

GLOBAL FRAUD ATTACK INDEX™

Third Quarter 2016

ATTACK INDEX

↑ 137%



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

Q1 2015
\$1.89

Q1 2016
\$7.30

↑ 386%

Dollars at risk per \$100 of sales

↑ 186% Digital Goods

↑ 38% Luxury Goods

↓ -19% Clothing

↑ 21% Electronics

↑ 116% Food/Beverage

↑ 137%
Total Fraud

Change in fraud attacks by industry

Acknowledgment

Sponsorship for the PYMNTS Global Fraud Attack Index was provided by Forter. Forter has no editorial influence over the Index's content. In addition, 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

↑ 137%

Attack rate more than doubled between Q2 2015 and Q1 2016 (attack rate refers to the percent of transactions that experienced fraud attacks in Q4 2015 compared to Q1 2015)

27

Fraud attacks are up 27% between Q4 2015 and Q1 2016 —typically we would expect fraud attacks to increase after holiday season, but not by such a large amount

\$7.30

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

Up \$3.10 (73%) out of every \$100 from Q3 2015

Up \$2.50 (52%) out of every \$100 from Q4 2015

34

Attacks per 1,000 transactions in 2016 Q1

Up 19 attacks per 1,000 transactions (a 126% increase) from Q2 2015,

Up 7 attacks per 100 transactions (a 26% increase) from Q4 2015

\$10.80

out of \$100 are at risk for digital goods

79

Percent of fraud attacks deployed by botnets (networks of infected computers)

4%

Account takeovers represent 4 percent of total fraud volume

3X

Attack Rate Almost Tripled for digital goods between Q2 2015 and Q1 2016

2X

Attack Rate More than Doubled for luxury goods between Q2 2015 and Q1 2016

The Global Fraud Attack Index Report

Fraud looms like a black cloud on the horizon. Will a monumental storm hit at any moment? Or will it be a slow, steady downpour that wears away at profit margins? Data breaches and the resulting loss of client trust and reputation, plus the clean-up expenses, have cost executives and managers their jobs. The lack of appropriate precautions, including prevention tools, detection techniques, and, worse, the inability to contain the storm once it hits, can bring an entire business to its knees.

According to one study, [annual fraud costs](#) for U.S. retailers reached a staggering \$32 billion in 2014.¹ In 2015, retailers lost an estimated 1.3% of revenue – more than double the rate of 2014.²

Worse, no matter what, fraudsters always seem to be one step ahead. It's their job to figure out how to breach a system and they do it well. Plug one hole and they'll come in through another.

But what if we envisioned a different world? One where merchants are armed with the same tools fraudsters use, but this time to protect their clients. Innovations like machine learning, combined with human expertise, research and experience, offer merchants not only the ability to withstand the storm, but to avoid it all together.

Forter and PYMNTS.com have partnered 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 are monitoring fraud attempts, reflected as a percent of U.S. sales transactions, on U.S. merchant websites. How big is the storm? Where is it? How is it changing? Read on to find out.

For each of the Index editions in 2016, we are using the fraud rates observed in 2015 as a benchmark for comparing the state of fraud each quarter.

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 FraudSM study

³ The rate of fraud attempts is measured as the number of fraudulent attempts on all of sales transactions.

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.

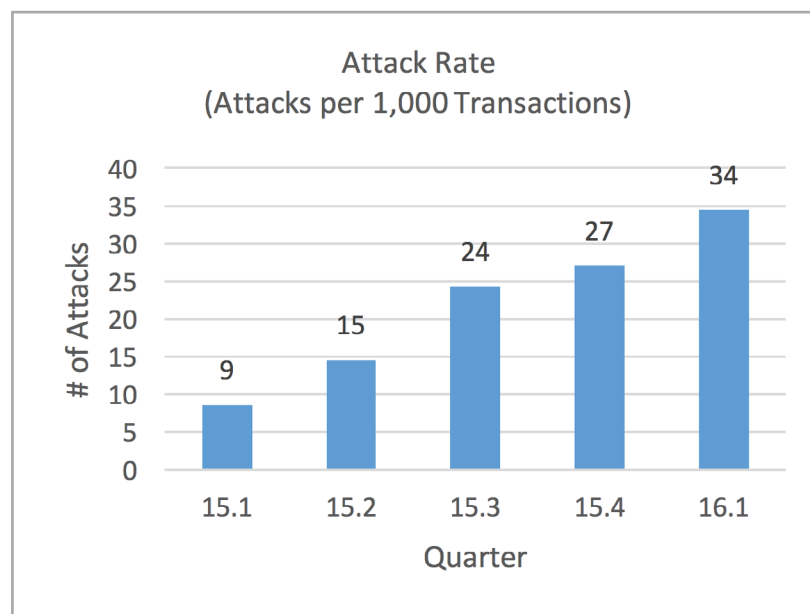
2015 and Q1 2016 in Online Fraud

There was a dramatic growth in the rate of fraud attacks all through 2015 and the first quarter of 2016.

