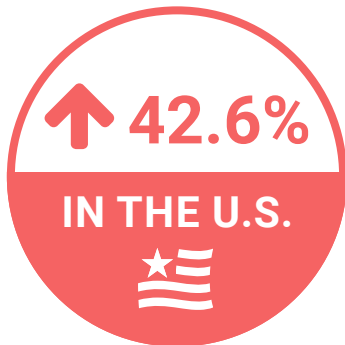


# GLOBAL FRAUD ATTACK INDEX™

October 2016

ATTACK INDEX

↑ 62%



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

Q2 2015  
\$4.90

Q2 2016  
\$7.60

↑ 55%

Dollars at risk per \$100 of sales

↑ 60.6% Digital Goods

↑ 87.2% Luxury Goods

↑ 91.8% Clothing & Footwear

↑ 11.9% Electronics

↑ 195.3% Food/Beverage

↑ 62%  
Total Fraud

Change in fraud attacks by industry

### **Acknowledgment**

The data model and supporting research was developed exclusively by the PYMNTS.com research and analytics team and is proprietary. Any research, unless indicated otherwise, is conducted exclusively by this team and without input or influence from the sponsoring organization.

# Global Fraud Index™

## The Global Fraud Attack Index Snapshot

**↑ 62%**

Growth in rate<sup>1</sup> of fraud attacks  
between Q3 2015 and Q2 2016

**15%**

Increase in fraud attacks since Q1 2016

**\$7.60**

\$7.30 out of every \$100 of sales are at risk  
(based on five product categories considered)

Up \$3.00 (71%) out of every \$100 from Q4 2015

Up \$1.00 (15%) out of every \$100 from Q1 2016

**39**

Attacks per 1,000 transactions in Q2 2016

Up 12 attacks per 1,000 transactions  
(a 47% increase) from Q4 2015

Up 5 attacks per 100 transactions  
(a 14% increase) from Q1 2016

**\$12.10**

About \$12.10 out of \$100 is at risk  
for luxury goods

**74**

74 percent of fraud attacks deployed by botnets  
(networks of infected computers)

**47%**

The attack rate by botnets increased for  
digital goods between Q3 2015 and Q2 2016

**87%**

The attack rate by botnets increased for  
luxury goods between Q3 2015 and Q2 2016

**5%**

5 percent of fraud attacks are account takeovers

<sup>1</sup> The percent of transactions that experienced fraud attacks in Q1 2016 compared to Q2 2016

# The Global Fraud Attack Index Report

In the beginning there was the internet, formless and empty. And then came the people who set up websites, the merchants who set up online shops and, later yet, the cloud with its promise of endless space and convenience. With them all came fraudsters and the opportunity for theft everywhere.

Fraud has existed since the beginning of time and is older than the Bible, but new technology has given everyone, especially fraudsters, new opportunities. In 2015, retailers reported an average of 236 blocked fraud attempts per month, up 33 percent from the year before. Overall, fraud losses in 2015 totaled 1.47 percent in revenue, compared to 1.32 percent in 2014 and 0.51 percent in 2013.<sup>2</sup>

Merchants know this to their peril. A single data breach can, in a best-case scenario, result in “restructuring” senior management and, in a worse-case scenario, shut down a company entirely.

In some ways, the growth of fraud makes sense. In order to succeed, fraudsters need to stay a step ahead of innovation. But what exactly are they doing to stay ahead? What’s popular? What’s not?

Forter and PYMNTS.com have partnered to track, analyze and report on important fraud trends in the world of payments and online commerce. Every quarter, we monitor fraud attempts on U.S. merchant websites to give you the latest insights on what’s going on. (Note: For each of the Indexes in 2016, we’re using 2015’s fraud rates as a benchmark.)

Our take-home this quarter: Fraud rates are climbing. They climbed last quarter and are still climbing this quarter. In fact, overall fraud rates have increased by 14 percent from last quarter to this quarter. To find out how fraudsters are doing it and what methods they favor, keep reading.

---

<sup>2</sup> “Fraud costs climb for online retailers,” Internet Retailer, <https://www.internetretailer.com/2016/04/13/fraud-costs-climb-online-retailers>

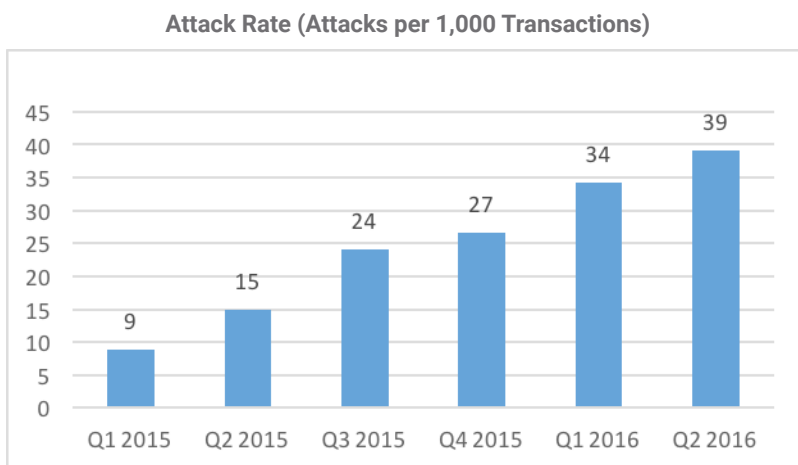
### Chart 1: Fraud Glossary

Term	Definition
Attack Rate	Out of every 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, regardless of success.
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). Fraud where new and creative techniques are demonstrated.
Location Manipulation	A 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. A location could be masked technologically via remote connections or more simply by a fraudster redirecting a shipment of goods.
Friendly Fraud	Fraud attempts where the “fraudster” turns out to be the true owner of the account or card. After receiving the goods or services, the card or account owner reports the transaction as “fraud,” resulting in a chargeback to the merchant.

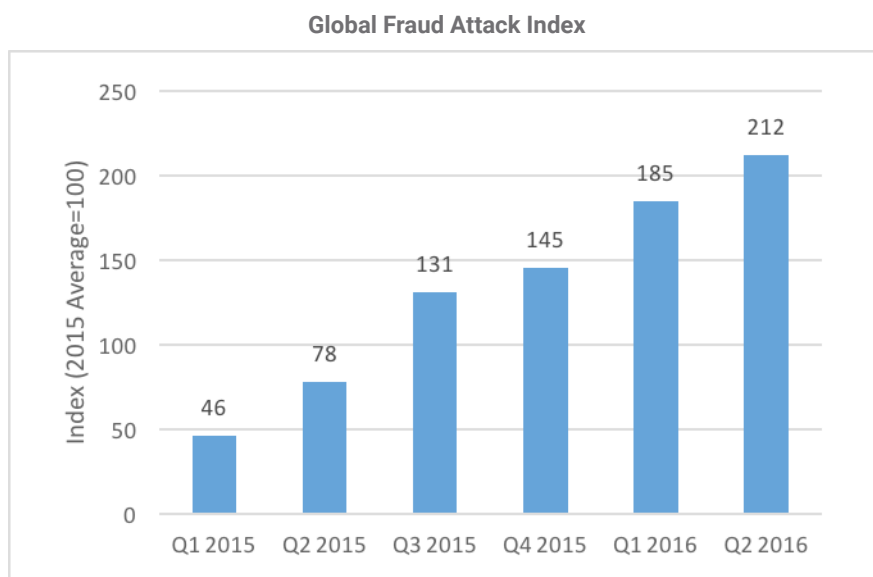
## The Latest in Online Fraud: Q2 vs. Q1

So far 2016 has been a rough year for fraud. Typically, we expect an uptick in fraud rates during the first quarter of each year. This is because during Q4 – the holiday season – the overall volume of transactions goes up, dragging the fraud rate down. However, this year, the first quarter's rate was far higher than expected. The fraud attack rate was 34 out of 1,000, a 26 percent increase from Q4.

This quarter, the rate went up again, with 39 fraud attacks on every 1,000 transactions. That's a 14.7 percent increase from last quarter. Last year during the same time period (Q2 2015), there were only 15 attacks on every 1,000 transactions. That's 163 percent growth.



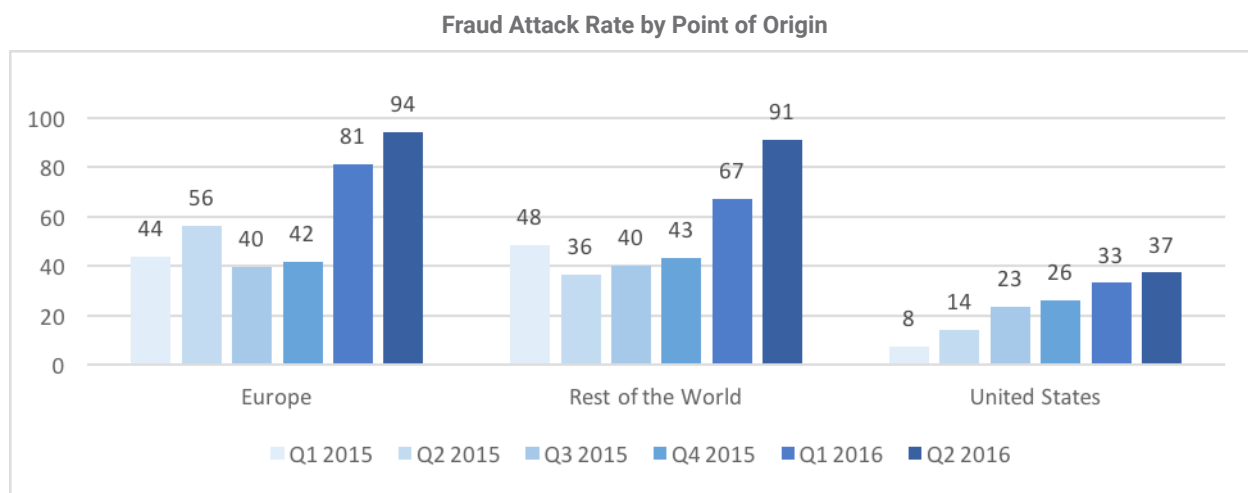
This quarter, the value of our fraud index is 212, compared to 185 last quarter and 78 a year ago.



So where are these attacks coming from? We sorted attacks on U.S. merchants into three categories: attacks from within the U.S., attacks from Europe and attacks from the rest of the world (ROW).

