a PYMNTS.com / FORTER collaboration

GLOBAL FRAUD ATTACK INDEX™

Second Quarter 2016

ATTACK INDEX

↑ 215%

↑ 11%

IN THE U.S.

Fraud attacks on U.S.
since the October 2015 Liability Shift

Q1 2015	Q1 2016
$1.89	$4.79

↑ 150%

Dollars at risk per $100 of sales

↑ 304%	Digital Goods
↑ 95%	Luxury Goods
↑ 37%	Clothing
↓ -17%	Electronics
↓ -36%	Food/Beverage

↑ 215%

Total Fraud

Change in fraud attacks by industry

Global Fraud Attack Index™

The Global Fraud Attack Index Snapshot

↑ 11%

Rise in fraud attacks since the October 2015 Liability Shift

3X

Attack Rate more than tripled between Q1 2015 and Q4 2015 (attack rate is percent of transactions subject to fraud attacks in Q4 2015 compared to Q1 2015)

$4.79

$4.79 out of $100 of sales are at risk (based on five product categories considered)

Up $2.90 (150%)
out of $100 from Q1 2015

27

Attacks per 1,000 transactions in Q4 2015

Up 18 (215%) attacks
per 1,000 transactions from Q1 2015

Up 3 (11%) attacks
per 100 transactions from Q3 2015

$8.62

out of $100 are at risk for luxury goods

83

Percent of fraud attacks that deploy botnets — networks of infected computers — to mount attacks

4X

Attack Rate more than quadrupled for digital goods between Q1 and Q4

2X

Attacked Rate almost doubled for luxury goods between Q1 and Q4

$7.77

out of $100 are at risk for digital goods

Introduction

The Global Fraud Attack Index Report

Fraud. The sheer word alone sends shivers up and down the spines of executives, risk managers, and even marketing and product managers within retail and financial services across America. Data breaches and the resulting cost of fraud have caused many to lose their jobs – from CIOs to CEOs. Lack of appropriate controls, prevention tools, detection techniques and — even worse – lack of appropriate containment when found can bring an entire business to its knees.

Why? It's costly. According to one study, annual fraud costs for U.S. retailers reached $32 billion in 2014.[1] Retailers lost an estimated 1.3% of revenue in 2015, more than double the rate of 2014.[2]

Not only does *actual* fraud "sting," but making inadvertently wrong decisions to avoid fraud costs merchants plenty as well. Up to 25% of declined sales transactions for eCommerce merchants were actually good sales to start. Fraud tests have huge rates of false positives.

The hardest part is that despite some good efforts, fraudsters always seem to be one step ahead. After, all, it's their full-time job to figure out how to beat the system, and pinpoint holes and weaknesses that they can exploit. Plug one hole, and the fraudster will sniff out the one left open and exploit it.

Sound a bit depressing? Envisioning that age-old favorite carnival game of whack-a-mole? Well how about if we envision a different world? One where merchants employ the same set of sophisticated tools themselves – not for bad, but for good? Innovations like machine learning, which offer the potential to react much faster and turn reaction into pro-action?

It's not out of the realm of possibility. It might be next to impossible to ever completely stamp out fraud. But in some areas, things are improving. In others, well, not so much.

Forter and PYMNTS.com partnered together to track, analyze and report on the important trends happening in the world of fraud as it relates to payments and commerce online. Every quarter we will monitor how fraud attempts, reflected as a percent of U.S. sales transactions,[3] on U.S. merchant websites are trending. Up? Down? Stable? Time to panic? Hopefully not.

[1] SmartMetric, Inc. "$32 Billion Lost by Retailers to Credit Card Fraud -- SmartMetric Brings Biometric Technology to the Credit Card", http://finance.yahoo.com/news/32-billion-lost-retailers-credit-161211566.html

[2] LexisNexis® True Cost of Fraud^{SM} study

[3] The rate of fraud attempts is measured as the number of fraudulent attempts as a percentage of all sales transactions. This includes fraud attempts that were both successful and unsuccessful.

Chart 1 shows you what we're going to be measuring every quarter and the lingo we're going to use.

Starting next issue we are going to launch the Global Fraud Attack Index. Now that we have a full year of data for 2015 we are going to treat 2015 as the base year for the Index (2015=100) and track the rise and fall of fraud over time relative to 2015.

Chart 1: Fraud Lingo

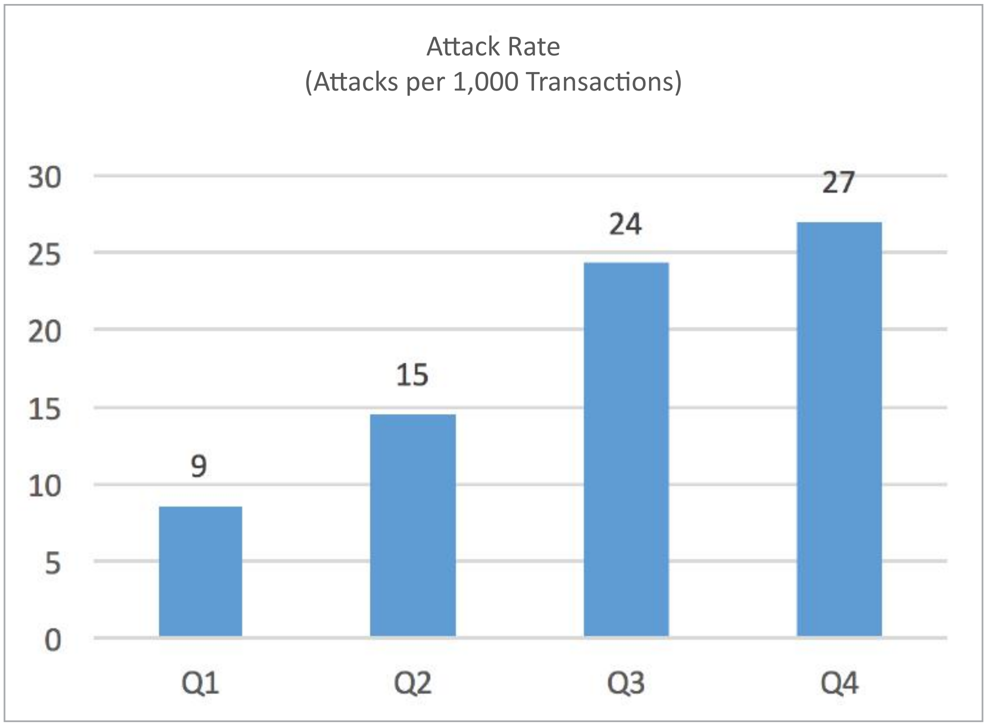
Term	Definition
Attack Rate	Out of 1,000 transactions, the number that were subject to successful or unsuccessful fraud attempts.
Attack Amount	The average amount of money that fraudsters were trying to steal, whether successful or not.
Potential Fraud Cost	How much money merchants would have lost if every transaction subject to a fraud attack was successful.
Botnet	Collections of computers that have been taken over, unbeknownst to the owner, for the purpose of mounting large-scale fraud attacks on retailers.
Sophisticated Fraud	Either advanced identity theft (the fraudster has access to multiple credentials and accounts of the victim) or advanced technical abilities (unusually sophisticated and complex/novel means such as clever malware). New and creative techniques are demonstrated.
Location Manipulation	Situation where the fraudster and the victim are not in the same place, and there was an obvious attempt by the fraudster to mask their true location. Location could be masked technologically via remote connections or could be altered via redirecting shipment.
Friendly Fraud	Fraud attempts where the "fraudster" turns out to be really the true owner of the account or card. After receiving the goods or services, the owner then reports the transaction as "fraud," resulting in a chargeback to the merchant.

