraud value chain have been forged to process the raw data into a form that can be more easily leveraged for monetization—each link taking its financial cut. In one of those links, bots have become the tool of choice that criminals use to wring every dollar they can from the data.

The number of data records stolen in a breach can range from tens or hundreds of thousands to hundreds of millions or even billions. Increasingly, the most targeted records are not payment card accounts, they are email addresses and passwords that can be used to access the online accounts of unsuspecting consumers. And, because people reuse username/password combinations across many different accounts, one stolen login could give a criminal access to more than one account.

Given the massive amount of information contained in an average hack, going through it manually to validate useable credentials would not be feasible. Enter bots. The recipient of bulk data wants to validate the username/password combinations on as many sites as possible. So they load up specially programmed bots (created by still other members of the fraud value chain—another specialty) with the thousands or millions of stolen credentials they purchased on the Dark Web and attack sites around the Internet.

The bots then engage in credential stuffing—automatically testing those credentials to see which accounts they can successfully log into. The credential stuffer then sells the smaller list of valid account credentials (either individually or in chunks) for much more than they paid for the original bulk list.

QUANTIFYING THE BAD BOT PROBLEM

Using bots to validate stolen credentials—a necessary precondition for account takeover fraud at scale—has become an important marker and attack type that companies must find a way to identify. In November of 2017, there were 8.3 billion login attempts on sites using Internet content delivery network provider Akamai's platform. Of these, an analysis by the company[2] determined that 3.6 billion were malicious—the vast majority of which were generated automatically by bots testing credentials.

"In other words," the report said, "43 percent of all logins seen by Akamai were attempts to log in to an account using password guessing or account details gathered from elsewhere on the Internet."

Certain types of companies are especially likely to be targeted by bots with malicious aims. Of the top six industries that experience the highest percentage of bad bot traffic on their websites, four are in the business of providing products or services that require at least some level of digital delivery, according to another recent report.[3]

Traffic generated by bad bots accounts for more than 53 percent of all visits to online gambling sites, more than any other merchant vertical, the report said. Airlines, ranked second at 44 percent, and ticketing sites (fifth at 23 percent) bracket financial sites and healthcare as the industries with the most bad bot activity as a share of total traffic. eCommerce retail ranked just behind ticketing, with more than 21 percent of activity on those sites originating from bad bots.

Bad bot activity is not restricted to credential stuffing (e.g., gambling, airline, ticketing and eCommerce all experience price scraping by competitors via bots), but it is a significant activity and leads directly to account takeovers.

THE GREAT ATO CONFLAGRATION

If the proliferation of online accounts—meant to benefit customers by reducing friction at checkout—is the fire pit, and the information stolen in data breaches is the wood, then automating the process of testing large numbers of credentials across thousands of websites is the lighter fluid that has turned account takeover fraud from a campfire to a wildfire.

According to one analysis, account takeover attacks in the fourth quarter of 2017 were 182 percent higher than they were during the same period a year earlier.[4]

For digital delivery merchants, the ramifications are clear. When fraudsters take over accounts they can drain them of any stored value (cash winnings, loyalty points, airline miles, gift card balances, etc.), or they can make purchases using the card on file required to establish the account and sell those goods for profit.

Bots have had a significant impact on making account takeover fraud available to the masses. Fraudsters no longer need the specialized knowledge of hackers and coders. They just need valid login credentials and the willingness to use them to steal. Both the information and the individuals are in plentiful supply, thanks to bots.

CONCLUSION

Account takeover fraud, like all fraud targeting online merchants, is becoming more sophisticated and difficult to detect. The bad bot attacks enabling ATO are an example of fraudsters raising the bar and they require a response.

For high-risk, digital-delivery merchant verticals like gambling and airlines suffering from account takeover fraud, initiating an organizational dialogue about bots is vital. Solutions designed to identify and manage malicious Web traffic generated by bots are an increasingly important part of defending businesses against ATO and can be employed as part of a layered defense against fraud.