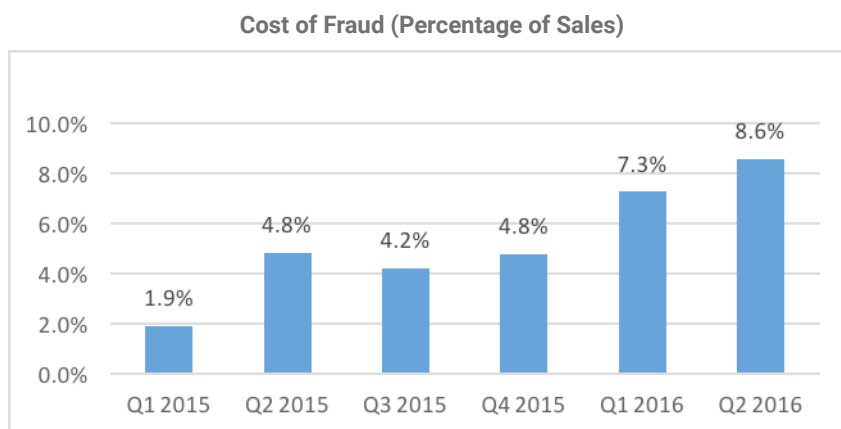
The biggest culprit? Europe. Europe generated 152 percent more attacks than the U.S. and ROW 144 percent more than the U.S. This is surprising because last quarter ROW originated 200 percent more attacks than the U.S., while Europe originated 127 percent more attacks.

But, as it turns out, Europe may not be leading in fraud attacks for long. The fraud rate caused by Europe rose 16 percent from last quarter, but 36 percent in the ROW. By comparison, it rose 12 percent in the U.S.



## The Cost of Global Fraud: High, Getting Higher

As fraud attack rates increase, so does the potential cost of fraud. Since last quarter, transactions that were hit by fraud went from 7.3 percent to 8.6 percent. At the beginning of 2015, less than 2 percent of transactions were subject to fraud. In other words, a year ago retailers could expect to lose less than \$2 out of every \$100 to fraud. That's quadrupled to \$8. If this kind of growth continues, retailers could find themselves in serious trouble.



However, the good news is while the cost of fraud is still increasing, it isn't increasing as quickly. From Q4 2015 to Q1 2016, the potential cost of fraud increased by 52 percent. And, from Q1 2016 to this quarter, the potential cost of fraud only increased by 18 percent.

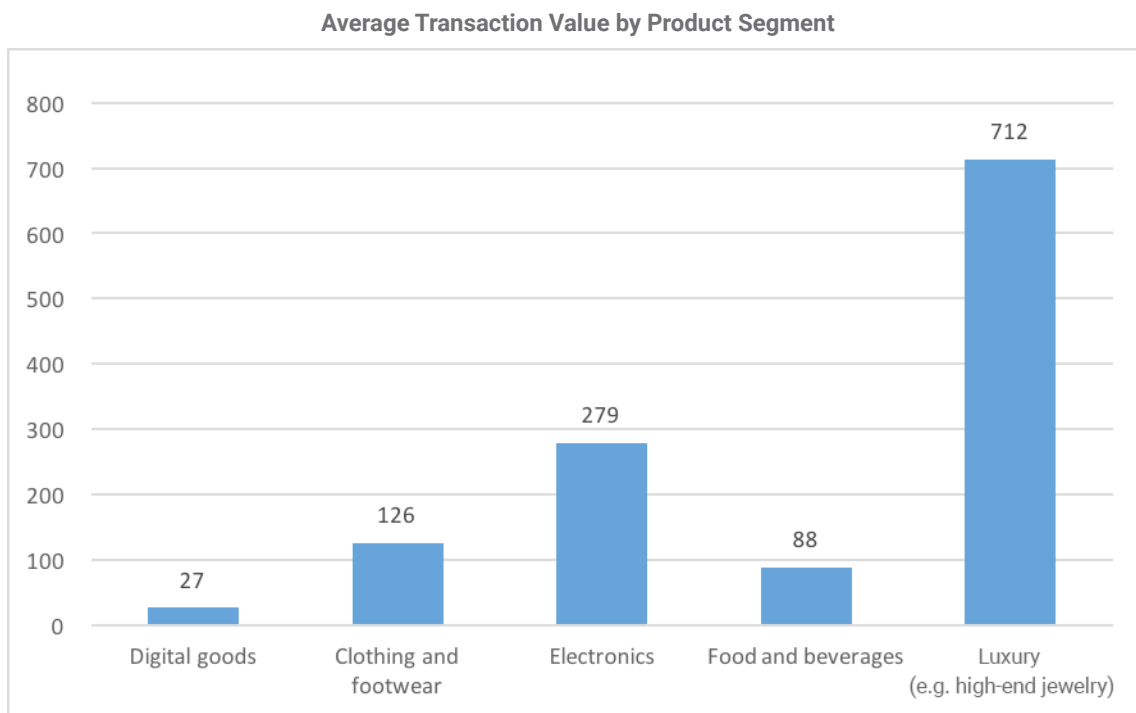
When we examine the point of origin, the cost of fraud for attacks that originated from the U.S. increased by 8 percent, a 1 percent uptick from last quarter. Attacks from ROW increased from 14.4 percent to 23.9 percent. Attacks from Europe increased from 18.9 percent to 23.2 percent.



## Fraud by Industry

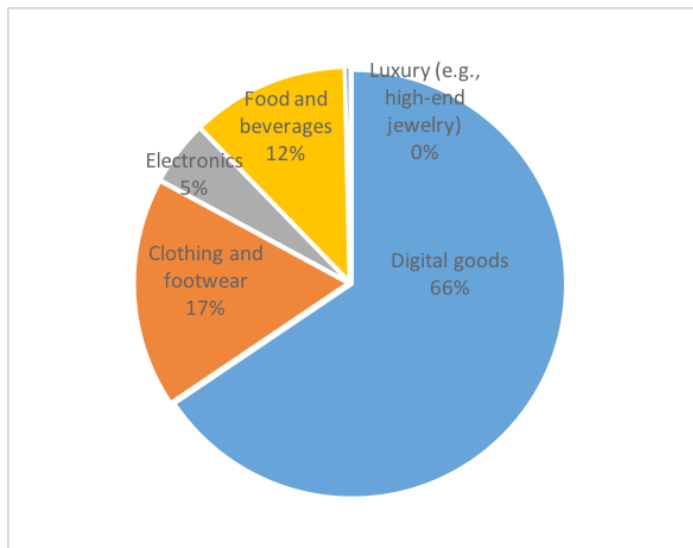
To delve deeper into the nature of fraud attacks, we took a look at five separate industries: digital goods, clothing, electronics, food and luxury.

To start our analysis, we calculated the average dollar value of a transaction for each category. For digital goods, this was \$27, for clothing \$126, for electronics \$279, for food \$88 and for luxury goods (which includes high-end jewelry) \$712.



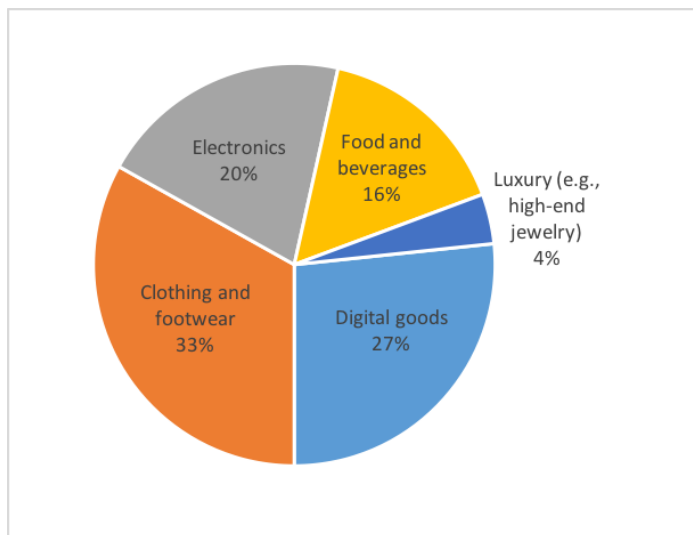
Since the dollar value for transactions can be very high for some of these industries, particularly, digital goods and luxury, it drives up the average. To offset this, we also calculated the percent of transactions that had a lower dollar value than average for these industries. For digital goods, this was 66 percent of transactions, for clothing 17 percent, for electronics 5 percent, for food 12 percent and for luxury 0.3 percent.

**Percentage of Fraudulent Transactions by Industry**



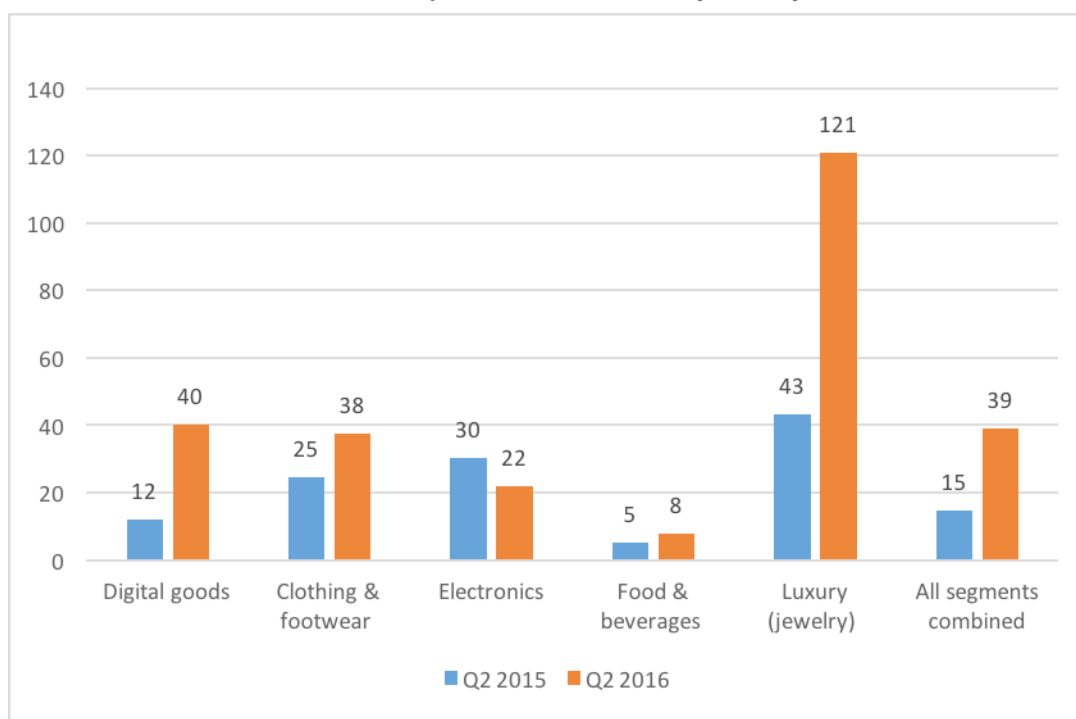
For Q2 2016, the overall industry weight is shown broken into dollar value and number of transactions in these pie charts. Digital goods accounted for 66 percent of transactions, but only 33 percent of the dollar value. On the other hand, jewelry accounted for only 0.3 percent of transactions but represented 4 percent of the total dollar value.