The Last Year in Online Fraud

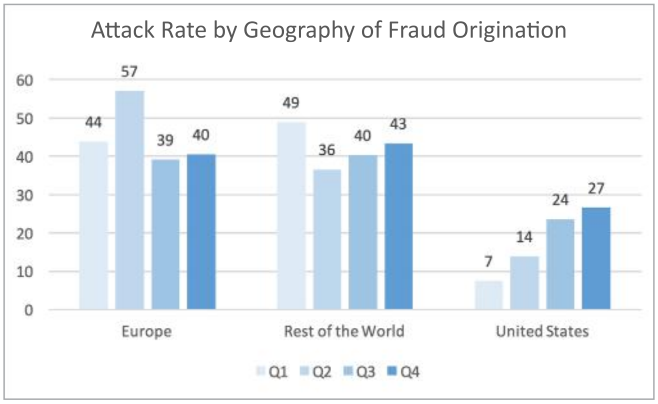
The rate of fraud attacks is the rate or percentage of all transactions that are attempts at fraud, including successful and unsuccessful attempts. The rate of fraud attacks has risen dramatically in the last four quarters. There's seasonal fluctuation in fraud as a result of shopping habits. Typically, the rate of fraud ratchets down in Q4 as the market is flooded with valid holiday shopping transactions — but not in 2015. The steady increase in fraud rates overwhelmed the decline we'd expect from seasonal fluctuations.

There is a possibility that this is due to EMV implementation. EMV is a technology that makes card-present fraud much more difficult and results in lower card-present fraud. One implication of this technology is that fraudsters shift to card-not-present (e.g. online) fraud. One explanation for the increased attack rate in the face of a spike in valid holiday transactions is the shift from card-present fraud to card-not-present fraud.

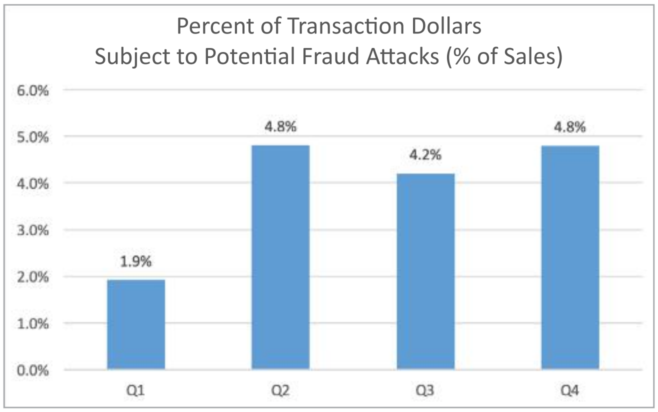
There were 27 fraud attacks for every 1,000 transactions (the "fraud attack rate") in Q4 2015 compared to only 9 in Q1 2015. That's an increase of 215% over 12 months. The only good news here is the rate of increase slowed between Q3 2015 and Q4 2015 — 11% between the third and fourth quarters compared to 67% between the second and third, and 69% between the first and second.



We sorted fraud attacks on U.S. merchants based on whether they arise from transactions that originate from within U.S., from Europe, or from other parts of the world (ROW). In Q4 2015, the rate of fraud was about 50% higher for transactions that originated from outside the U.S. than from transactions that originated within the U.S. Fraud attacks increased in Q4 2015 for each of these geographies compared to Q3 and dramatically since Q1.



The total potential cost of fraud continues to rise. Over the year the fraction of dollars that were hit with fraud attacks increased 290 basis points from 1.9% in Q1 2015 to 4.8% in Q4 2015. At the beginning of the year less than $2 out of $100 was subject to a fraud attack. By the end of the year that had increased to $5 out of $100. Fraud can place a significant amount of retailer profit at risk.

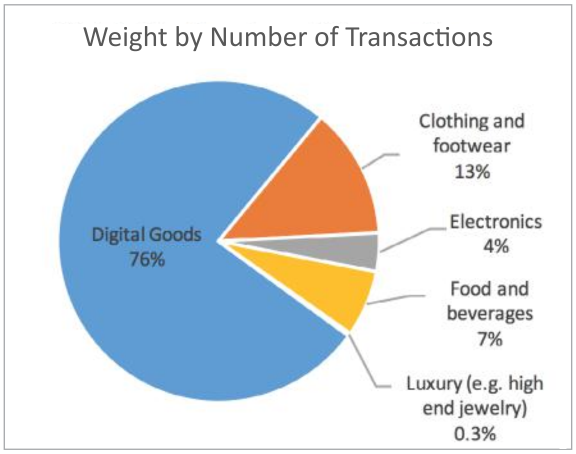


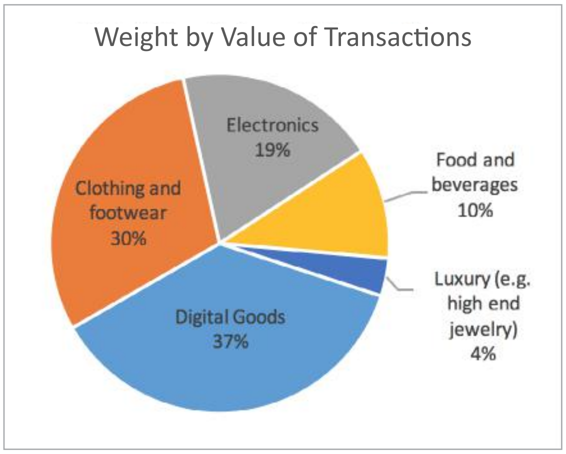
While fraud costs grew in Q4 2015, the rate slowed to 14%, compared to -13% in between Q2 and Q3 and 151% between Q1 and Q2. The slowdown resulted from two primary causes: first, the amount involved in the average attack coming from outside the U.S. declined considerably in the last quarter and, second, the growth in the average attack rate coming from inside the U.S. slowed during the quarter.

Industry Segments

Now we are going take a look at fraud attacks by industry. We look at five key segments: digital goods, clothing, electronics, food, and luxury. Naturally, they are highly diverse. The average transaction size for digital goods in 2015 was $27, compared to $126 for clothing; $279 for electronics; $88 for food; and $712 for luxury goods which include high-end jewelry.[4] But the smaller transactions are more common. Digital accounts account for 76% of transactions; clothing 13%, electronics 4%, food 7%, and luxury 0.3%.

For Q4 2015, the overall product weights by transactions and values are shown below. Digital goods account for 76% of transaction but only 37% of the dollar value of transactions.

