Radial 2018 Fraud Index

Radial

2016 was a banner year for eCommerce growth and 2017 followed the same upward trend. That's good news for retailers. But with that growth also came an uptick in online fraud, largely due to more widespread EMV adoption, massive data breaches and the sheer sophistication of cyber criminals. That's very bad news for retailers, especially those that manage fraud themselves and as a result, bear the financial liability for all fraudulent transactions.

Data scientists in Radial's Fraud Technology Lab analyzed transactions from hundreds of clients and billions of data elements to create Radial's Fraud Index. The Index addresses five trends every retailer should be mindful of.

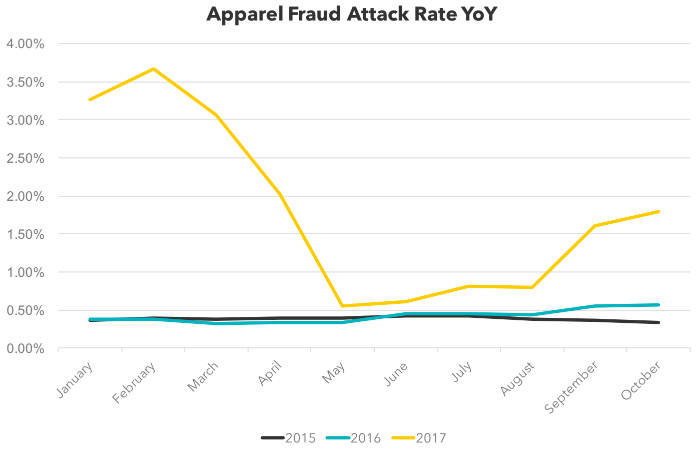
Trend 1: Card-Not-Present fraud continues to rise with some market segments more vulnerable than others but the blame does not lie solely with EMV.

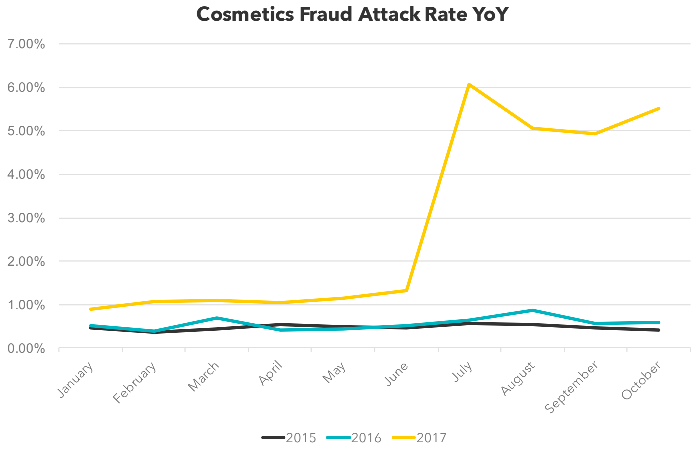
The web contributed nearly 42 percent of the growth in the U.S. retail market in 2016, representing 11.7 percent of total sales. Card-Not-Present (CNP) fraud also saw similar growth at 40 percent, impacting 3.4 percent of consumers in 2016 versus 2.4 percent in 2015, according to Javelin Strategy and Research. Javelin also said in the June 2017 study that eCommerce merchants are losing 8 percent of their revenues to fraud, up from 7.6 percent reported in a similar survey last year.

Logic alone tells us more online sales means more online fraud regardless of EMV. However, we do know that EMV has contributed to the influx of online fraud because criminals, like water, will always find the path of least resistance. There is also well documented historical evidence from nations that took the EMV plunge years before it was mandated in the U.S. Combine that, with the fact that more than half of consumer credit cards have been issued with smart chips (85 percent according to CPI Card Group) and about 60 percent of debit cards are EMV-ready, there's no doubt EMV is forcing a percentage of CNP fraud as criminals shift to the safer online haven.

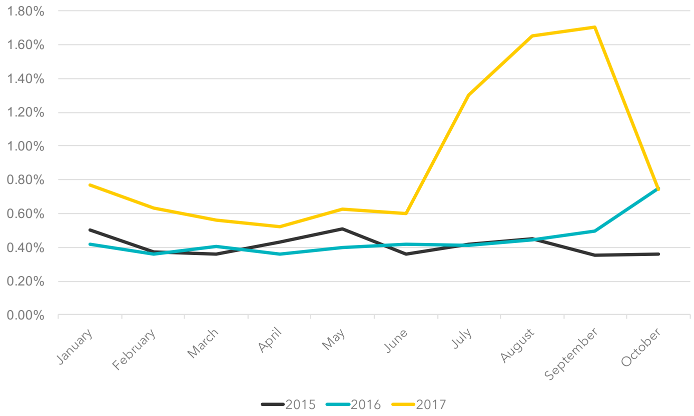
According to Radial data, 2017 saw fraud attacks soar more than 400 percent in the cosmetic segment versus 2016. Apparel wasn't far behind with more than a 4 times increase in attacks followed by a 2 times increase in the electronics, home and entertainment segments. Interestingly, footwear saw a drop. However, for 2015 through 2017 footwear attacks hit their highest attack rate in June year-over-year. The only exception was in 2017 where attack rates peaked in both June and October.

The charts below show the growth in fraud attacks rates across market segments for January through October of 2015–2017. Clearly, fraud attacks are up across the industry as a whole. This should put retailers, especially those in segments with the greatest threats, on high alert.