**Value of Fraudulent Transactions by Industry**



The attack rate varied considerably depending on industry. As a benchmark, remember that across all industries, the attack rate averaged out to be 39 out of 1,000 this quarter. Luxury represented the high end, with an attack rate of 121 per 1,000 transactions — a dramatic increase from last quarter, when the rate was 93 per 1,000 transactions. Digital goods, which had a relatively low attack rate in Q2 2015, now has the second highest attack rate. Food and beverage represented the lower end, 8 per 1,000 transactions, up from last quarter's 6 per 1,000 transactions.

**Attack Rate per 1,000 Transactions by Industry**



This shows a comparison of the fraud attack rate for Q2 2015 and Q2 2016 broken out by industry. Below is an examination of fraud attack rates since Q1 2015, which is when we began tracking fraud for this report.

	Attack Rate (per 1,000 Txn)						Potential Cost (% of Revenue)					
	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016
Digital Goods	7	12	25	29	35	40	0.6%	1.8%	6.3%	7.8%	10.8%	13.7%
Clothing & footwear	15	25	20	20	34	38	3.1%	9.6%	4.1%	3.6%	7.2%	7.9%
Electronics	20	30	20	17	25	22	2.9%	5.4%	1.8%	2.6%	3.9%	2.7%
Food & beverage	5	5	3	3	6	8	0.3%	0.3%	0.2%	0.2%	0.4%	0.6%
Luxury (jewelry)	31	43	65	60	93	121	4.9%	5.7%	9.0%	8.6%	9.5%	14.0%
All segments combined	9	15	24	27	34	39	2.0%	4.9%	4.0%	4.4%	6.6%	7.6%

## Methods of Attack

So if fraud is increasing, what are fraudsters doing differently this quarter? Last year during Q2, botnets terrorized merchants by accounting for a full 46 percent of attacks, while simple fraud accounted for a mere 3 percent of attacks.

While botnets still account for a staggering amount of fraud, they are on the decline. This quarter, they accounted for 75 percent of fraud attacks — high, but it's a drop from their all-time peak of 80 percent during Q3 2015.

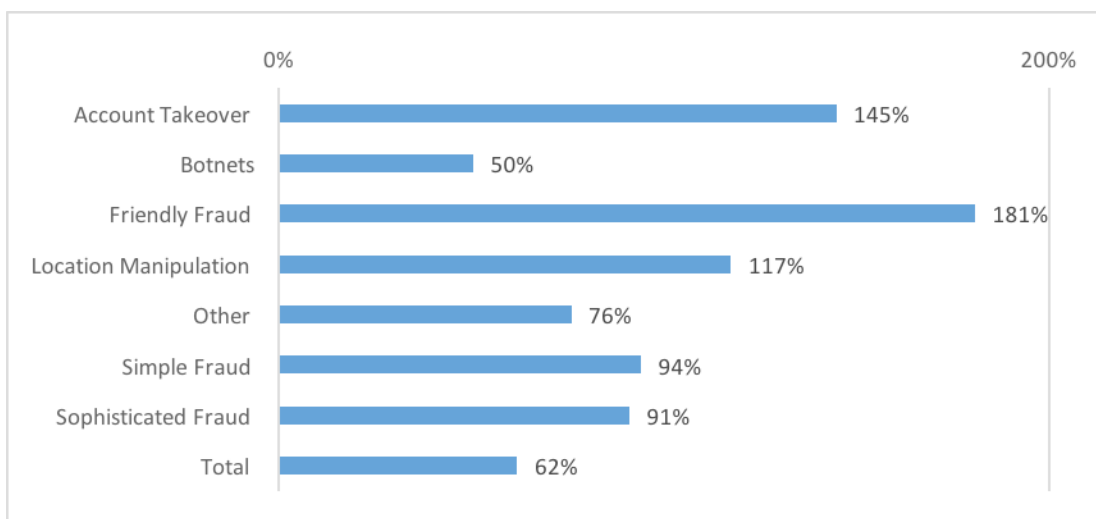
Account takeovers, sophisticated fraud and friendly fraud are on the rise: They each increased by 1 percent this quarter.

Fraud Type	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016
Account takeover	16%	8%	3%	3%	4%	5%
Botnets	34%	46%	80%	81%	77%	75%
Friendly fraud	14%	9%	2%	2%	3%	4%
Location manipulation	11%	7%	3%	3%	5%	4%
Other	18%	18%	8%	7%	8%	9%
Simple fraud	5%	8%	2%	3%	2%	3%
Sophisticated fraud	5%	8%	2%	3%	2%	3%

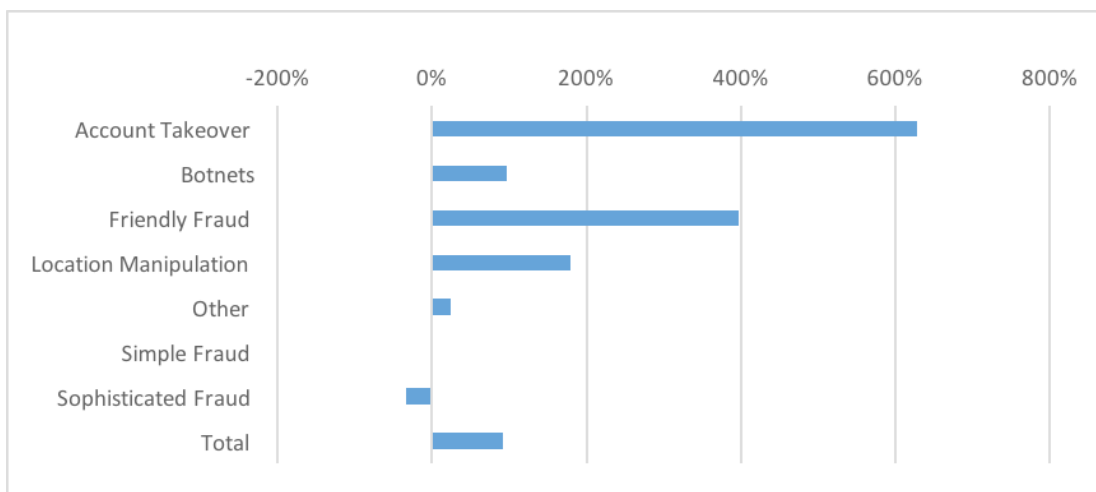
To be able to discuss changes throughout the year, we compared the increase in attack rate and transaction dollars at risk for each method between Q3 2015 and Q2 2016. The highest growth was for account takeovers: The attack rate increased by 145 percent, and the potential cost by 628 percent.

In general, attack rate rose for all categories. However, in the case of potential cost of fraud, every category increased except for sophisticated fraud, which declined by 33 percent.

**Growth in Attack Rate from Q3 2015 to Q2 2016**



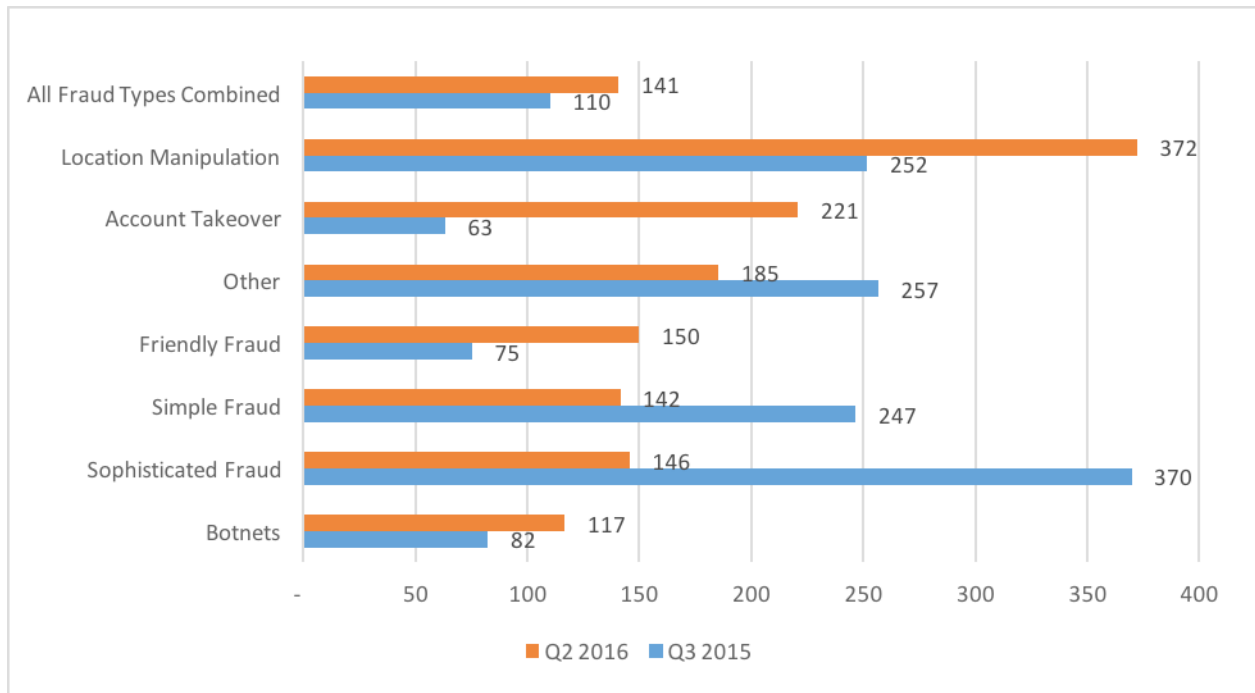
**Growth in the Potential Cost of Fraud from Q3 2015 to Q2 2016**



In terms of cost, the overall dollar amount of an average transaction increased from \$110 in Q3 2015 to \$141 this quarter. Correspondingly, the average value of a fraud attack also increased for some types of fraud. Location manipulation rose from \$252 to \$372, and account takeover sky rocketed from \$63 to \$221.