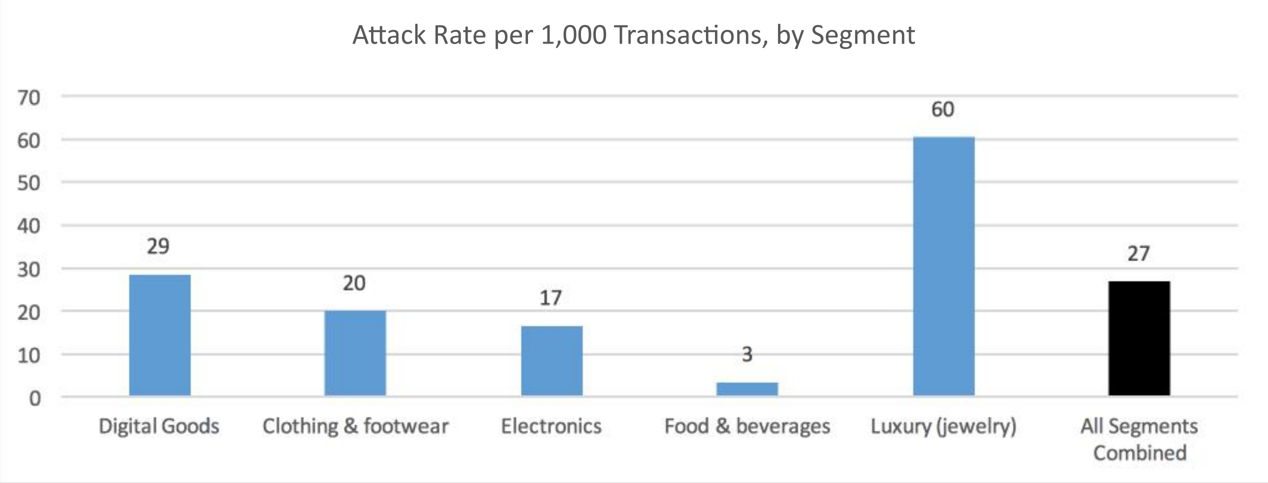




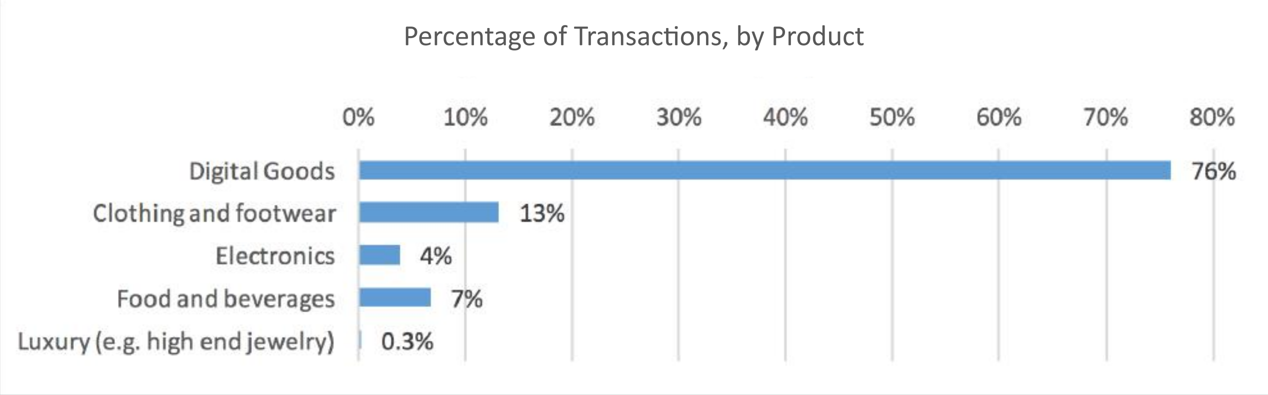
The attack rate (attacks per 1,000 transactions) varies considerably across these segments from a high of 60 in luxury to a low of 3 in food and beverage.

[4] Average transaction values are for all transactions completed across the segment group.

These are different than the average attack amounts which are the amounts that fraudsters are attempting to steal.



Not surprisingly, fraudsters are more likely to go for a big screen TV or an expensive bracelet than a bacon cheeseburger. The fraction of transaction dollars similarly varies across the segments. Luxury goods, because they are valuable targets, and digital goods, because they are easy targets, top the charts and again, food and beverages are not where fraudsters are aiming their firepower.



The fraud attack rate by segment reveals what segments are driving the changes in fraud attacks and in transaction dollars at fraud risk. Between Q1 and Q4 of 2015, the fraud rates in digital goods quadrupled from 7 to 29 and luxury has doubled from 31 to 60. Clothing increased by a third from 15 to 20, although the increase was not steady over the year. The transaction data for digital goods also showed huge increases in the average attack amount and, combined with the increase in the attack rate, the potential fraud in terms of the amount of transaction volume has exploded to increase thirteen-fold from 0.6% of dollars in Q1 to 7.8% in Q4.

	Potential Cost (% of revenue)				Potential Cost (% of revenue)			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Digital goods	7	12	25	29	0.6%	1.8%	6.3%	7.8%
Clothing & footwear	15	25	20	20	3.1%	9.6%	4.1%	3.6%
Electronics	20	30	20	17	2.9%	5.4%	1.8%	2.6%
Food & beverages	5	5	3	3	0.3%	0.3%	0.2%	0.2%
Luxury (jewelry)	31	43	65	60	4.9%	5.7%	9.0%	8.6%
All segments (combined)	9	15	24	27	1.9%	4.8%	4.2%	4.8%

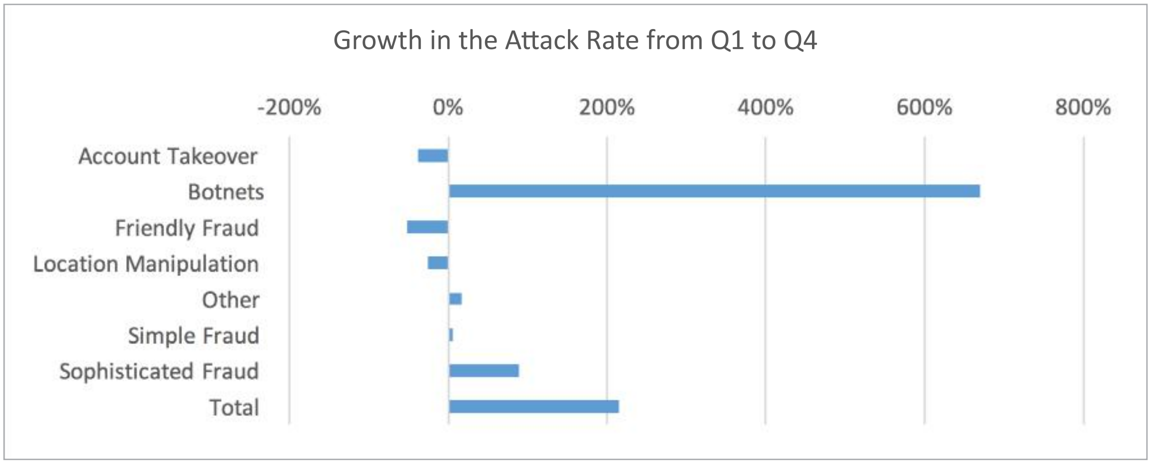
Methods of Attack

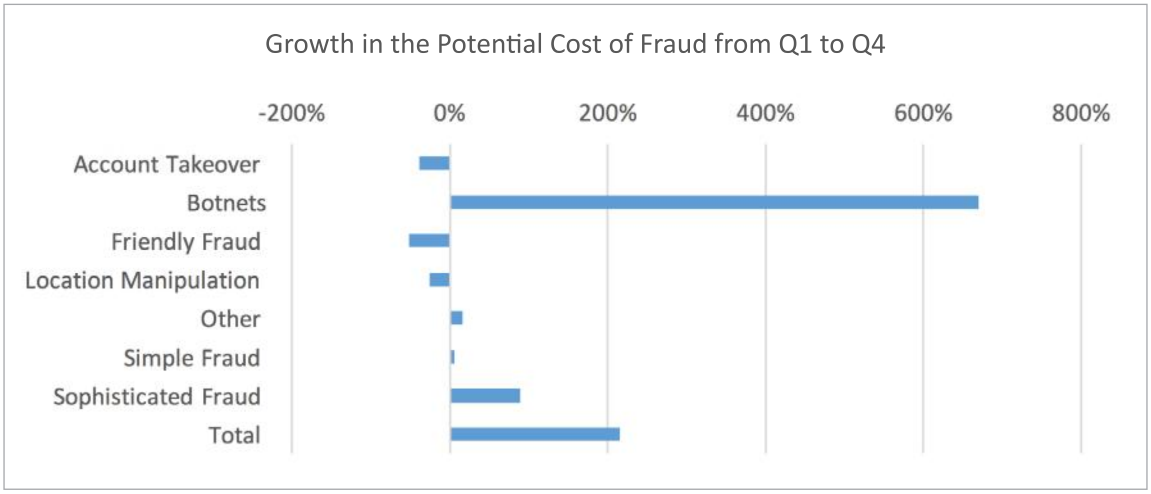
For transactions that originate in the U.S., we have data on what kind of fraud attack it is. There has been a dramatic change in the types of attacks over 2015. At the beginning of the year botnets accounted for 34% of attacks, followed by account takeovers at 17% and location manipulation at 10%. Friendly fraud accounted for 15%.