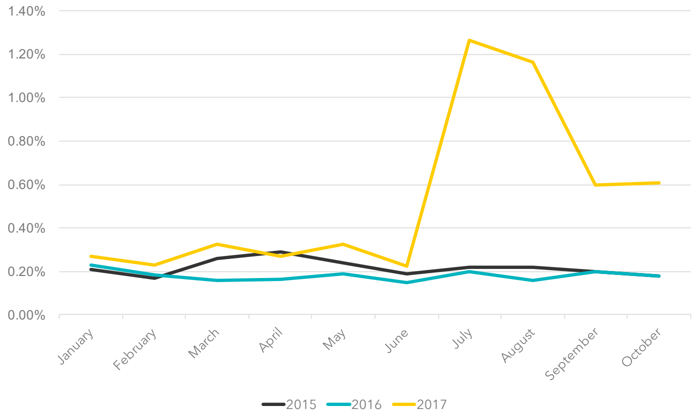




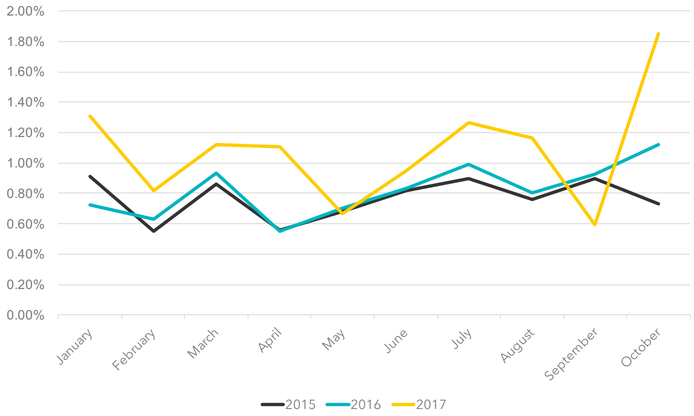
Entertainment Fraud Attack Rate YoY



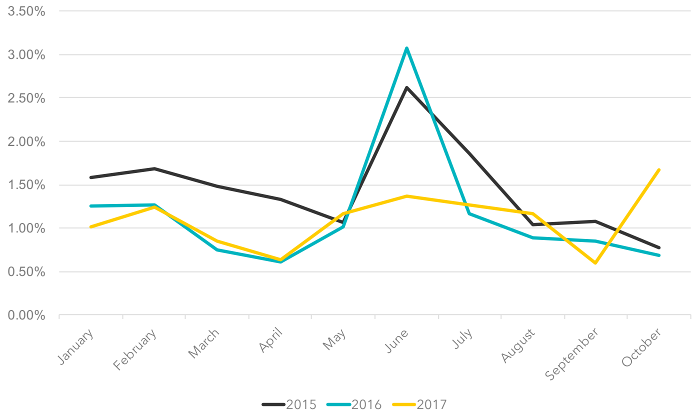
Home Fraud Attack Rate YoY



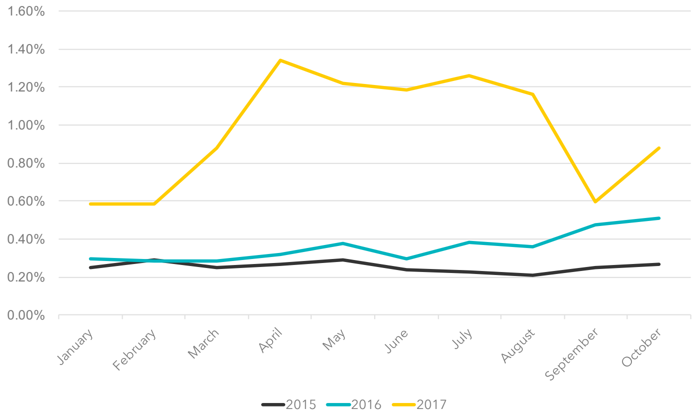
Jewelry Fraud Attack Rate YoY



Footwear Fraud Attack Rate YoY



Sporting Goods Fraud Attack Rate YoY



But there are other factors of influence beyond EMV. The next trend looks at data breaches and how criminals wreak havoc for months if not years after a breach occurs (especially when breaches go unreported).

Trend 2: Data breaches are igniting fraud attacks with 2017 reporting the highest number of breaches since tracking began.

The number of U.S. data breaches tracked in 2016 hit an all-time record high of 1,093, according to Identity Theft Resource Center (ITRC) and CyberScout (formerly IDT911). This represents a 40 percent hike over the near record high of 780 reported breaches in 2015. As of September 2017, 1080 breaches with 171 million records exposed had already been reported – a 375 percent increase in exposed data over 2016. And the news gets worse.

Today's fraud attacks are done with tomorrow's reported breached data. Because breaches are often not discovered or reported until months after the breach occurred or sometimes not at all, criminals have the time and tools to amplify the damage long before businesses and consumers take action. And depending on the data, this damage can have long-term impact. Equifax, one of 2017's worst data breaches started in mid-May and wasn't discovered until the end of July ultimately compromising identity information of 145.5 million U.S. consumers including: names, social security numbers, addresses, birthdates, and for some, driver's license numbers.