For other types of fraud, the dollar value decreased. Sophisticated fraud sank from \$370 to \$146, and simple fraud from \$247 to \$142.

**Average Attack Amount (\$) by Type of Fraud**

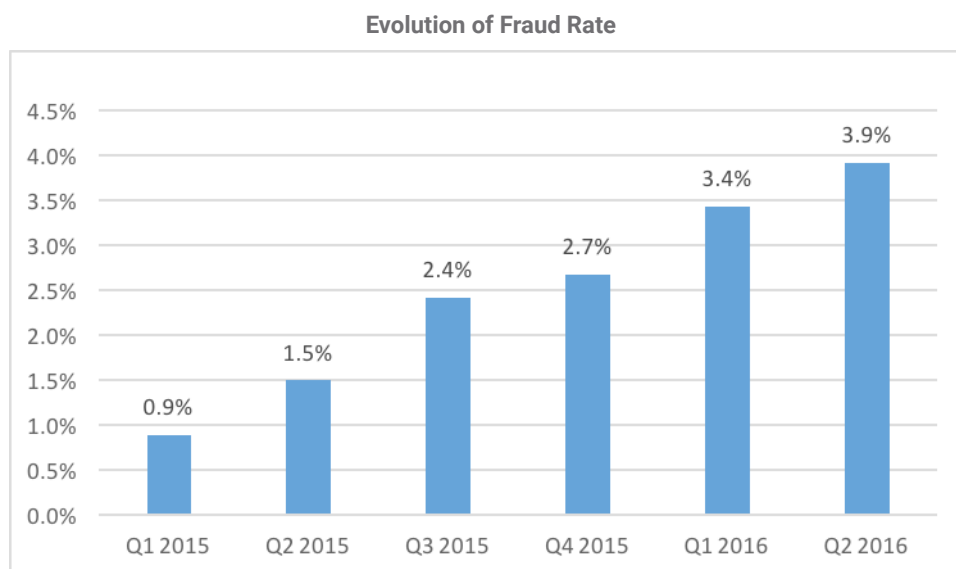


When botnets represent 75 percent of fraud attacks, there's a tidbit of good news: Their average transaction value is lower than the rest of the fraud types. As a result, botnets accounted for 62 percent of transaction dollars subject to attack during Q2 2016.

Fraud Type	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016
Account takeover	5%	6%	2%	4%	7%	10%
Botnets	28%	19%	62%	66%	58%	62%
Friendly fraud	15%	5%	2%	4%	6%	5%
Location manipulation	20%	16%	6%	7%	10%	7%
Other	26%	41%	18%	12%	14%	12%
Simple fraud	4%	5%	2%	1%	1%	1%
Sophisticated fraud	3%	7%	8%	5%	3%	2%

## Deep Dive – Attack Rate

The fraud attack rate has been growing steadily each quarter since we first put out this report. During the first two quarters, we analyzed the increase in fraud rate, which was staggering: a 69 percent increase from Q1 2015 to Q2 2015 and a 62 percent increase from Q2 2015 to Q3 2015. Since then the attack rate has continued to increase, but at a slower pace: 10 percent from Q3 2015 to Q4 2015, 29 percent from Q4 2015 to Q1 2016 and 14 percent from Q1 2016 to Q2 2016.

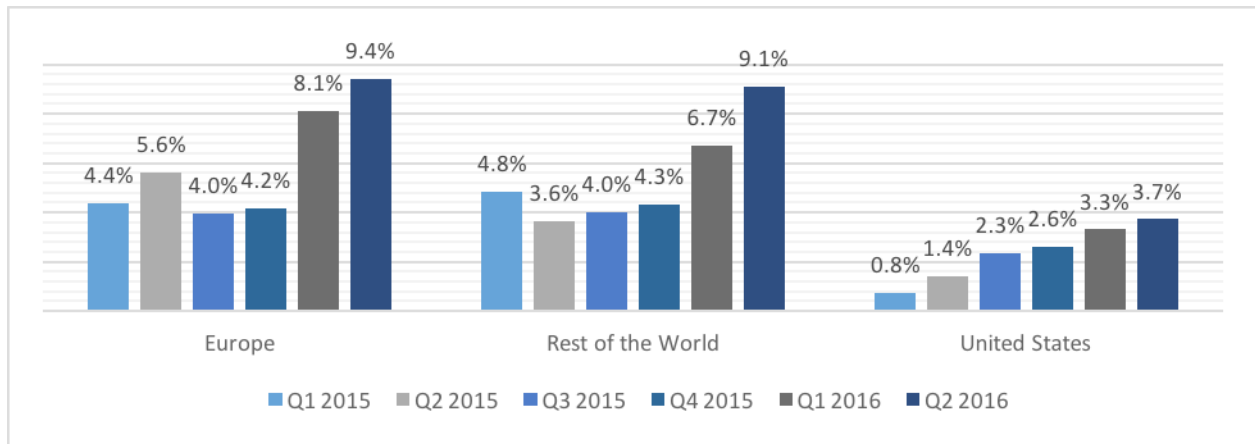


In terms of fraud origin, although the attack rate is growing steadily but slowly in the U.S., the U.S. was the originator of the fewest number of attacks during all periods analyzed.

In Europe, the attack rate was volatile. It decreased from 5.6 percent in Q2 2015 to 4 percent in Q3 2015. Then from Q4 2015 to Q1 2016, it jumped from 4.2 percent to 8.1 percent, an increase of 94 percent. From last quarter to this quarter, the attack rate increased more slowly: by 16 percent.

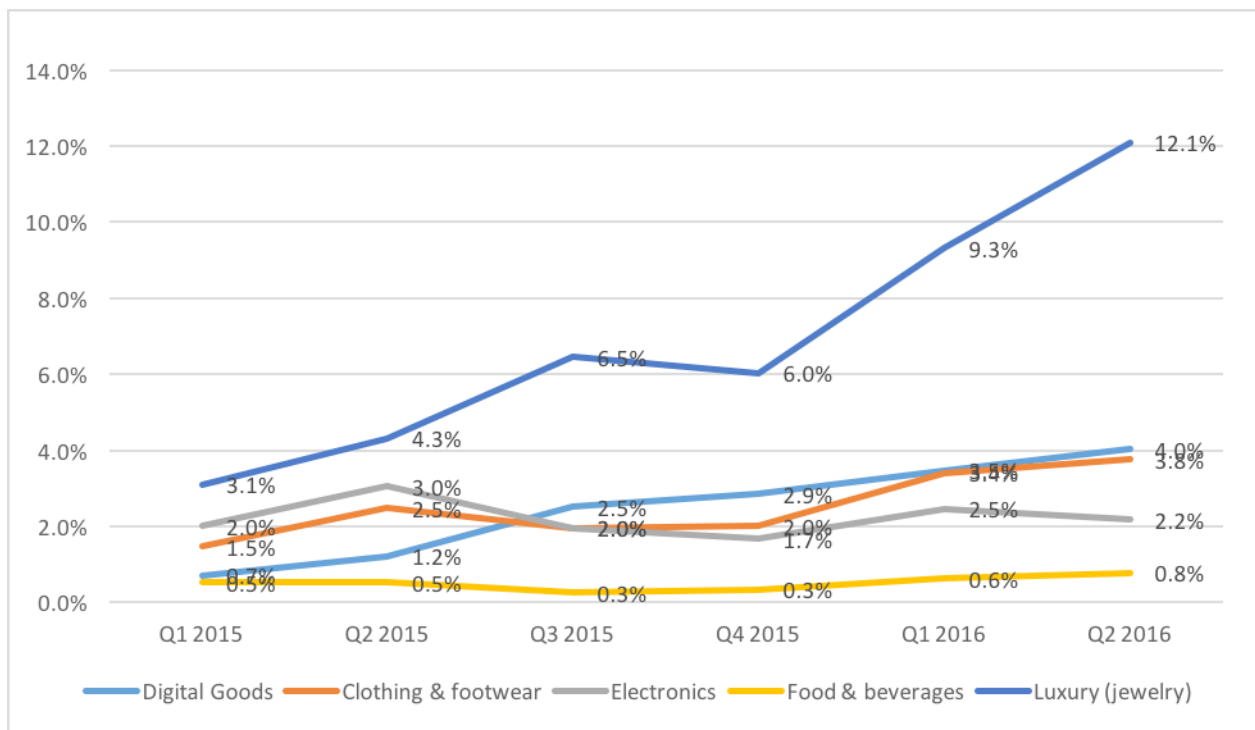
Fraud attacks in ROW were similarly volatile. The attack rate decreased from 4.8 percent in Q1 2015 to 3.6 percent in Q2 2015. However, it increased by 55 percent from Q4 2015 to Q1 2016 and then by 36 percent from Q1 2016 to Q2 2016.

Fraud Attack Rate by Point of Origin



We also analyzed the attack rate for each industry.

Fraud Rate by Industry





In general, attack rates have increased for all industry segments: some drastically, some with more volatility. Unsurprisingly, Luxury had the highest attack rate and Food and Beverage the lowest rate.