	Q1	Q2	Q3	Q4
Account takeover	17%	9%	4%	3%
Botnets	34%	47%	84%	83%
Friendly fraud	15%	11%	2%	2%
Location Manipulation	10%	6%	2%	2%
Other	17%	19%	6%	6%
Simple fraud	1%	2%	1%	1%
Sophisticated fraud	5%	7%	2%	3%

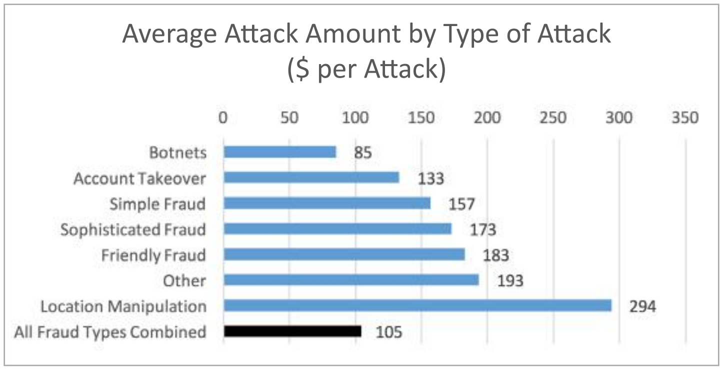
By the end of the year though, most fraud attacks came from "botnets" — collections of computers that have been taken over, unbeknownst to the owner, for the purpose of mounting large-scale fraud attacks on transactions. They accounted for a whopping 83% of all fraud attacks. Meanwhile, account takeovers only accounted for 3% of attacks and location manipulation 2%.

To summarize the changes over the year, we've calculated the percent increase in the attack rate for each method and the percent increase in the transaction dollars at risk — comparing Q4 2015 with Q1 2015. The number of attacks from botnets increased from 2 per 1,000 in Q1 to 24 per 1,000 in Q4, and the share of transaction dollars subject to botnet attacks increased from 0.2% to 6.0%. Only sophisticated fraud showed significant growth (although at a low overall level)—from 0.35 attacks per 1,000 to 0.55 attacks per 1,000 and from 0.01% to 0.19% of transaction dollars at risk.





The average size of the transaction targeted varies considerably across these methods of attack. As the chart below shows, botnets have the lowest average attack amount of all the types of fraud. Because the average attack amount is lower than other types of fraud, it offsets to some degree the potential transaction dollars that are at risk.



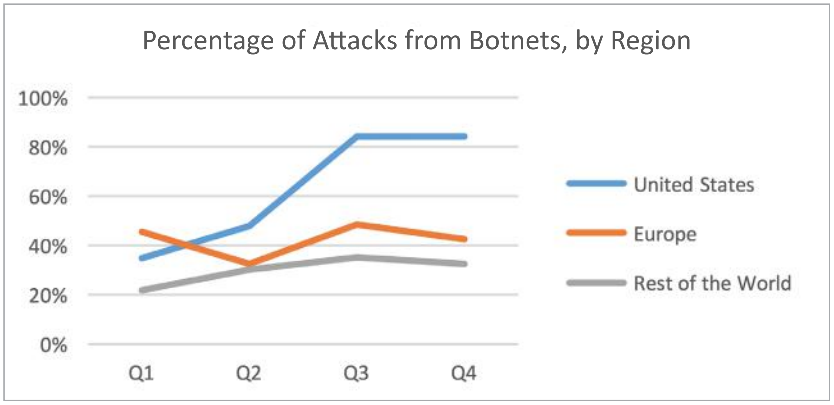
While botnets are the most common method of attack, representing 83% of all attacks, they involve one of the lowest dollar-value of transactions. As a result, botnets account for 69% of transaction dollars subject to attack during Q4.

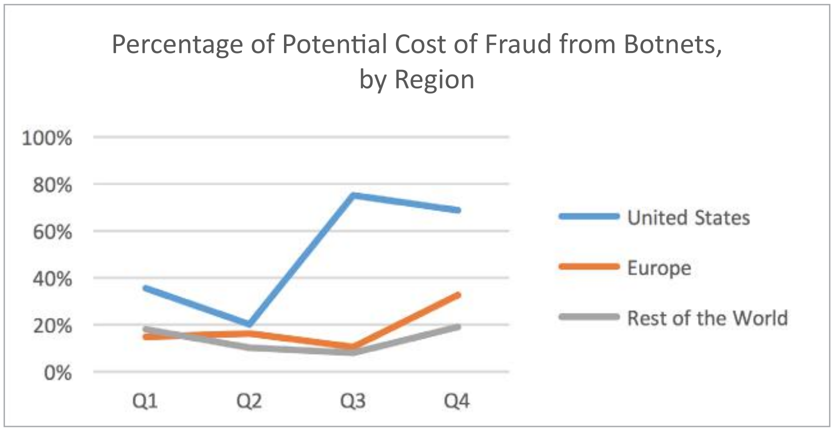
	Q1	Q2	Q3	Q4
Account takeover	5%	7%	2%	4%
Botnets	35%	20%	75%	69%
Friendly fraud	7%	6%	2%	4%
Location Manipulation	22%	15%	3%	6%
Other	24%	41%	9%	11%
Simple fraud	3%	5%	1%	1%
Sophisticated fraud	4%	6%	8%	5%
Total	100%	100%	100%	100%

Deep Dive – Botnets

Fraudsters now deploy bot armies to make their attacks on consumers and merchants. They recruit computers from unsuspecting users and infect them with malicious software. The cybercriminal — the botmaster — then uses the botnet under his control to mount various nefarious activities. That includes denial of service attacks, pump and dump stock scams, and many others. And it includes deploying them to hit transactions. A whole industry has emerged, operated mainly on the dark web, that sells cybercrooks everything they need to develop their armies and mount their attacks. With a botnet, cybercrooks can target point of sale devices and other points of transactions to hatch their plots.

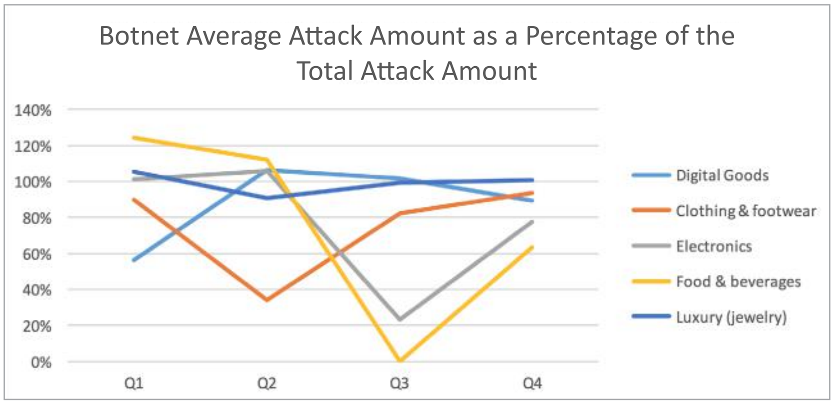
Botnets have been on the rise mainly for transactions done within the U.S. They rose dramatically from Q1 to Q3 for transactions that originated in the U.S. but not for transactions that originated in Europe or the rest of the world (ROW). That story is slightly different when we look at the percent of transaction values hit by botnets. There's still a huge increase in the U.S. but also evidence that the use of botnets is increasing from transactions originating from Europe and the ROW.

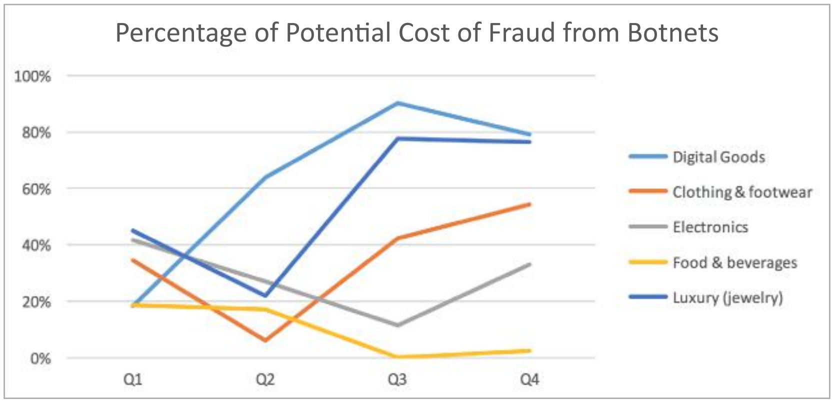




The rest of our deep dive focuses on the U.S.