Figure 1

Data Breaches & Fraud Attack Rates

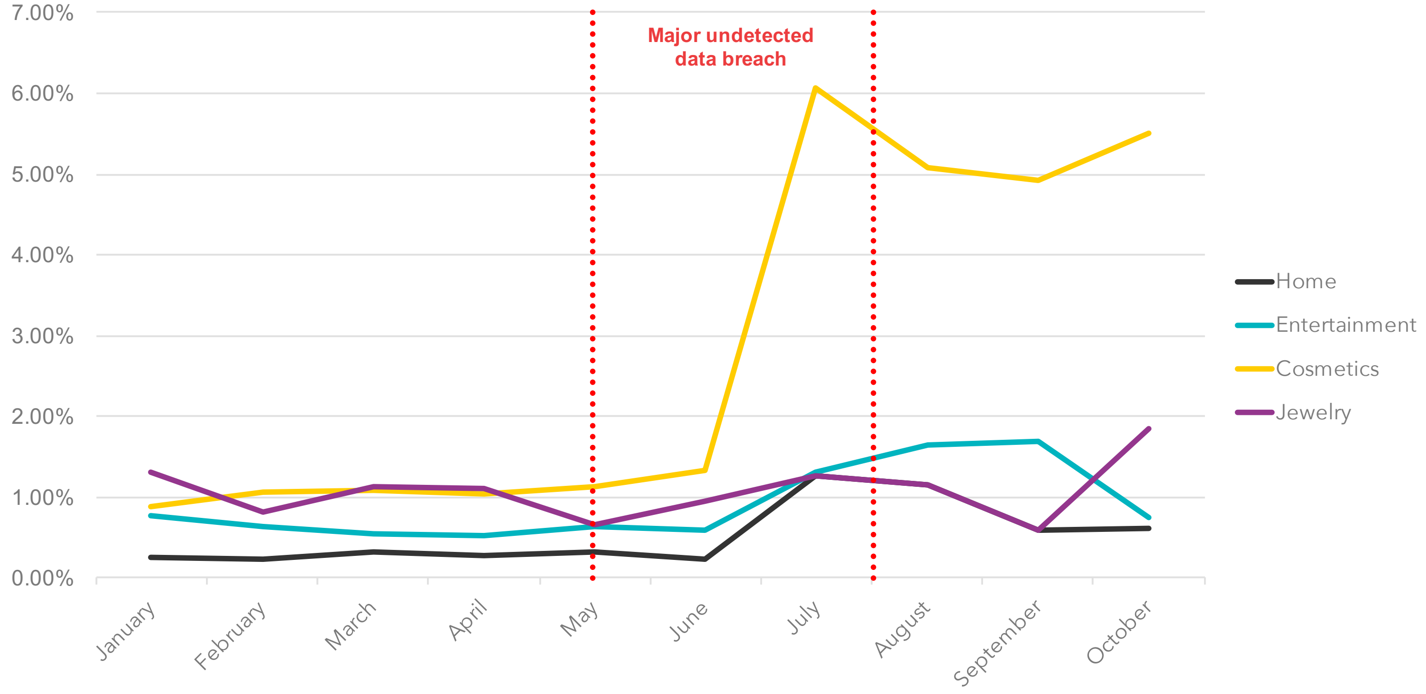
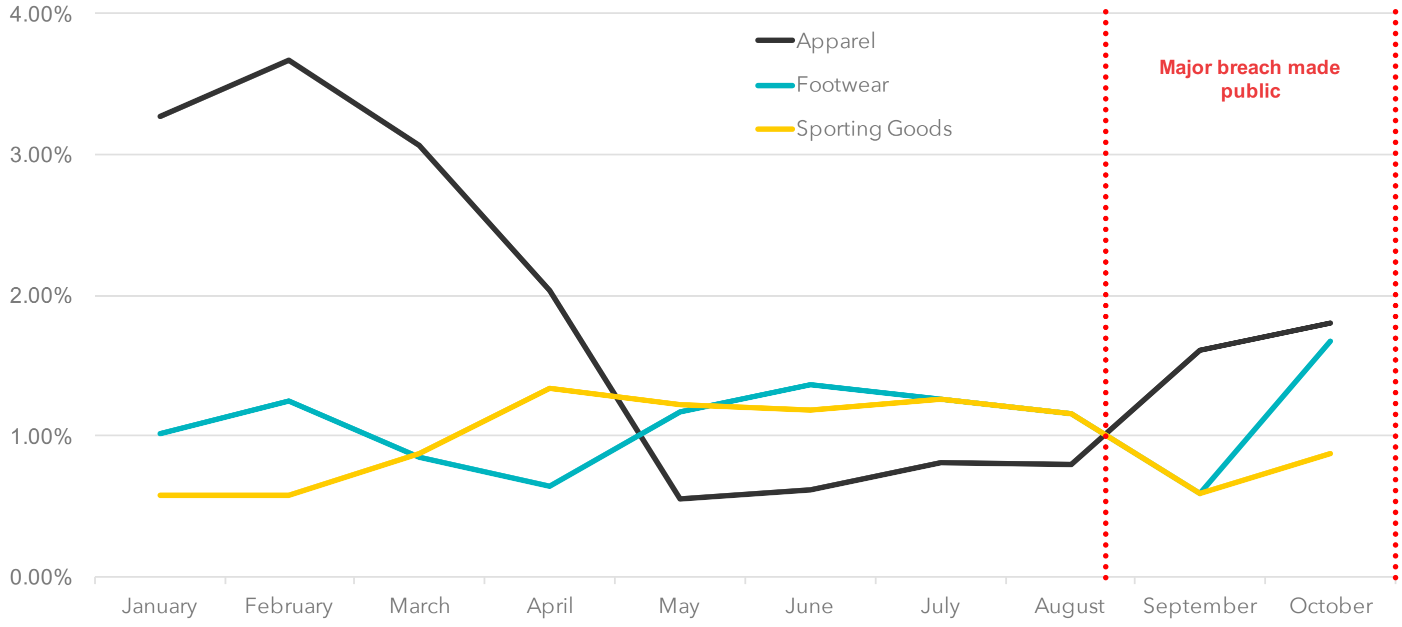


Figure 1 shows a significant uptick in fraud attacks across four separate market segments coinciding with this same time period. While we can't state with absolute certainty this mid-year breach was solely responsible, the size alone of the breach makes it less than coincidental. Also interesting is the noted decrease in fraud attacks in these same four markets when the breach was made public in September and the subsequent attack rate increase shown in Figure 2 in three new markets as fraudsters shifted their focus.