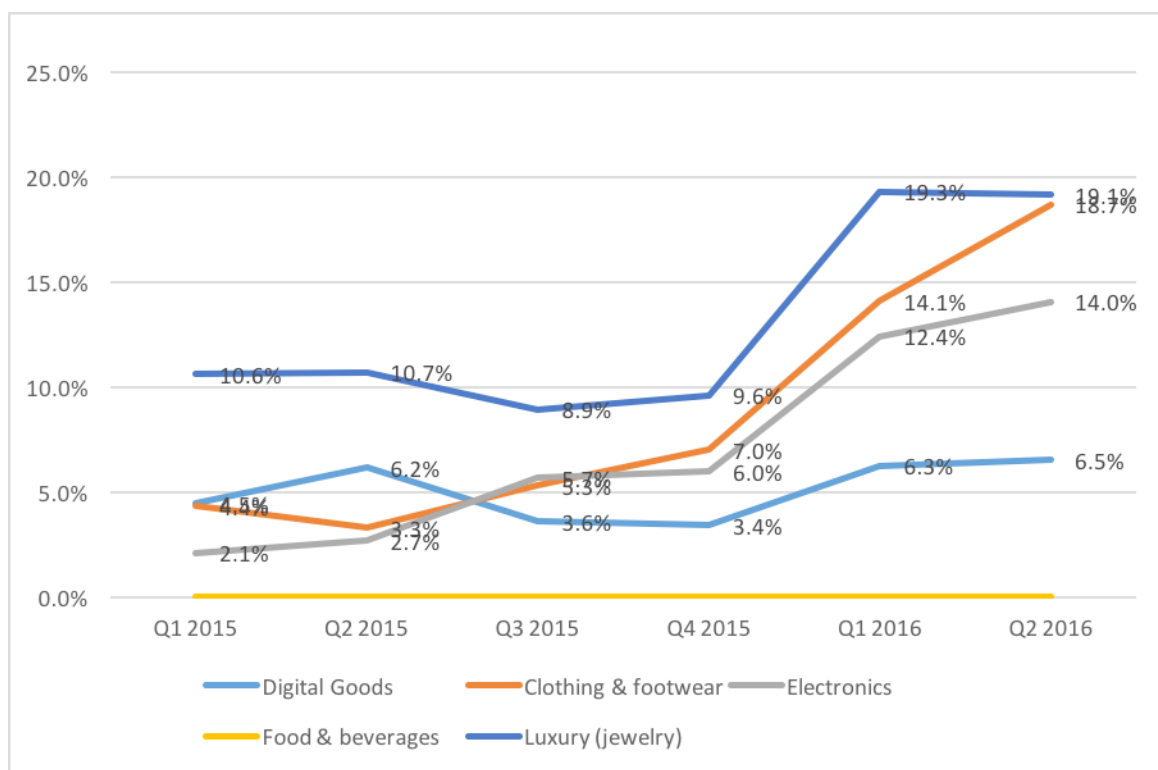
Digital Goods increased from 0.71 percent in Q1 2015 to a rate of 4.03 percent during Q2 2016, an increase of 469.13%. During the same period, Luxury increased by 290 percent and electronics by 156 percent.

Clothing and Footwear actually dropped from Q2 2015 to Q3 2015 by 26.5 percent and then rose again, to 3.76 percent in Q2 2016.

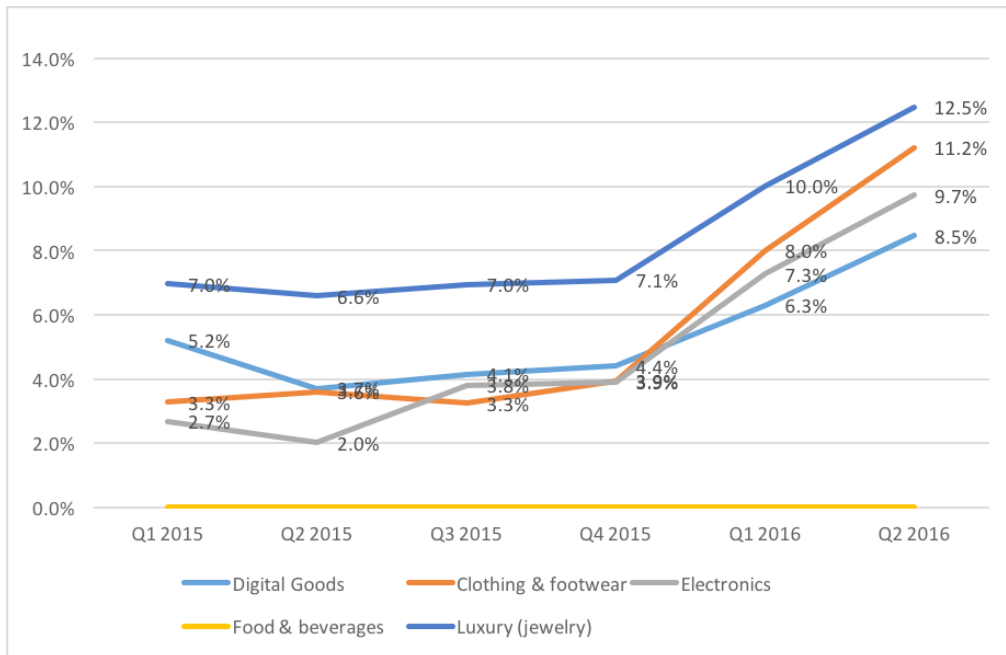
Food and Beverage also dropped between Q2 2015 and Q3 2015 from 0.26 percent to 0.52 percent. It then increased by 31 percent from Q3 2015 to Q4 2015, 85 percent from Q4 2015 to Q1 2016 and 24 percent from Q1 2016 to Q2 2016.

We also took a look at how fraud origination point differs across industries. For all three regions – U.S., Europe, and ROW – Luxury has the largest fraud rate. For Europe and ROW, Clothing and Footwear comes in second place. In Europe, in particular, the attack rate on Clothing and Footwear is high: 18.7 percent during Q2 2016 vs. 3.4 percent in the U.S. Additionally, in the U.S., the difference between Luxury and the other industries was particularly steep.

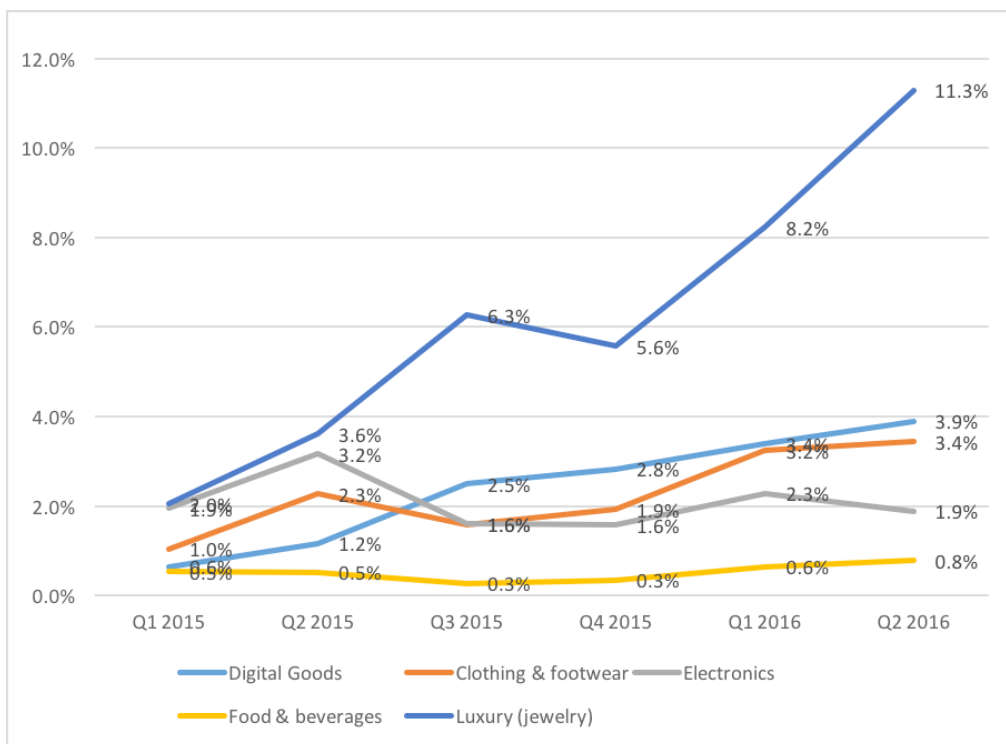
Attack Rate in Europe



### Attack Rate in RoW

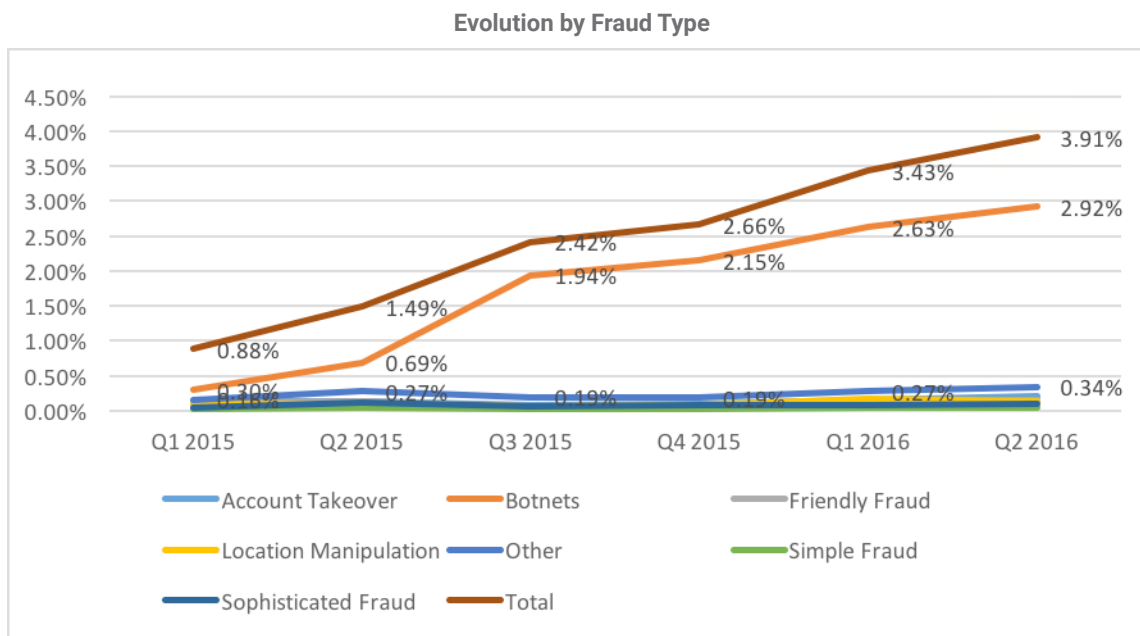


### Attack Rate in the U.S.



Much of the steady growth in attack rates seems to be increasingly driven by botnets, which have now become the favorite tool for fraudsters among all fraud types.

We analyzed each industry to weigh the effect of botnets on their performance. Just between Q1 2015 and Q2 2016, the attack rate for botnets increased by a solid 882 percent.



In most industries, except for Food and Beverages, botnets account for the majority of fraud attacks.