Over the course of 2015 the percentage of attacks from botnets increased — at least when comparing Q4 and Q1 — for every merchant segment with the exception of food and beverage, where they declined close to zero. But the big rise — and the main reason botnet attacks increased overall — came in digital goods and luxury goods. The next biggest rise came in clothing and footwear.

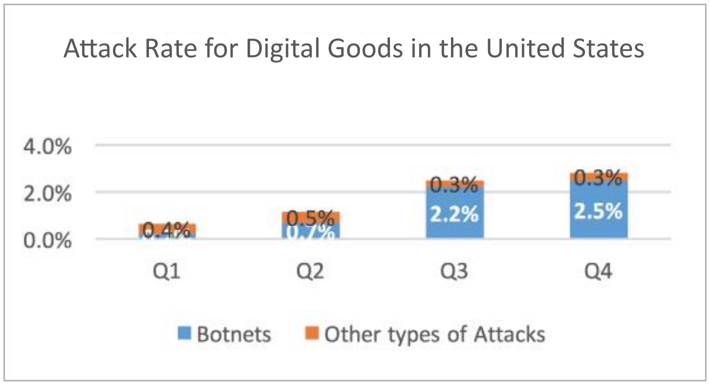


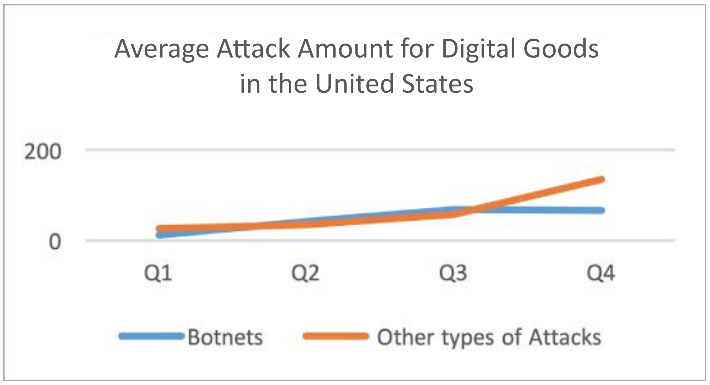


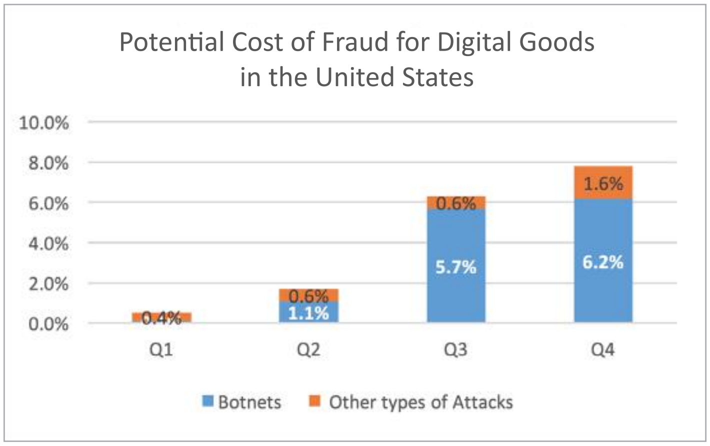
The rise of botnets in digital goods and clothing and footwear is important because these two categories account for 67% of transaction dollars and 89% of transactions. On the other hand, for anyone selling luxury goods, the rise of botnets is scary.

Digital Goods in the United States

We see that the attack rate is increasing but at a slower rate during Q4 2015. However, the average attack amount continued to increase for attacks other than botnets. As a result, the total potential cost of fraud continued to climb for botnets but the other types of attacks became slightly more important due to the increase in the average attack amount.

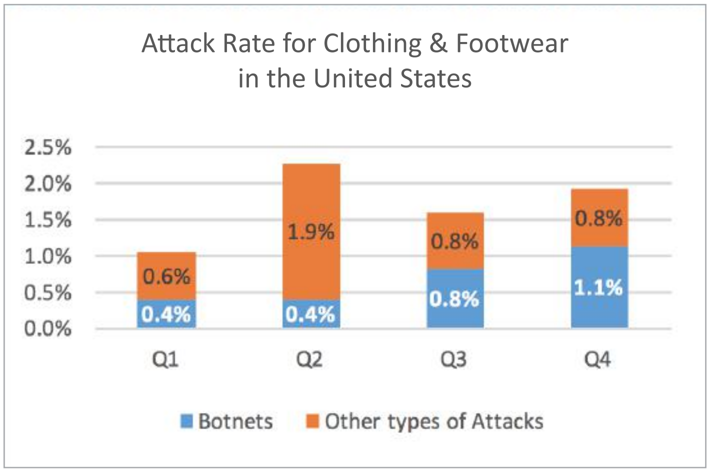


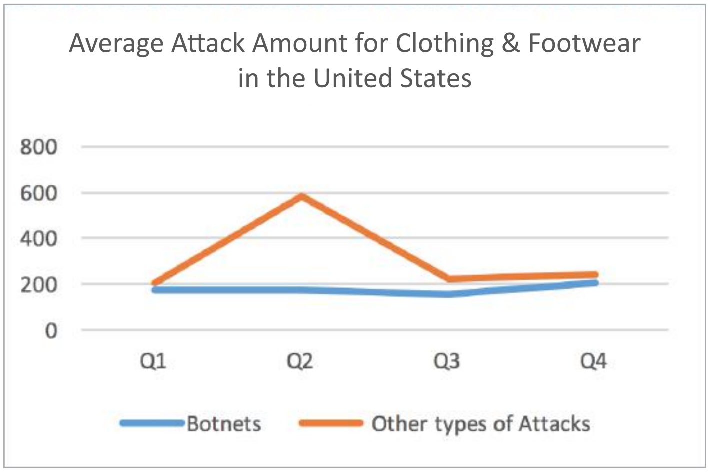


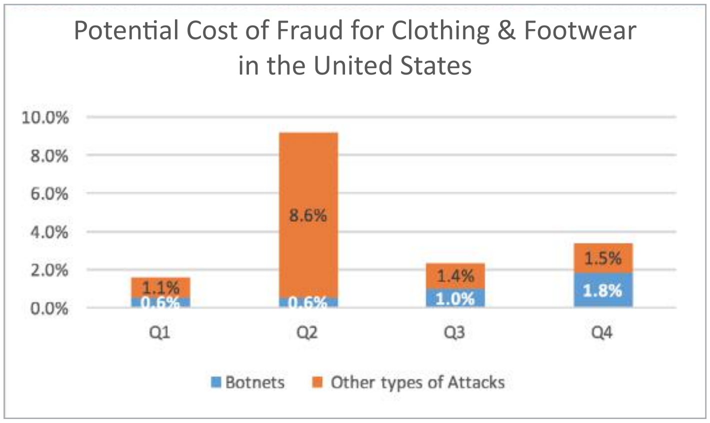


Clothing & Footwear in the United States

In the Clothing & Footwear segment, the overall attack rate continued to climb, but in this case the increase is due to increases in the botnet attack type. In fact, attacks from non-botnet type of attacks remained constant at 0.8% of all transactions where botnets increased from 0.8% to 1.1%. Average attack amounts are up, but by only a small amount. In turn the potential cost of fraud increased from 2.4% to 3.3%.