Figure 2

Data Breaches & Fraud Attack Rates



For retailers that manage fraud on their own and rely solely on machine learning, breaches present a serious threat – one they can't react to quickly – making them an easy target for fraudsters.

And let’s not forget consumers

One of the most disturbing things about data breaches is the inaction taken by consumers to improve the security of their online accounts. After all, how many of us use the same password for multiple accounts? A closer look at the ramifications of this very consequential consumer practice exposes just a few of the ways criminals use it to their advantage.

Armed with login information purchased on the dark web following a data breach, fraudsters can easily hijack additional consumer accounts. They can place orders, have them shipped to the address of their choice and then resell the merchandise. The consumer is none the wiser until they discover a credit card charge that they dispute, and now the burden of proof lies with the retailer. This is a repeatable and prolific process for fraudsters that can go undetected for months all due to password recycling by consumers.

In addition, criminals leverage good factors from multiple accounts to create synthetic identities that don’t trigger any negative flags during fraud screening. They place orders, apply for new credit cards and fly completely under the radar until the compromised customers realize they are victims. At this point, customer service starts getting calls, customers file chargebacks, manual reviews go up, customer friction increases, and the snowball effect of the breach spreads exponentially throughout the retailer’s organization. Bottom line — the ramifications of password recycling are mind boggling.

And it’s not just the ability to make fraudulent retail purchases.

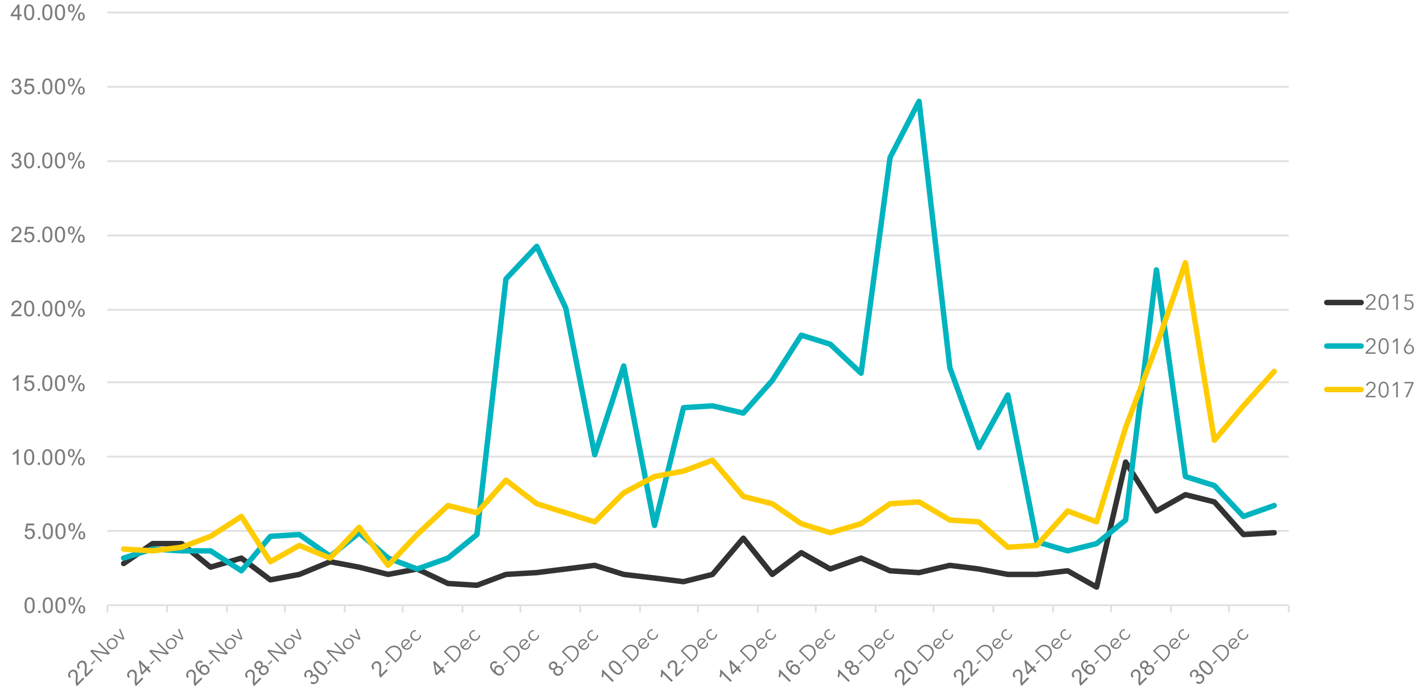
What if fraudsters use that recycled login information to access bank accounts, file fraudulent tax returns, or set up false seller accounts on popular marketplaces? In fact, this year’s data breach goes beyond that with fraudulent mortgages and student loans being targeted along with the typical fraudulent retail activity. With data breaches on the rise, retailers and consumers alike need to make security a top priority.

Trend 3: Digital gift cards steadily increase in risk YoY showing on average a four times increase in fraud attacks from Thanksgiving to Christmas over 2015.

Digital gift cards remain a popular target for fraudsters as they take advantage of the surge in order volumes during the holiday season to mask their criminal intent. Figure 3 shows a dramatic increase in fraud attack rates in 2016 and 2017 peak seasons versus 2015. While the average number of attacks overall aren't as high in 2017 (7.3 percent) compared to 2016 (10.7 percent), they are still significantly higher than 2015 (3.1 percent).