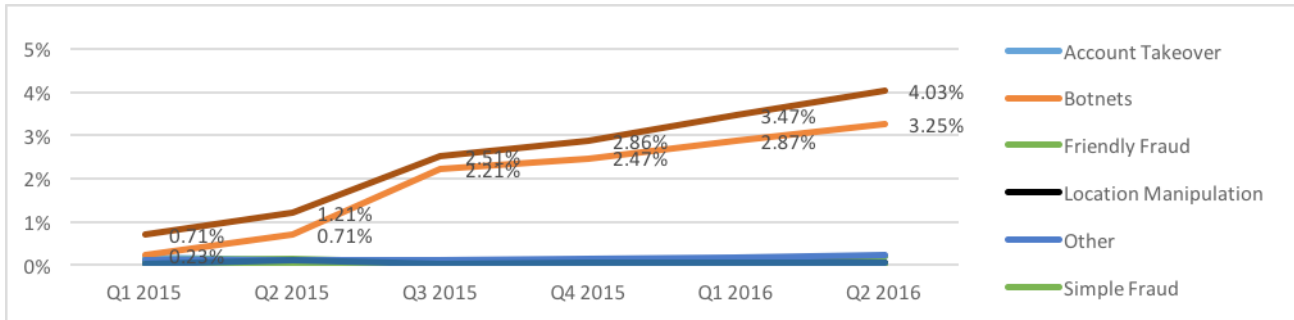
In Digital Goods, botnets grew by 20 percent from Q1 2015 to Q2 2015 and by 210 percent from Q2 2015 to Q3 2015 and then continued growing at an average rate of 13.8 percent.

For Clothing and Footwear, until Q2 2015, botnets was not the main cause of fraud. But after Q2 2015, the botnet rate of fraud grew to 2.19 percent by Q2 2016, while other types of fraud remained below 0.5 percent.

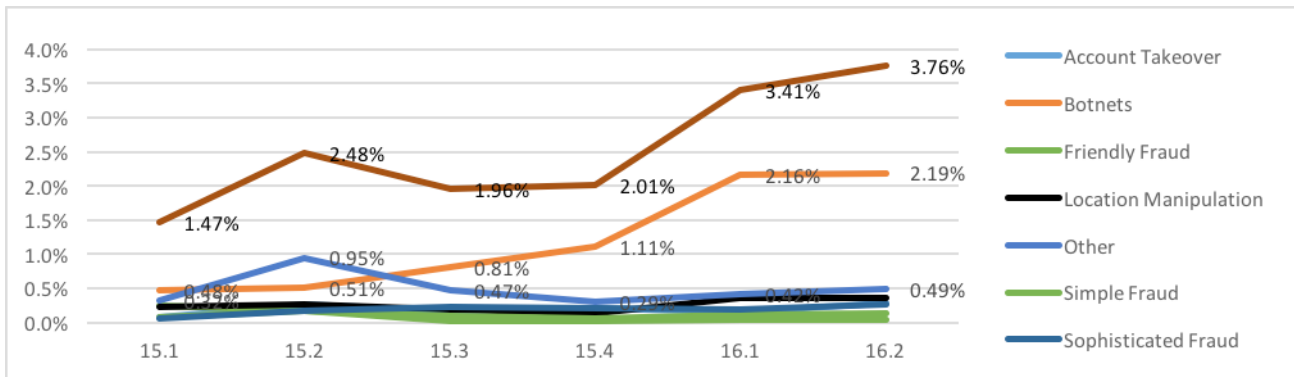
For Electronics, the botnet fraud rate actually dropped from 0.8 percent in Q1 2015 to 0.53 percent in Q2 2016.

In the Luxury industry, the botnet attack rate dropped by 12 percent in Q4 2015 and then grew by 40.5 percent the following quarter, growing again by 53 percent during Q2 2016.

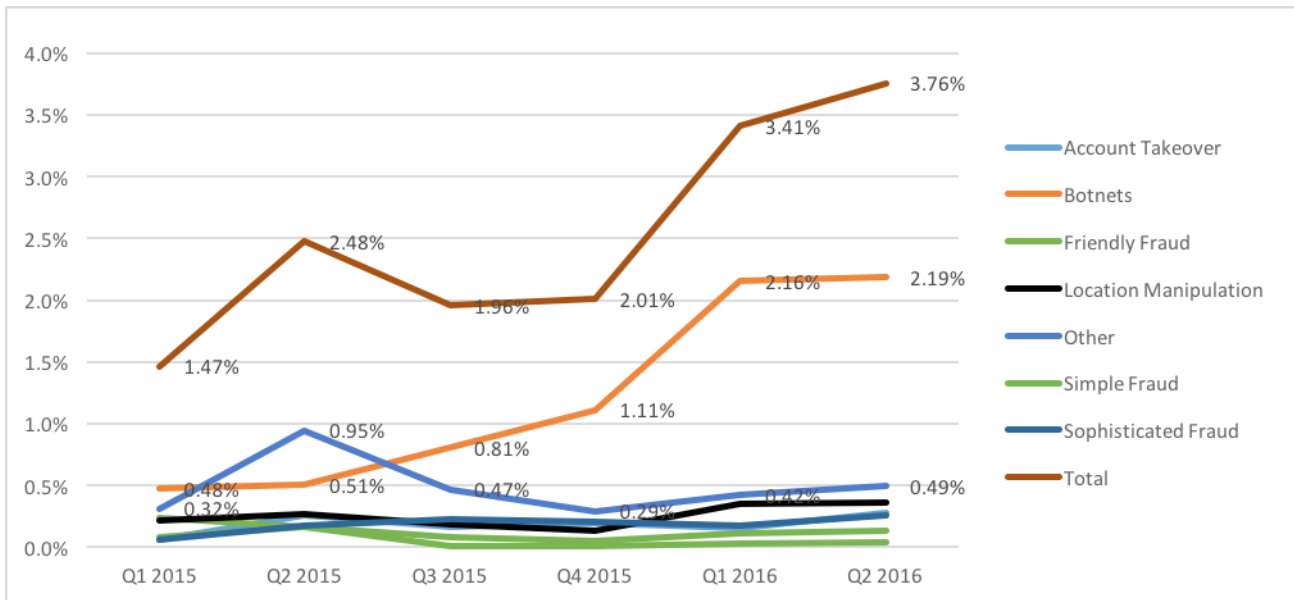
Digital Goods Fraud as a Percentage of All Transactions



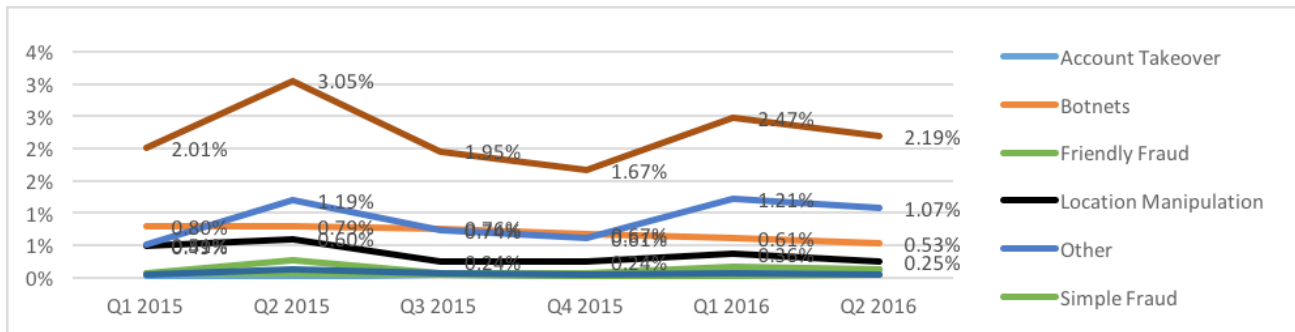
Clothing & Footwear Fraud as a Percentage of All Transactions



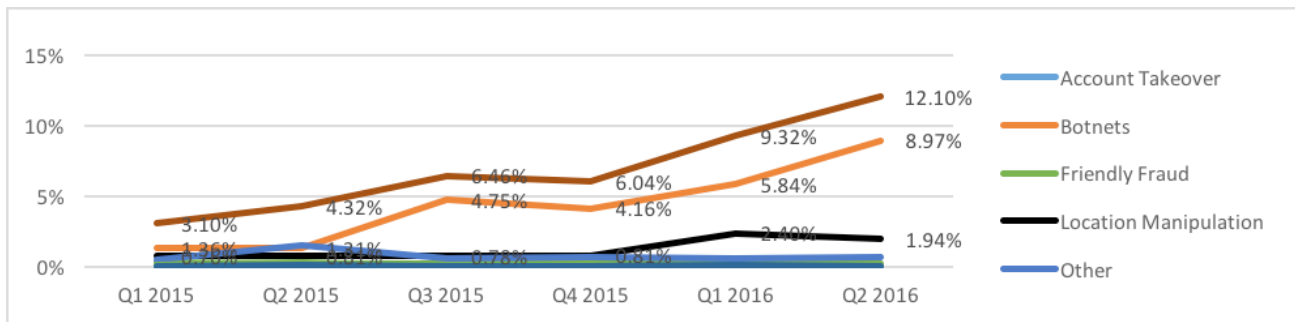
Clothing & Footwear Fraud as a Percentage of All Transactions



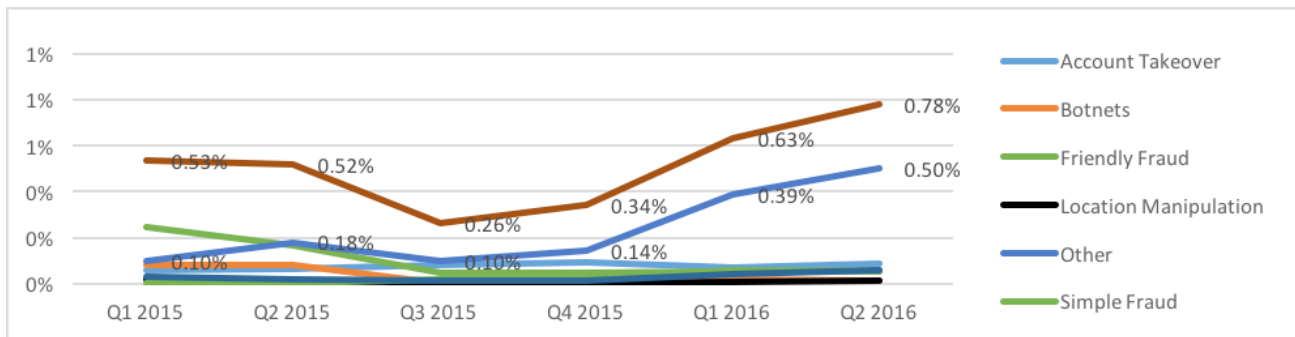
Electronics Fraud as a Percentage of All Transactions