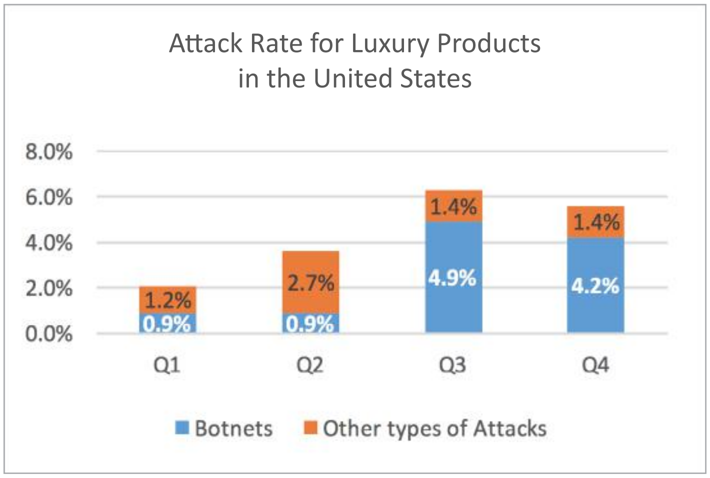


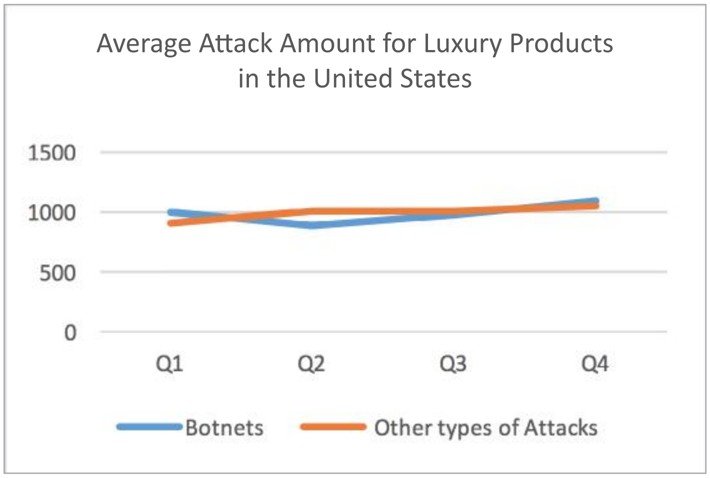


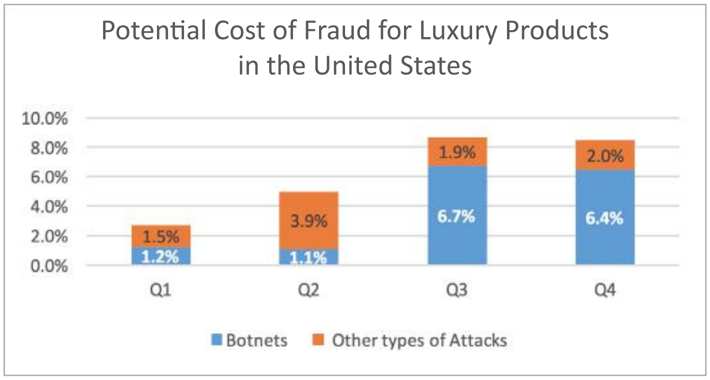


Luxury Goods in the United States

The luxury goods segment represents relatively little in terms of overall potential costs because there are so few transactions in this segment. On the other hand, if you are a luxury goods seller, potential fraud costs are enormous since almost 8.5% of transaction dollars during Q4 were hit by successful or unsuccessful fraud attacks. This is largely attributable to the huge increase in bots. While the average attack amount is increasing, it is modest compared to the increase in the attack rate, which almost doubled from 31 attacks per 1,000 transactions in Q1 to 60 attacks per 1,000 transactions in Q4.







Not too many eCommerce verticals are more appealing to fraudsters than those that deal in electronics, offering as they do big-ticket items that can easily be resold. But even **Laura Park, Director of OWC** (who runs the eCommerce website MacSales.com), was surprised at first to learn that fraud attempts on the site experienced a significant bump in Q2 — even though it aligns with latest industry data regarding the electronics segment.

“We’ve always seen the highest number of fraudulent attempts in our busy season — middle of December, early January,” Park said in a recent conversation with PYMNTS. “So it was really interesting, when we looked at the data, to find that we actually did have a huge bump typically around March into early April.”

Noting that the time period tends to represent a lower volume order compared to others (such as the holiday season), Park attributes the peak in fraudulent activity on MacSales.com to the fact that “the percentage of good orders to bad orders is going to be a little bit more off than it would be during our busy season.”

Oh Where, Oh Where Does That (Big) Fraud Come From?

As for where those fraud attempts are coming from, OWC has found that a significant amount originate within the U.S. — and that does not surprise Park, as her experience is that other countries with which her company does business do not generally report the same rates of online fraud that occur domestically.

Those U.S.-based cybercriminals, notes Park, tend to be recognized by multiple attempts.

“You'll see the same people that we've blacklisted from multiple occasions in the past coming back again and again,” she tells PYMNTS. “They're basically just poking at your system to try to see what works, and as soon as they find a flaw, everybody adjusts and here they come.”

Fighting Back – Hard

In combatting that practice, OWC finds value in keeping an eye on even the smallest of changes in ordering activity. For example, if a large influx of orders in a single day appears to be coming from the U.S. but the IP is pinging to another country, the company will adjust how they’re looking at it so that that behavior gets flagged more often.

OWC has recognized that a lot of the fraud attempts in the space of online electronics sales begin in the form of a small order — with the fraudster testing the system — after which they will attempt a much larger one.

But the problem for a lot of online merchants is that once the “test” order has gone through, their system will then recognize that fraudster as an existing — and therefore legitimate — customer, making the subsequent, more serious theft harder to stop before it occurs.

To avoid that conflict on its site, OWC has implemented into its own system a rule that tracks additional attempts.

By Park's account, the most common fraudulent attempts on MacSales.com fall into two categories: those in which the fraudster will place an order using a legitimate customer's shipping address and attempt to reroute the item(s) to a different one when in transit, and "friendly fraud" — a situation where the fraudster has so much of a legitimate customer's information that they will contact his or her bank and attempt to change it.

To address the former scenario, OWC has implemented safeguards with its carriers: If a person attempts to reroute a package in transit, it will automatically be sent back to the company.

Fraud Is Never Friendly

Combatting "friendly fraud" — which Park describes as "utterly terrifying, from a merchant standpoint" — meanwhile, takes a little more work. OWC uses a couple of different tools to monitor a customer's behavior prior to purchase, with Park noting that while a legitimate customer will typically "shop around, look at different things, check the prices on a few different items before going through," a fraudster, on the other hand, will "put 50 hard drives in their cart and [immediately] check out." The latter behavior is usually suspicious.

Of course, as Park says, monitoring it manually "is a little bit of a nightmare," as the task requires that the merchant essentially have the order flagged already before it can go back and check. In that regard, OWC's experience with Forter has been of great help, she adds.

OWC's primary method of confirming legitimate customers was whitelisting IP addresses, a process Park says was "used much more carefully" than the corresponding method of blacklisting them.

"The blacklist," Park explains, "did not actually prevent the orders from coming through. We let [the fraudsters] in, so that we could see what they were trying to do. And we would just review the order and then cancel it so that we still had that kind of back end data about where they were coming from, what the IP looked like," and so on.

"The more 'bad' orders we saw," she continues, "the easier it was to identify what we were looking for. Whenever it was time to review [be it quarterly or yearly], that was when we would pore over all that data — determine trends, how they're changing, the big problems going forward, what we can adjust on our end, et al — to stop more bad ones and let more good ones through."

Park adds that there was "always a fine line" in doing that procedure manually, "Because you don't want to stop too many orders, or you're just annoying your good customers. But you also don't want to let too many go because those are the ones that are going to hurt when they come back later."

There's Gold In The Data

Although industry data shows that the prior trend of a decline in fraud attacks on eCommerce sites during Q4 (as a result of an increased number of legitimate transactions during the holiday season) has begun to shift — with the fraud rate having actually risen by 11 percent from Q3 to Q4 of 2015 — with the October EMV shift being attributed as a likely cause, Park tells PYMNTS that OWC itself has not experienced that same trend.

Her belief, in fact, is that the expanding implantation of EMV in the U.S. is not going to necessarily lead to an uptick in attempted online fraud (compared to offline), but rather to fewer instances of major data theft.

Despite the consumer perception of the use of a credit card online as being more dangerous than the use of one in a physical store, Park states plainly: "Working for an eCommerce company, we spend way more time thinking about how we're going to protect our customers' data than brick-and-mortar stores do."

What EMV is really going to protect against, in Park's estimation, is instances of fraudsters using electronic methods — such as piggybacking on a store's heating vent electronics, for example — to access card data that is stored on merchant terminals.