1. 2018 Bad Bot Report: The Year Bad Bots Went Mainstream, Distil Networks
2 . Q4 2017 Akamai State of the Internet Report, Akamai Technologies
3. 2018 Bad Bot Report: The Year Bad Bots Went Mainstream, Distil Networks
4. Q4 2017 Cybercrime Report, ThreatMetrix

Increased Digital Gift Card Risk Eating Profits

When it comes to digital gift cards, merchants face a double-edged sword. On one hand, digital gift card demand is growing at a rate of 200 percent, sending a clear message to merchants that consumers value this purchase option. On the other hand, fraudsters love them too. So much so, digital gift card fraud doubled from 2015 to 2016 and then quadrupled from 2016 to 2017, according to Radial data. Combine this increase in fraud with higher false positives and more chargebacks, it's no wonder digital gift card profitability is being squeezed.

With margins already thin even without these added pressures, every merchant offering digital gift cards needs to regain control with the right strategies to make every legitimate transaction more profitable.

Radial's report, ***A Strategic Guide to Counter Digital Gift Card Fraud***, details four actionable strategies to make this a reality.

1) PRIORITIZE ORDER CONVERSION

The sheer velocity of delivery and instant monetization make digital gift cards an attractive and lucrative target for cyber criminals, and therefore, a high-risk purchase option for merchants. This higher risk innately instills increased caution, creating higher false positives as merchants struggle to balance risk and order conversions. In fact, false declines are up 25 percent over 2016. However, because order conversion is tied to several factors that many retailers lack such as big data, advanced fraud management systems, and human expertise, these inadequacies are amplified for digital goods.

Any merchant 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.

Just as limited data is constricting, the same is true for inadequate fraud tools. 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 to improve conversions. Equally important, a layered approach makes it more difficult for fraudsters to compromise fraud detection systems, frustrating criminals before they can wreak havoc.

In fact, eCommerce companies that invest in a multi-layered approach, including advanced identity and fraud transaction verification and authentication, experience 65 percent fewer successful fraud attempts. [1]

2) INVEST IN A SOLUTION THAT INDEMNIFIES FRAUD

According to Radial data, digital gift card fraud attacks have 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. This is 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. 2017 followed suit with attacks by order volume growing 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 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 look for a fraud management partner willing to take on the 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.

3) LOWER FRAUD MANAGEMENT OPERATIONAL COSTS

Fraud management, chargeback losses, and false positives are all negatively impacting the bottom- line and the impact is growing. Digital goods merchants lost 9.7 percent of revenue on average to fraud. Fraud management consumed 6.9 percent of that loss. 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.[2]

With fraud management costs and revenue losses rising year over year, merchants must 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 straightforward. Digital transactions are more complex, have a higher velocity, and are 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.

4) INCREASE REVENUE SHARE OF EVERY LEGITIMATE ORDER

It's important for merchants to assess options in the market by asking fraud providers the right questions, because the answers are explicitly linked to the profitability of every transaction.

What is the fraud provider's average conversion rate for digital gift cards? This will be a good indicator of a provider's digital gift card prowess. 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 these factors drive higher conversions.

What is the provider's fee structure and do they indemnify for fraud? Do they charge for every transaction or only the orders that are successfully converted? If they charge for every transaction and 25 percent of the orders are rejected, the converted orders just became less profitable.

Bottom-line, high-risk markets come with their own set of challenges, which means fraud management may not be a one size fits all. When implemented holistically, these four actionable strategies are a compass for digital gift card profitability.

1. 2017 LexisNexis® True Cost of Fraud Study, LexisNexis Risk Solutions
2. 2017 Financial Impact of Fraud Study: Exploring the Impact of Fraud in a Digital World, Javelin Strategy & Research

About Card Not Present

Card Not Present®, 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 CardNotPresent.com.

About Radial

Radial is a leader in omnichannel commerce technology, payments and fraud, and operations, enabling brands and retailers to profitably exceed customer expectations. Radial's solutions connect supply and demand through efficient omnichannel technologies, fulfillment and transportation options, intelligent fraud, payments, and tax systems, and personalized customer care services.

Hundreds of retailers and brands confidently partner with Radial to simplify their post-click commerce and improve their customer experiences. Radial brings flexibility and scalability to their supply chains and optimizes how, when, and where orders go from desire to delivery. Learn how we work with you at www.radial.com.