Luxury Fraud as a Percentage of All Transactions



Food & Beverage Fraud as a Percentage of All Transactions

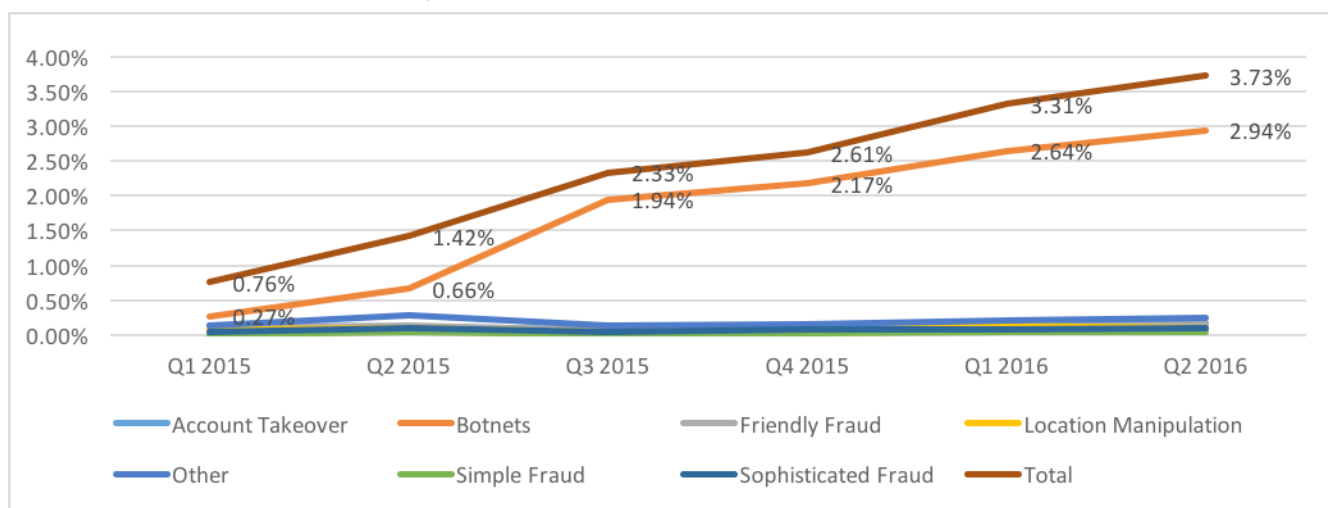


While we're on the subject of botnets, let's discuss them by region. In U.S., botnets have always been the most significant cause of fraud, while the other types have been negligible. However, this is not the case for Europe and ROW.

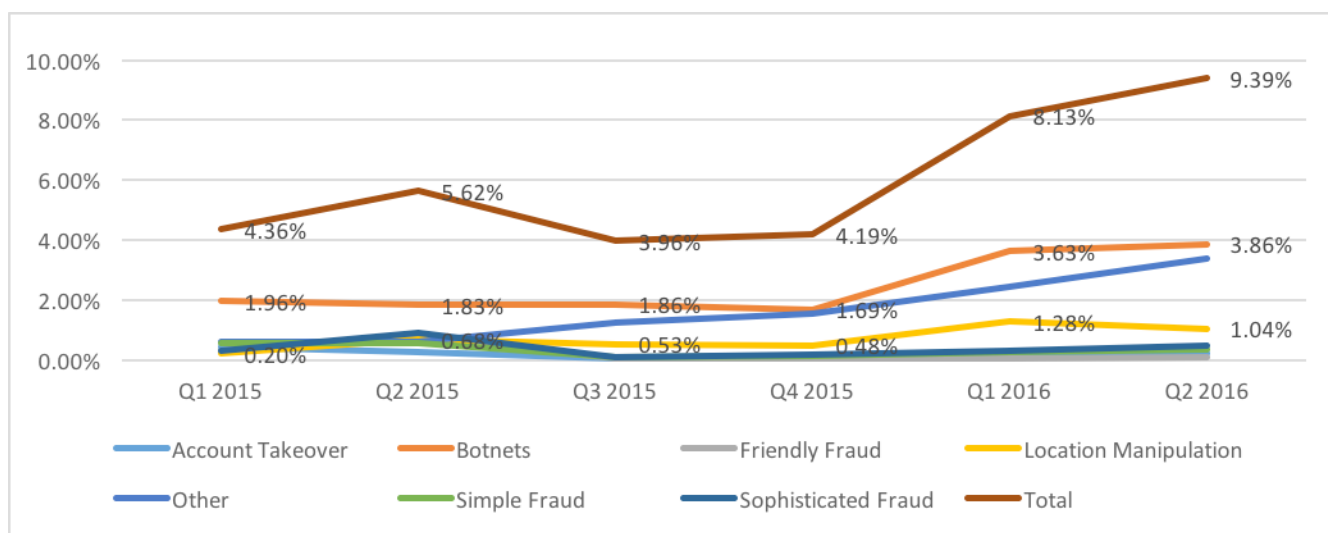
In Europe, botnets had small variations until the last quarter of 2015, then grew 115 percent for the first quarter of 2016.

Finally, in ROW, all causes of fraud had small variations during 2015, with botnets mirroring this pattern. The real standout is account takeover, which showed an increase of 112 percent during Q1 2016.

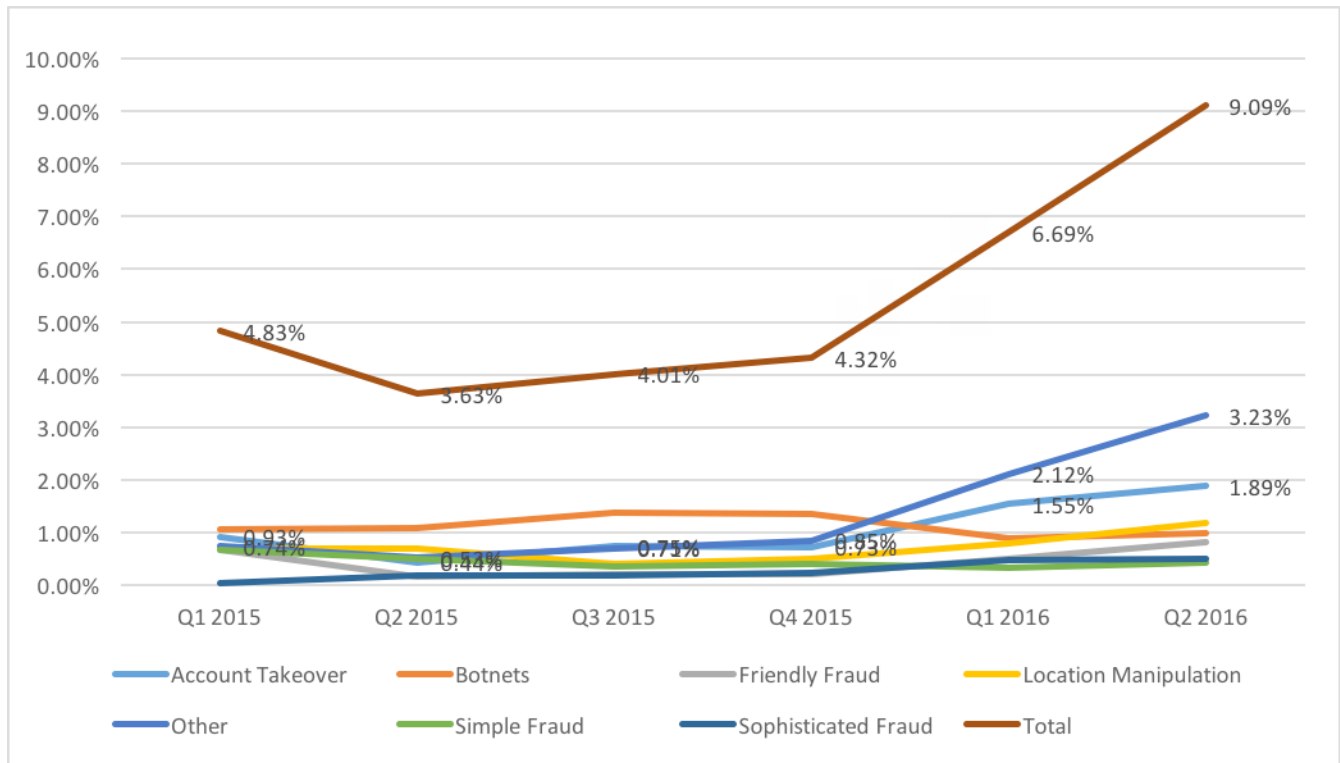
**Types of Fraud Attacks Affecting U.S. Merchants**



**Types of Fraud Attacks Affecting European Merchants**



Types of Fraud Attacks Affecting RoW







## The Ever More Frightening Task of Fighting Fraud

It's no secret that hackers and other bad actors are getting smarter every day, and the results from the latest October 2016 Global Fraud Attack Index™, a PYMNTS/Forter collaboration, paint a rather depressing picture for online retailers and their fight against fraudsters.

According to the Index research, these fraudsters are finding better results than ever before. The fraud attack rate went up by a whopping 62 percent between Q3 2015 and Q2 2016, whereas fraud attacks grew by 15 percent compared to Q1 2016.

As fraudsters develop new, sophisticated methods of intrusion that allow them to increase the amount of attacks levied, online retailers are being pushed to invest time and money to protect their businesses and customers. And with the holidays and surge in purchasing that accompanies them right around the corner, merchants need to be ready to stop fraudsters in their tracks.

According to Liz Garner, vice president of the Merchant Advisory Group, as more consumers turn to eCommerce solutions for their holiday and year-round shopping stops, many digital retailers are investing heavily in security solutions in order to safeguard their online businesses.

"Online sales nearly quadrupled in the past decade and now account for roughly \$340 billion in total retail sales," Garner said, citing statistics from the U.S Department of Commerce. "I think some of the increase is due to just that general growth in eCommerce transactions."