If Wishes Were Horses …

Park finds it unfortunate that the current legal procedures prevent her from "spreading the wealth," as it were, by red-flagging cybercriminals for the benefit of other eCommerce platforms.

"As a merchant, you can only report the fraudulent transactions that go through — and ship and deliver — as theft," she explains. "You cannot report the attempts."

"Unless you're looking at massive amounts of data and not just one customer's at a time — you can't really pool that information," states Park.

She describes the situation as "frustrating" that "the law is not as 'on top of it,' shall we say, as it should be."

Other than a merchant's ability to notify a bank that one of their customer's information has been compromised — a step that OWC itself would often take — or a customer perhaps turning to the FBI's cybercrime division, Park says that the industry-wide solution for right now otherwise comes down to customers being well-informed and vigilant on the lookout for fraud.

"That might not be happening a lot," admits Park, "but really, the ball's in their court. It's the only way to report [fraud] to the proper authorities."

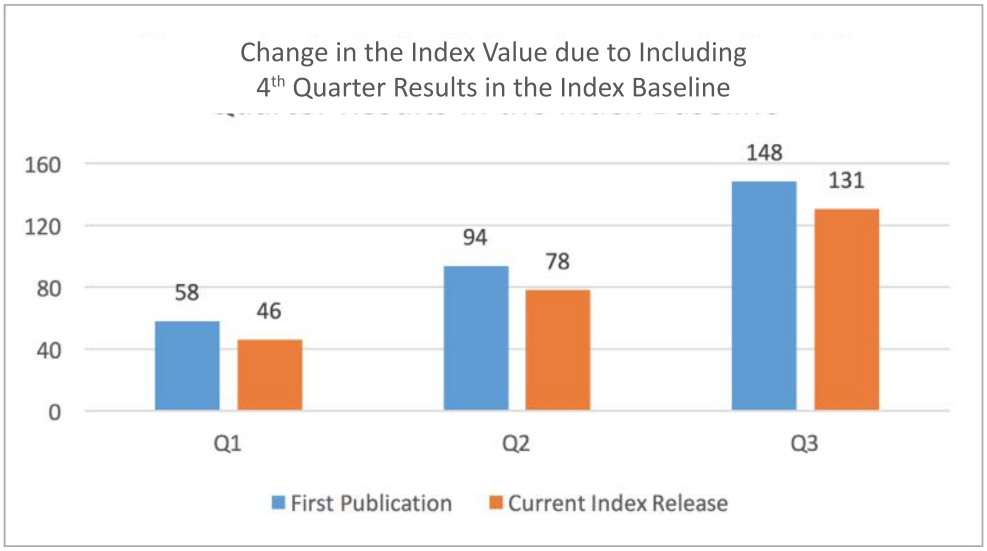
Methodology

In this, our second iteration of the Global Fraud Attack Index™, we have updated our methodology in two ways to improve the overall results. First, we updated the baseline for the index measurement and second, we adjusted the weighting of the industry segments measured in this index.

Index Baseline

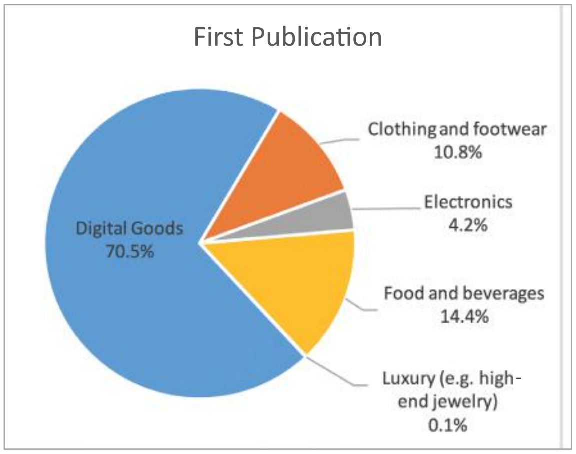
At the time we published our last index, we only had data for the first 3 quarters of 2015 available. Now that data for all 4 quarters is available, we have updated the index baseline and adjusted the prior results accordingly.

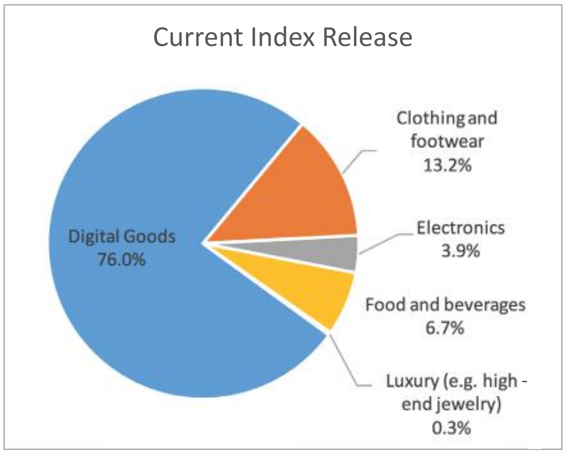
Since the attack rate for the Q4 is larger than the average attack rate over the first 3 quarters, the index baseline is higher. As a result, each of the prior index values is now lower. For example, in the first publication of this index, the value for Q3 2015 was 148. Based on the new higher index baseline, the Q3 index value is now 131. The new index value for Q4 increased by 11% to 145.



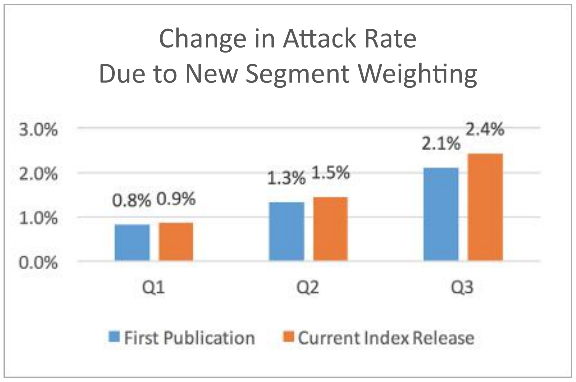
Segment Weighting

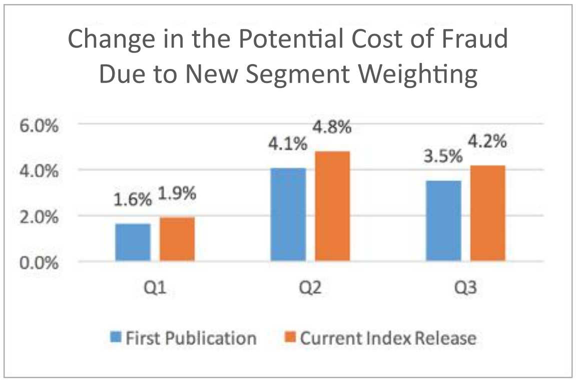
The underlying data used for the index is collected by industry segment, method of fraud, and geographic origination of the fraud attempt. We calculate total results as an average of the industry results weighted by total sales in each of the industry segments we cover. In the first version of the index we aggregated results according to the number of transactions in each segment from the data we collected. We have revised this weighting to more accurately reflect fraud activity by aggregating based on the total number of eCommerce transactions of all U.S. merchants.





As shown on the charts above, the new aggregate results reflect more digital goods and clothing and footwear sales and fewer transactions in the food and beverage category. The attack rates vary by quarter but food and beverage always has the lowest attack rate and as a result, the average attack rates are now slightly higher, but the overall trend is unchanged.





What is the Index?

The Global Fraud Attack Index™ measures the growth (or decline) of attempted fraud[5] on U.S. merchant websites. It also quantifies the potential cost to merchants, left unchecked, of these attempts based on average attack amounts and how these amounts are trending over time.

Index Development

We collected data on the attack rate, the average attack amount and the total number of eCommerce transactions in the market. This data was used to evaluate trends in the attack rate, the attack amounts, and the potential cost of fraud to merchants. The data was segmented based on the geographic location of the fraudster, by the primary merchant segment, and by the type of fraud being perpetrated.