Figure 3

Digital Gift Card Fraud Attack Rate YoY

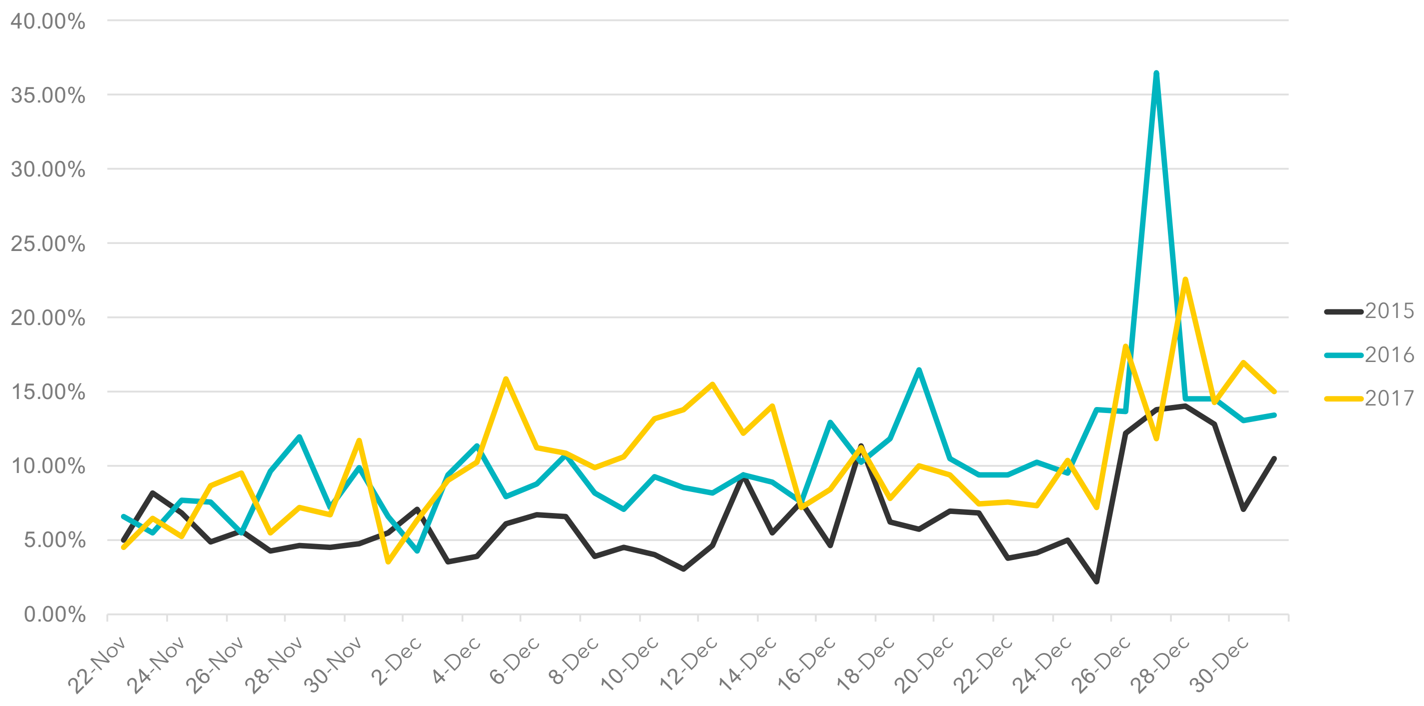


Fraud attacks ramp up sharply in 2016 as early as December 5 and maintain an average attack rate of 17.2 percent through December 22 when average attack rate counts drop sharply to 4.1 percent December 23 through December 25. By contrast, for the same time periods in 2017, the average attack rates were 6.79 percent and 5.39 percent. Despite the fact that fraud attack counts were lower in 2017, they had a greater impact financially with an average dollar volume attack rate of 10.9 percent compared to 9.7 percent in 2016.

Figure 3 also shows a dramatic increase in attack rate counts post December 25 for both 2016 and 2017. However, the attacks in 2017 were more prolific – 60 percent higher than 2016 from December 26 to December 31. Overall, the average year-over-year attack rate counts for 2016 and 2017 were four times higher than 2015. With e-gift cards becoming more and more popular especially during the holidays, retailers need to be on high alert not only during season, but year round.

Figure 4

Digital Gift Card $ Volume Fraud Attack Rate YoY



Taking a closer look at the data in Figure 4, the beginning of the season started out relatively calm with Thanksgiving on November 24, and 23 for 2016 and 2017 respectively tracking only slightly higher than Thanksgiving (November 26) 2015. But that track shifted dramatically as the 2016 and 2017 seasons progressed. In fact, the average fraud attack rate by dollar volume from Thanksgiving through Christmas in 2017 was nearly 75 percent higher than 2015. While the average dollar attack rate for this same time period in both 2016 and 2017 nearly mirrored each other (9.35 and 9.42 percent respectively), we do see 10 days (December 5 to 14) of sustained attacks in 2017 that are significantly higher than 2016. The key takeaway from this data is the unpredictable nature of attacks, especially in high risk areas, reinforcing the need for expert fraud management.