This is a sharp deviation from the norm. Typically, fraud rates drop in Q4 of every year since the volume of transactions go up due to holiday shopping. Post-holiday season, in Q1, an increase in fraud rates is expected since the volume of transactions drops down.

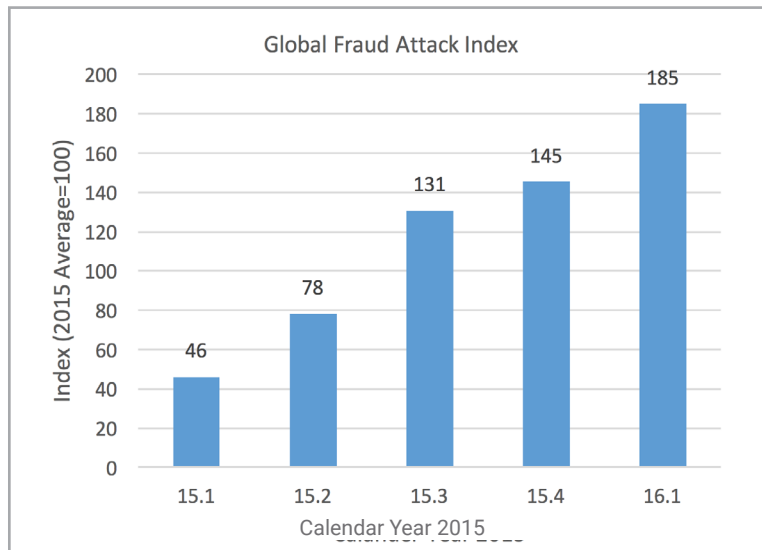
However, the steady increase in fraud rates throughout 2015 drowned out the decline we'd normally expect to see from holiday shopping during 2015 Q4. Furthermore, the uptick in fraud rates we've seen this Q1 is far larger than expected.

There were 34 fraud attacks for every 1,000 transactions in Q1 of 2016, compared to 15 out of 1,000 observed during the second quarter of 2015. That's an increase of 126%. In addition, fraud attack rate has increased from quarter to quarter. From Q3 of 2015 to Q4 of 2015 the fraud rate increased by 11%; from Q4 2015 to Q1 2016 it increased by a solid 26%.



Going by our fraud attack index, the value of the index in Q1 2016 is 185, which means that the current attack rate is 85% higher than the average rate during 2015.

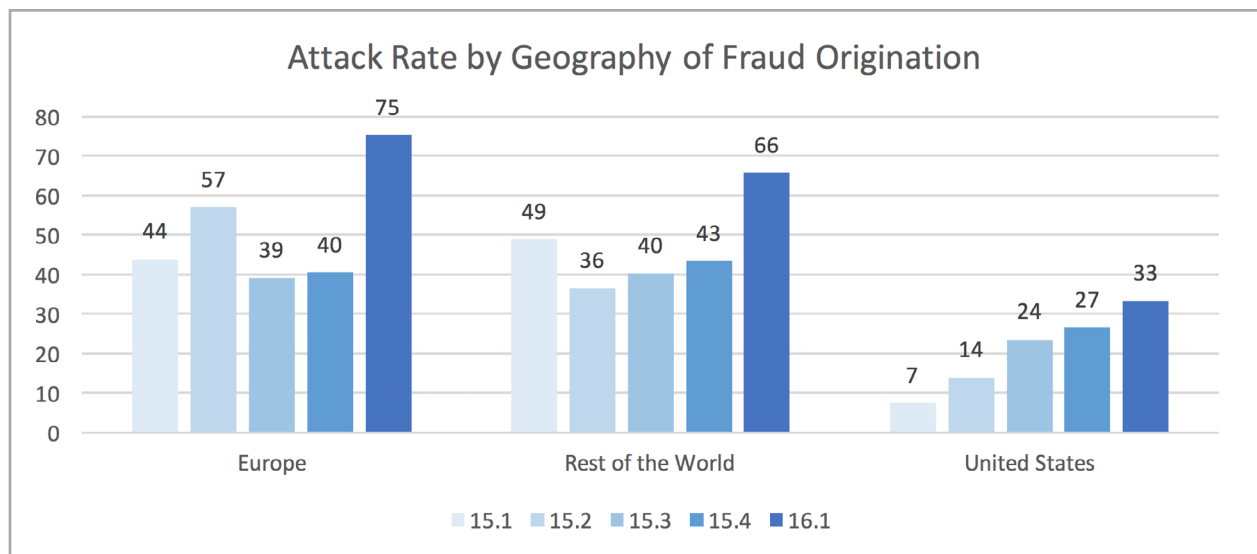
The Global Fraud Attack Index Report



To dig deeper, we sorted cases of fraud attacks on U.S.-based merchants by analyzing transactions that shipped inside the U.S., to Europe or to other parts of the world (ROW).