## The Ever More Frightening Task of Fighting Fraud

PYMNTS recently caught up with Garner to discuss the risk of fraud for online merchants and what can be done to fight fraud.

### **More digital dollars, more (fraud) problems**

According to the Index research, digital retailers are at a higher risk of fraud than any other segment, making the continuous uptick especially scary for eCommerce merchants.

For Q2 2016, digital goods were the most popular target for fraudsters, measured by the number of transactions. Nearly 66 percent of online attacks were targeted at digital retailers, greater than triple the number of attacks aimed at the next highest category, traditional clothing and footwear stores.

In Q2, every 40 out of 1,000 digital good transactions were targeted by fraudsters — up from just 12 out of 1,000 transactions a year before.

Garner attributed this increase to a spike in the amount of overall online spend. As business is increasingly conducted over the web, fraudsters have become attracted to digital malfeasance as well, she said.

### **The ever-rising cost of doing business amidst fraud**

As shoppers turn to eCommerce stores for their shopping needs, thanks in large part to the convenience online shopping provides, fraudsters are also taking their business online. The Index research indicates that merchants like the ones that work with Garner are investing greater sums of money in fraud prevention.

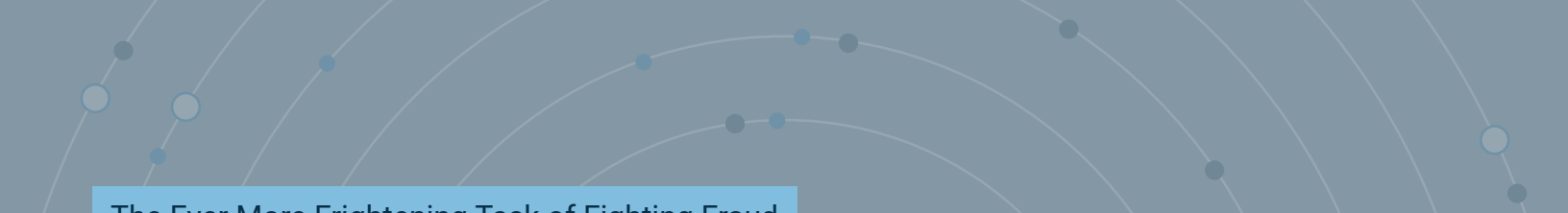
Rising investment in fraud prevention indicates at the rising cost of fraud. A year ago, merchants could anticipate that a tiny fraction of their profits, less than \$2 for every \$100 spent, would be subject to fraud. That number has quickly quadrupled to \$8 per \$100 spent over the past year, and merchants are having to do more to combat it.

While the increase in digital sales is a boon for merchants that conduct business online, it's also been a profitable rise for fraudsters. Garner noted that most merchants spend up to 40 percent more on fraud prevention than they actually lose to bad actors every year.

As business has shifted to the online ecosystem and financial wrong-doers have followed suit, merchants must take greater care to protect themselves from criminals, she said.

"Because it's such a huge part of a lot of merchants' businesses, merchants are constantly developing tools and investing money in fraud prevention," Garner said.

“In Q2, every 40 out of 1,000 digital good transactions were targeted by fraudsters — up from just 12 out of 1,000 transactions a year before.”



## The Ever More Frightening Task of Fighting Fraud

### Investing in the right places

So how can companies fight this seemingly unending increase in fraud without breaking the bank?

With so much being spent to thwart online fraud, Garner said that it is crucial that companies spend their money on the best possible fraud solutions.

Garner said that many sophisticated retailers invest in solutions that offer a deep and multi-leveled plan for stopping bad actors, as well as ones that have found success in a wide range of industries.

She pointed toward travel providers, particularly airlines, as an example of a vertical that is leading the way in fighting fraud. The difference maker, according to Garner, is data.

“Airlines are a great example of a situation where you’re collecting a little bit more data about your customer in order to issue an airline ticket,” she said. Garner cited international travel as a particularly good example of this, since a known traveler ID, a passport, and other required items can help airlines get to know their types of customers better.

Loyalty programs are another way for some companies to potentially gain an advantage on fraud. According to a high-level, Fortune 500 travel company executive PYMNTS spoke with on background for this story, loyalty programs can help companies identify whether a customer is who they claim to be.

“At the heart of it, a loyal customer is someone who has been in your store before,” the executive explained. “From that, we can judge elements they’re bringing to a transaction that should be the same on the first, second, third and each subsequent trip. If those elements don’t line up, if they aren’t consistent, then that shows you should reconsider whether this transaction is authentic.”

By this notion, the fraud fight may be, in large part, all about crunching data.

### What is the Index?

The Global Fraud Attack Index™ measures the growth (or decline) of attempted fraud<sup>3</sup> on U.S. merchant websites. It also quantifies the potential cost (if left unchecked) to merchants, based on average attack amounts and how these amounts are trending over time.

### Index Baseline

This Index was created by evaluating the attack rate relative to the average fraud rate during 2015. Specifically, we calculated the fraud rate for each of the four quarters during 2015, followed by the average of the four quarters, using that as the Index base.

The fraud rate per 1,000 transactions for the first four quarters of 2015 was 9, 15, 24 and 27, respectively. That averages to 18.6, and this became the Index baseline. Since the attack rate for Q1 2016 increased to 34, it was 85 percent greater than the 18.6 Index baseline. We consider the Index baseline to be 100, and therefore the Index value of Q1 2016 is 185.

### 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, primary merchant segment and 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. This data was separated by transactions and fraud attempts that originated in the U.S., Europe and ROW.

The U.S. attack rate is equal to the percentage of U.S. consumers buying from U.S. 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 U.S. to a European country that was an attempt at fraud (both successful and unsuccessful). For ROW, the attack rate was equal to the percentage of cross-border transactions from the U.S. 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 try to steal through their efforts to commit fraud. This is the average of all attacks, by region, product type and the type of fraud being attempted.

---

<sup>3</sup> Attempted fraud is defined as all sales transactions which are identified as potential fraud, both successful and unsuccessful

### 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 were successful. The calculation is simple once all the data is collected.

$$\text{Potential Cost of Fraud (\%)} = (\# \text{ of Txn} * \text{Attack Rate} * \text{Avg Attack Amount}) / \text{Total eCommerce revenue}$$

Data for the attack rate and average attack amount was provided by Forter and described above.

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

### 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 starting in 2013. However, data for total quarterly eCommerce sales is 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:

$$\text{Segment eCommerce Sales}_{\text{current quarter}} = \text{Total eCommerce sales}_{\text{current quarter}} * (\text{segment sales in 2013} / \text{Total eCommerce 2013})$$

The U.S. Census Bureau provides data at a three-digit North American Industry Classification System (NAICS) level and a breakout of sales by product type for all “non-store retailers” based on NAICS code 454 (some of the product groups are more detailed than a three-digit level). In these cases, we used 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 assumed 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 the same for total sales and eCommerce sales. We used this ratio to estimate eCommerce sales during 2015 for categories that were more detailed than three-digit NAICS codes would allow.<sup>4</sup>

---

<sup>4</sup> 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 programming 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 messenger 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 722 Food service and drinking places less 7224 drinking places and 722511 full service restaurants)

### Number of Transactions

The total number of eCommerce transactions was 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 was 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 the U.S. Census Bureau as described above and, for the other regions, we had to estimate the cross-border eCommerce from the U.S. to Europe and to ROW.

We relied on third-party research stating that cross-border sales from the U.S. were 8.7 percent of all U.S. eCommerce sales.<sup>5</sup> In addition, 47 percent of those sales were to Europe.<sup>6</sup>

We estimate the value of transactions in each region.

- The value of U.S. transactions was from the data.
- Value of European transactions = (Value of U.S. transactions) \* (8.7/100) \* (47/100).
- Value of transactions in ROW = (Value of U.S. transactions) \* (8.7/100) \* (1 - 47/100).

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

---

<sup>5</sup> U.S.: Cross-Border ECommerce Report; Critical Facts and Insights for International Expansion, Update 2014, The PayPers, <http://www.thepaypers.com/news-and-reports/us/5>

<sup>6</sup> Ibid.

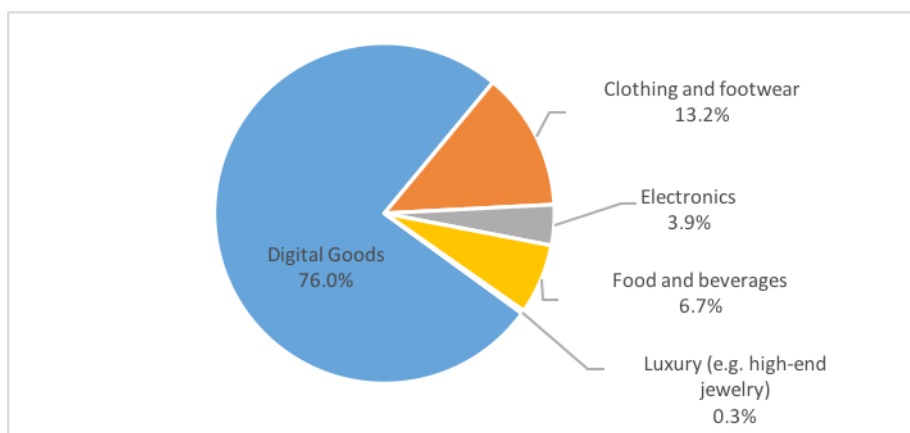
### Merchant Segments

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.
- Food and Beverage: food delivery (Local messenger 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 minus 7,224 drinking places and 722,511 full-service restaurants)
- Electronics: direct sellers and retailers of electronic goods, including laptops, tablets, e-readers, smartphones and accessories
- Food and Beverages: digital food delivery requests including grocery
- Luxury: high-end brand merchandise including clothing, jewelry and accessories (e.g., Rolex, Louis Vuitton, etc.)
- Digital Goods: e.g., gift cards, eBooks, music, gaming; also includes business-related virtual services such as hosting and software solutions

We calculated total results as an average of the industry results weighted by total sales in each of the industry segments we covered. We considered the segment weighting to reflect fraud activity by aggregating based on the total number of eCommerce transactions of all U.S. merchants.

Weight of Segments Included in this Index



### **PYMNTS.com**

[PYMNTS.com](https://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.

### **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](mailto:globalfraud@pymnts.com).

## Disclaimer

The Global Fraud Attack Index™ a PYMNTS/Forster 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.