Figure 5

YoY Fraud Attack Rates

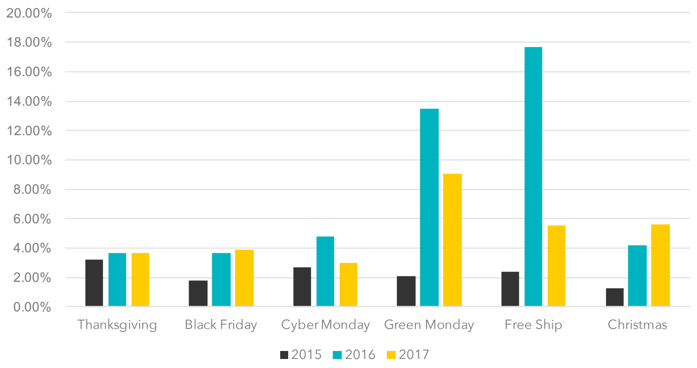
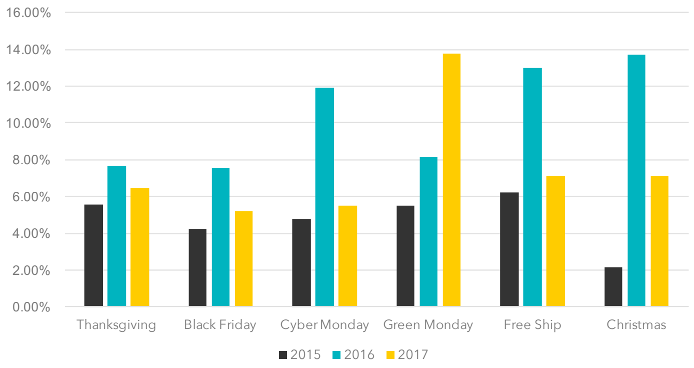


Figure 6

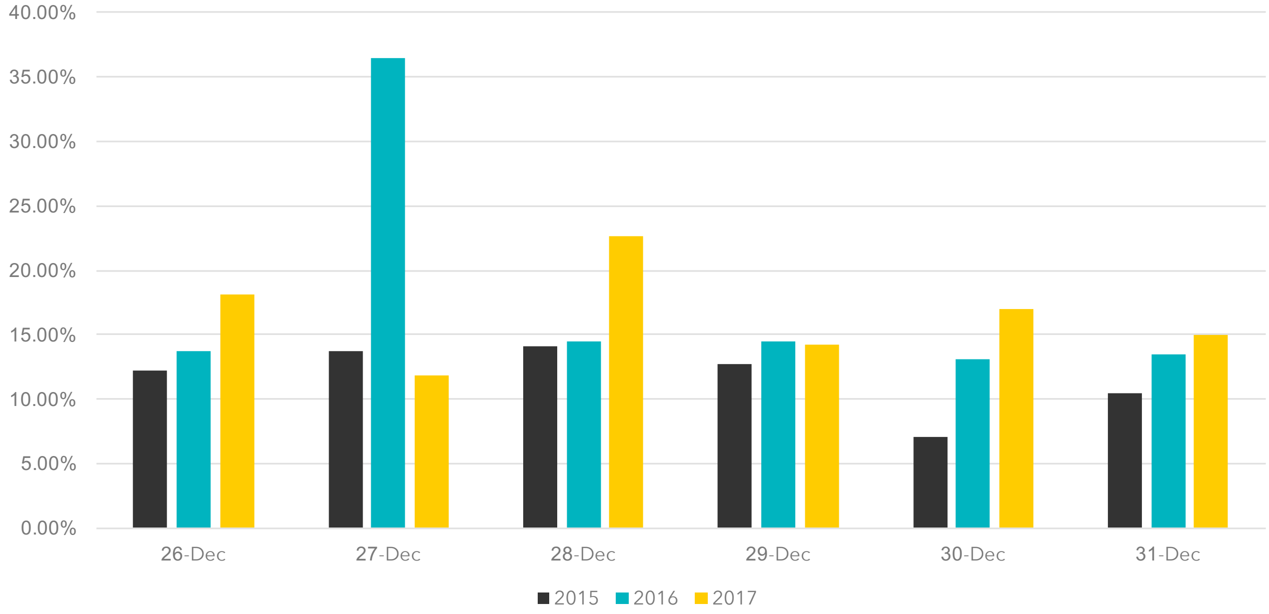
YoY Dollar Volume Fraud Attack Rates



Looking at key days during the season, Figures 5 and 6 show fraud attack rates by order count and dollar volume respectively. 2016 and 2017 exceeded 2015 on every day. Although even fraudsters take time off to celebrate the holiday, the attacks they did execute on Christmas day were significantly more jarring from a financial perspective than 2015. Figure 6 shows a dollar attack rate of 13.73 percent in 2016, a staggering 535 percent higher than the 2.16 percent dollar attack rate in 2015. 2017 fell nearly in the middle at 7.12 percent, 230 percent higher than 2015.

Figure 7

Post Holiday Gift Card $ Volume Fraud Attack Rates



Finally, fraudsters come back with a vengeance year-over-year following Christmas as they take advantage of the surge in returns and post season bargain hunters. Figure 7 shows dollar volume attacks hit the highest of the entire season on December 27, 2016 at 36.5 percent. Similar results, although lower, were seen in 2017 when dollar attack volumes hit a season high of 22.59 percent on December 28. However, the average dollar attack rate for 2017 and 2016 from December 26 to December 31 were only a percentage point different at 16 percent and 17 percent respectively largely a result of 2017 seeing a surge in average attack counts of 15.5 percent compared to 9.68 percent in 2016.

In short, retailers are caught in a conundrum: offer gift cards to keep good customers happy, but at the same time increasing the risk of fraud, or don’t offer gift cards thereby eliminating fraud risk, but at the same time creating fewer options for the customer.