Attack Rate

Forter provided data on the attack rate, or the percentage of all sales transactions that were attempts at fraud (both successful and unsuccessful), and the average attack amount. These data were separated by transactions and fraud attempts that originated in the United States, Europe and the Rest of the World.

The US attack rate is equal to the percentage of US consumers buying from US merchants that resulted in an attempt at fraud (both successful and unsuccessful). For Europe, the attack rate is equal to the percentage of cross-border transactions from the US to a European country that was an attempt at fraud (both successful and unsuccessful). For the Rest of the World, the attack rate was equal to the percentage of cross-border transactions from the US to a country other than Europe that was an attempt at fraud (both successful and unsuccessful).

Average Attack Amount

The average attack amount is the average amount that fraudsters were trying to steal through their efforts to commit fraud. This is the average of all attacks, by region, product type, and the type of fraud that was being attempted.

Potential Cost of Fraud

The potential cost of fraud is the total cost of fraud as a percentage of revenues that would be paid by merchants assuming that every fraud transaction was successful. The calculation is simple once all the data is collected.

*Potential Cost of Fraud (%) = (# of Txn * Attack Rate * Avg Attack Amount) / Total eCommerce revenue*

Data for the Attack Rate and for the Average Attack Amount were provided by Forter and described above.

Data for the total revenues and number of transactions were prepared by PYMNTS.com.

[5] Attempted fraud is defined as all sales transactions which are identified as potential fraud, both successful and unsuccessful

Total eCommerce Revenues

The total value of eCommerce sales for each of the product categories was based on data from the U.S. Census Bureau. Detailed eCommerce data is only available from 2013 and by year. However, total quarterly eCommerce sales are available. We assumed the ratio of total segment sales to total eCommerce sales was constant over time and estimated the total segment revenues by quarter as:

Segment eCommerce Salescurrent quarter=Total eCommerce salescurrrent quarter(segment sales in 2013 / Total eCommerce 2013)*

The U.S. Census Bureau provides data at a three-digit NAICS level and a breakout of sales by product type for all “non-store retailers” based on NAICS code 454. However, some of the product groups are more detailed than a three-digit level. In these cases, we use data from the economic census, which provides data for total sales (not eCommerce sales) at the six-digit level. This data is made available once every five years and is currently available for 2012.

In these cases we assume that the level of sales at the six-digit level as a percentage of the corresponding two or three digit category is constant over time and is the same for total sales and eCommerce sales. We use this ratio to estimate eCommerce sales during 2015 for categories that are more detailed than three-digit NAICS codes would allow.[6]

[6] We have used this methodology to estimate total e-commerce revenues for:

- Digital Goods: digital gaming and software (software publishers 511210 —subset of NAICS 511 “Publishing”)
- Digital Goods: Movie and Music subscriptions (cable and other subscription programing 515210 and Radio Stations 515112 – subset of 515 “Broadcasting”)
- Digital Goods: Data hosting (Data processing, hosting and related services 518210 – subset of 518)
- Luxury: Jewelry stores (code 44831 – subset of 448 “Clothing and Clothing accessory”)
- Food and Beverage: Food delivery(Local messanger and delivery 492210 – subset of 48-49 “Transportation and Warehousing”)
- Food and Beverage: Food service delivery excluding full service and drinking places (equal to NAICS 772 Food service and drinking places less 7224 drinking places and 722511 full service restaurants)

The Number of Transactions

The total number of eCommerce transactions were estimated by dividing the total value of eCommerce transactions by the average transaction price. The average transaction amount was calculated based on the Internet retailer Top 1,000 list, which reports the total value of eCommerce sales by firm. We identified which segment each company on the Top 1,000 list was included in and calculated the average transaction amount for each of the five segments included in this report.

The number of transactions were estimated by dividing the total eCommerce revenues by the average transaction amount.

We then estimated the total value of eCommerce and the number of transactions for each of the three regions. For domestic U.S. sales, we used data provided by Census as described above. However, for the other regions we had to estimate the cross-border eCommerce from the U.S. to Europe and to the Rest of the World.

We rely on third-party research that cross-border sales from the United States are 8.7% of all U.S. eCommerce sales.[7] In addition, 47% of those sales are to Europe.[8]

We estimate the value of transactions in each region.

- Value of US transactions is from the data
- Value of European transactions is equal to the value of US transactions times 8.7% times 47%
- Value of transactions in the rest of the world is equal to the value of US transactions times 8.7% times 1 minus 47%.

The number of transactions in each region is equal to the total value of transactions by region divided by the average transaction price. We assume that the average transaction price for each region is the same.

[7] United States: Cross-Border E-commerce Report; Critical Facts and Insights for International Expansion, Update 2014. They PayPers, http://www.the-paypers.com/news-and-reports/us/5

[8] Same report ODD METRIC and WOULD PREFER CLIENT DATA. The data is incomplete.

Merchant Segments

The following merchant segments were included in development and analysis of the Index:

- Clothing and footwear – covers a variety of merchant segments from casual to smarter wear. High-end brands would be categorized in Luxury due to differing patterns of fraud.
- Electronics - direct sellers and retailers of electronic goods, including laptops, tablets, e-readers, smartphones and accessories.
- Food and beverages – digital food delivery requests including groceries.
- Luxury – high-end brand merchandise including clothing, jewelry and accessories (e.g. Rolex, Louis Vuitton, etc.)
- Digital goods - digital goods such as gift cards, e-books, music, gaming. Also includes business-related virtual services such as hosting and software solutions.

Types of Fraud

The following are definitions of the types of fraud referenced within the report.

- Account takeover - account takeover is when a fraudster breaks into and takes over a victim's account, using it to perform activities such as making a purchase.
- Botnets - collections of computers that have been taken over, unbeknownst to the owner, for the purpose of mounting large-scale fraud attacks.
- Friendly fraud - situation when the "fraudster" turns out to be the true owner of the account or card.
- Location manipulation - situation where the fraudster and the victim are not in the same place, and there was an obvious attempt by the fraudster to mask their true location. Location could be masked technologically via remote connections or could be altered via redirecting shipment.
- Simple fraud - attacks which are easily spotted and the fraudster has either made little attempt to conceal their own identity, or made a naive attempt (e.g. such as claiming that their name is "Mickey Mouse"). This can be a sign of a brute force attempt, but also can be a sign of a fraudster attempting to test the system, to search for weakness.
- Sophisticated fraud - either advanced identity theft (the fraudster has access to multiple credentials and accounts of the victim) or advanced technical abilities (unusually sophisticated and complex/novel means such as clever malware). New and creative techniques are demonstrated.

About

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Forter

Forter provides new generation fraud prevention to meet the challenges faced by modern enterprise eCommerce. Only Forter provides fully automated, real-time Decision as a Service™ fraud prevention, backed by a 100% chargeback guarantee. The system eliminates the need for rules, scores or manual reviews, making fraud prevention friction-free.

The result is fraud prevention that is invisible to buyers and empowers merchants with increased approvals, smoother checkout and the near elimination of false positives - meaning more sales and happier customers. Behind the scenes, Forter's machine learning technology combines advanced cyber intelligence with behavioral and identity analytics to create a multi-layered fraud detection mechanism.

Feedback

We are interested in your feedback on this report. If you have questions, comments, or would like to subscribe to this report, please email us at globalfraud@pymnts.com.

Disclaimer

The Global Fraud Attack Index^{TM} a PYMNTS/Forter Collaboration, may be updated periodically.
While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED “AS IS” AND ON AN “AS AVAILABLE” BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.

You agree to indemnify and hold harmless, PYMNTS.COM, its parents, affiliated and related companies, contractors and sponsors, and each of its respective directors, officers, members, employees, agents, content component providers, licensors, and advisers, from and against any and all claims, actions, demands, liabilities, costs, and expenses, including, without limitation, reasonable attorneys’ fees, resulting from your breach of any provision of this Agreement, your access to or use of the content provided to you, the PYMNTS.COM services, or any third party’s rights, including, but not limited to, copyright, patent, other proprietary rights, and defamation law. You agree to cooperate fully with PYMNTS.COM in developing and asserting any available defenses in connection with a claim subject to indemnification by you under this Agreement.