The right choice is somewhere in the middle with an experienced partner that understands the digital gift card business and also assumes all of the risk.

Trend 4: Shipping and fulfillment methods carry different risk, but all areas saw an increase in attacks in 2017.

Surprisingly, fraud attacks were 2.5 times higher for ground shipments for the first three quarters of 2017 compared to 2016. Despite this increase, ground shipments carry the least financial risk when it comes to fraud – for every $211 of good orders shipped via ground there is a $1 of fraud attacks. In contrast, and not surprising, same day (e.g., digital gift cards) poses the highest financial risk – with every $10 of good orders comes a $1 in fraud attacks. Overnight shipping remains a favorite with fraudsters and the riskiest physical shipping method for retailers as evidenced by a $1 of fraud attacks for every $13.

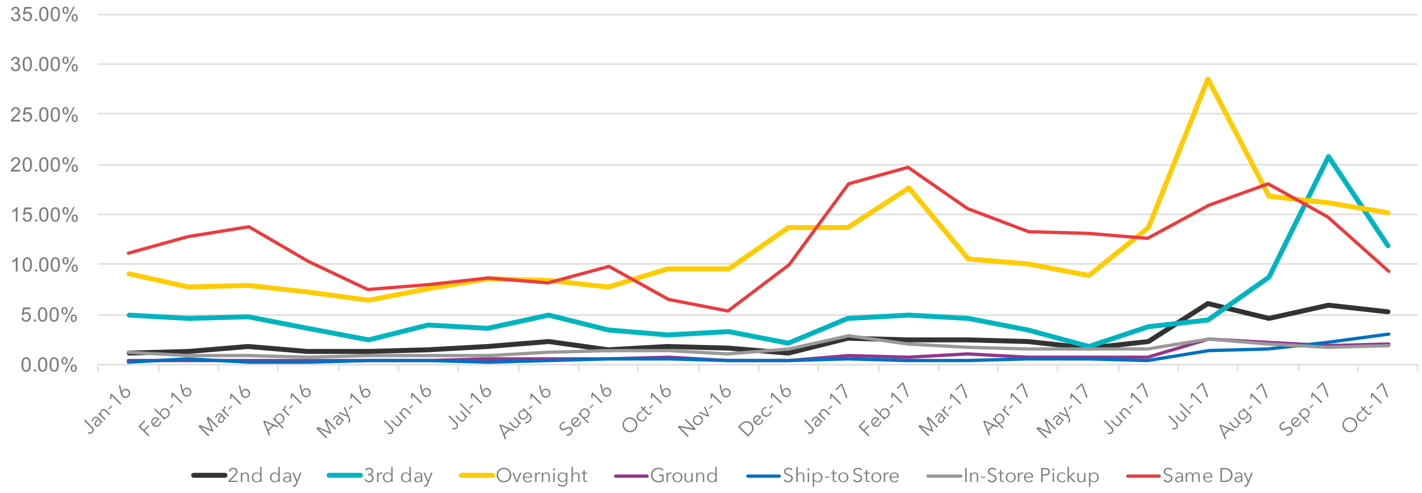
Figure 8

Q1-3 2017	Increase in Fraud	$1 of Fraud per Dollars of Good Orders Shipped
Ground	**2.5x**	**$211**
Expedited	**1.7x**	**$63**
Overnight	**1.7x**	**$13**
Online Gift Cards	**1.7x**	**$10**
Store Fulfillment	**1.8x**	**$128**

Figure 8 breaks down the numbers for different shipping and fulfillment methods including orders picked up in-store through an In-Store Pickup or Ship-to Store program. Let's face it fraudsters would rather remain behind scenes than risk getting caught in a store, but there are times when getting physical goods the same day works to their benefit. Although store pick up ranks fourth in terms of financial risk ($1 of fraud for every $128) among the shipping & fulfillment models, it is surpassed only by ground shipping for the highest increase in fraud attacks compared to 2016. As more and more retailers embrace store fulfillment as a means to increase revenue and customer loyalty, they will also be facing increased fraud risk they may not be equipped to deal with.

Figure 9

Fraud Attack Dollar Rate by Shipping & Fulfillment Method



Digging deeper, Figure 9 shows fraud attack rates climbed steeply during the 2016 holiday season for same day deliveries and overnight shipments as fraudsters want quick execution to receive and unload their goods during the frenzy of peak shopping. Interestingly, third day shipping comes in as the next highest contender for fraud attacks, as fraudsters try to disguise themselves among shoppers unwilling to pay expedited shipping fees.

The remaining shipping and fulfillment methods carry less risk but they show slow and steady activity making it more difficult for retailers to detect. Also quite noticeable is the spike in fraud attack dollars across every category mid-year 2017, which correlates with this year's worst data breach, showing once again the far reaching impact of online security breakdowns.

The message here is that retailers can't rely on screening for fraud in any one shipping or fulfillment category. Fraudsters change tactics often to remain under the radar. And while they may favor the quickest delivery method, particularly during the holidays, they also tap slower methods throughout the year.

Trend 5: Credit card BIN Country and IP Country are red flags for fraud with certain geographies representing higher risk internationally across market segments.

Many retailers avoid selling internationally due to the increased complexity of cross-border eCommerce and the perceived higher risk for fraud. However, cross-border eCommerce can be lucrative, and understanding the risks is essential to success. The tables below depict the riskiest countries for all international eCommerce volume by IP address and Bank Identification number (BIN) across apparel, home and entertainment market segments.

While there is a shift in the top five countries year over year, some countries, most notably Comoros, Brazil, and Mexico remain consistently riskier countries for both IP and BIN attack rates. Fraud attacks originating from these country's IP address dropped from 2016 to 2017, but the reverse was true for attacks originating from credit card BINS, with some exceptions. Many of these countries struggle economically. In fact, Brazil has been in economic crisis for the past few years, and Mexico continually deals with widespread corruption. While Comoros is making headway in improving its infrastructure and political stability, it is also still struggling.

IP Country Fraud Attack Rates for International eCommerce Sales

APPAREL				HOME				Entertainment			
2017		2016		2017		2016		2017		2016	
Brazil	9.38%	Comoros	9.91%	Comoros	9.77%	Comoros	13.27%	Brazil	10.97%	Brazil	13.66%
Comoros	6.80%	Mexico	7.14%	Hong Kong	2.21%	Venezuela	3.94%	Comoros	6.14%	Comoros	12.48%
Dominica	5.08%	Brazil	6.25%	Timor-Leste	1.91%	Mexico	3.17%	Dominica	5.87%	Mexico	4.79%
Mexico	4.74%	Venezuela	5.22%	Brazil	1.52%	Dominica	3.12%	Mexico	5.23%	Venezuela	3.16%
Jamaica	4.44%	Dominica	5.13%	Bassas da India	1.49%	Brazil	2.65%	Austria	3.14%	Ecuador	1.97%

BIN Country Fraud Attack Rates for International eCommerce Sales

APPAREL				HOME				Entertainment			
2017		2016		2017		2016		2017		2016	
Brazil	23.77%	Brazil	17.76%	Comoros	60.62%	Comoros	30.04%	Brazil	27.27%	Brazil	33.65%
Austria	8.75%	Comoros	10.21%	Brazil	8.05%	Austria	18.62%	Comoros	13.71%	Comoros	9.48%
Comoros	7.54%	Mexico	9.61%	Mexico	6.00%	Brazil	10.40%	Austria	9.37%	Austria	8.26%
France	6.37%	Austria	4.17%	Austria	5.29%	Mexico	9.06%	Mexico	6.89%	Mexico	6.96%
Gabon	5.66%	Taiwan	3.91%	Hong Kong	3.87%	Dominica	3.47%	Italy	4.66%	Gabon	3.93%

Drilling down further by vertical, fraud attacks originating with a BIN of Brazil increased more than 33 percent for apparel but decreased in both home and entertainment. This is common for most, but Comoros and Austria are the exceptions with two verticals increasing. Comoros doubled in home while increasing 44 percent in entertainment. Austria also doubled, but for apparel, while entertainment went up 13 percent.

The table below shows the countries by vertical with the highest attack rate by BIN and IP for all eCommerce volume within each country. Again, we see the usual suspects as well as some newcomers. While we see mostly temperate attack rates across the board, there are some rather disturbing callouts. Nearly 20 percent of eCommerce fraud in Italy's entertainment market segment was attributed to credit cards issued from that country's BIN, while nearly 30 percent of eCommerce fraud in Dominica originated from an IP address in that country. Even more startling is the amount of eCommerce fraud for cosmetics in Venezuela – nearly 75 percent – that originates from a Venezuelan IP address. And not to be ignored, French-based credit card BINs accounted for 21 percent of France's apparel eCommerce fraud.

Attack Rate of Country eCommerce Volume

Vertical	BIN Attacks		IP Attacks	
	Country	Attack Rate	Country	Attack Rate
Home	Mexico	3.24%	Timor-Leste	4.9%
	Brazil	2.42%	Brazil	2.9%
	Comoros	1.75%	Hong Kong	2.8%
	Hong Kong	1.01%	Bassas da India	2.3%
	Austria	0.95%	Comoros	2.2%
Entertainment	Italy	19.44%	Dominica	28.9%
	Austria	7.57%	Brazil	8.1%
	Brazil	6.74%	Austria	7.7%
	Comoros	3.09%	Mexico	3.0%
	Mexico	2.60%	Comoros	1.9%
Cosmetics	Senegal	15.94%	Venezuela	73.8%
	Taiwan	14.53%	India	32.4%
	Brazil	9.13%	Mexico	14.1%
	Argentina	4.54%	Taiwan	11.9%
	Comoros	1.12%	Comoros	1.2%
Apparel	France	21.08%	Jamaica	12.4%
	Brazil	7.85%	Dominica	6.7%
	Gabon	2.77%	Brazil	5.7%
	Austria	2.25%	Mexico	3.6%
	Comoros	1.20%	Comoros	0.7%

What does all this mean?

The surge in eCommerce sales and ultimately fraud is only going to continue. From a sales perspective that means more revenue for a retailer, but the revenue increase is intrinsically linked to how good a retailer is at stopping fraud. Based on the data in the Fraud Index, retailers need to be experts, but fraud management is really not where most retailers excel.

With more than 15 years of delivering fully outsourced and indemnified fraud solutions, our expertise and data tell us any retailer who is managing fraud themselves or relying on machine learning is losing money, customers and potentially putting their business at risk.

Fraud management takes people, processes, and technology that goes far beyond what today's tools can deliver.

Consider this real world scenario. Radial received a $9,000 order from a client's customer that had never shopped with any of our clients before. The billing address did not match the shipping address; the credit card was from the UK; the order was shipping overnight in the U.S.; the browser information indicated the person was in the UK and the AVS check failed. If we had relied solely on machine learning, this order would have failed the taste test on so many levels. Through enhanced investigative techniques, we learned the customer owns three homes, two in the U.S. and one in the UK. The order was approved – saving a high value customer, not to mention a high value sale for our client.

How would you have fared?

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.

Or contact us:
sales@radial.com
1-877-255-2857

Radial