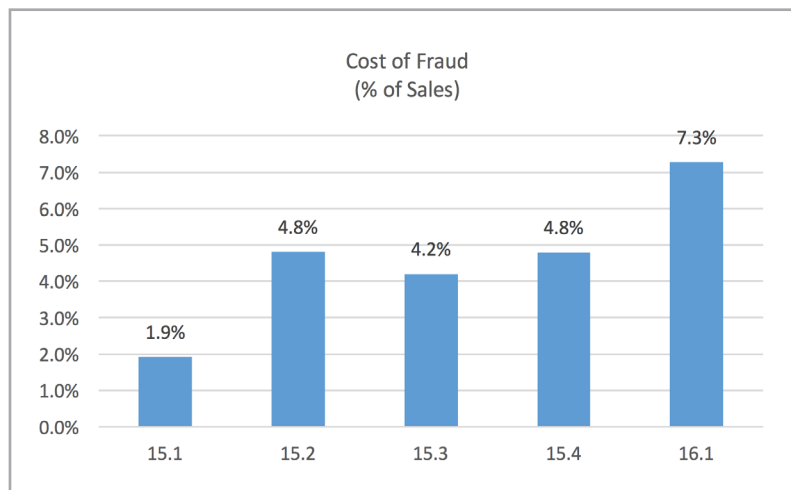
Transactions within the U.S. received the fewest attacks, transactions from European customers generated 127% more attacks than domestic transactions, and the ROW 200% more attacks.

Transactions to the U.S. also saw the smallest increase in its fraud rate since last quarter. The fraud rate increased 22% from 2015 Q4 to 2016 Q1 in the U.S., 88% for Europe and 53% for the ROW.



The Rising Cost of Global Fraud

The potential cost of fraud continues to rise. Between Q2 2015 and Q1 2016, the fraction of dollars that were hit with fraud attacks increased by 250 basis points from 4.8% in Q2 2015 to 7.3% in Q1 2016. At the beginning of 2015 less than \$2 out of \$100 was subject to a fraud attack. However, by Q1 2016, that increased to \$7.3 out of every \$100. This increase could take a significant toll on a retailer's profits.



When we compared the quarterly increase of the potential cost of fraud, we saw it increase by 14% from Q3 2015 to Q4 2015 and 52% from Q4 2015 to Q1 2016. Even though the cost of fraud has increased everywhere, the increase was most significant outside of the U.S.

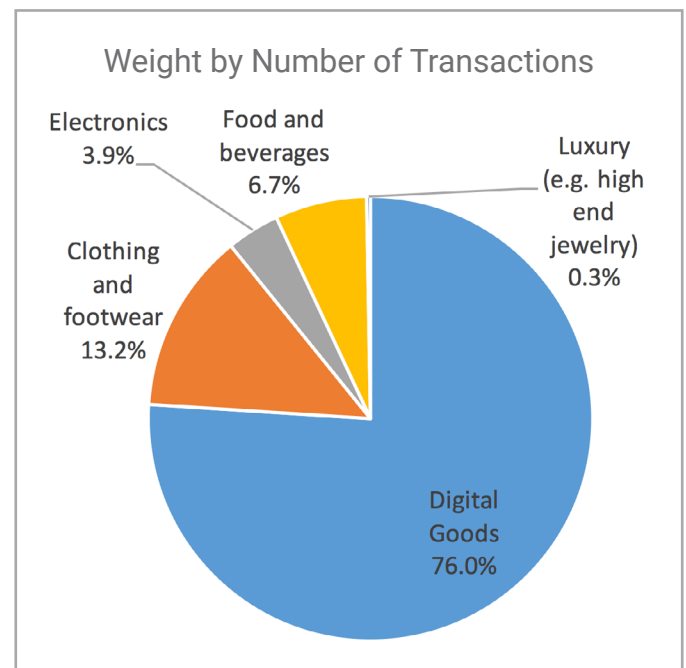
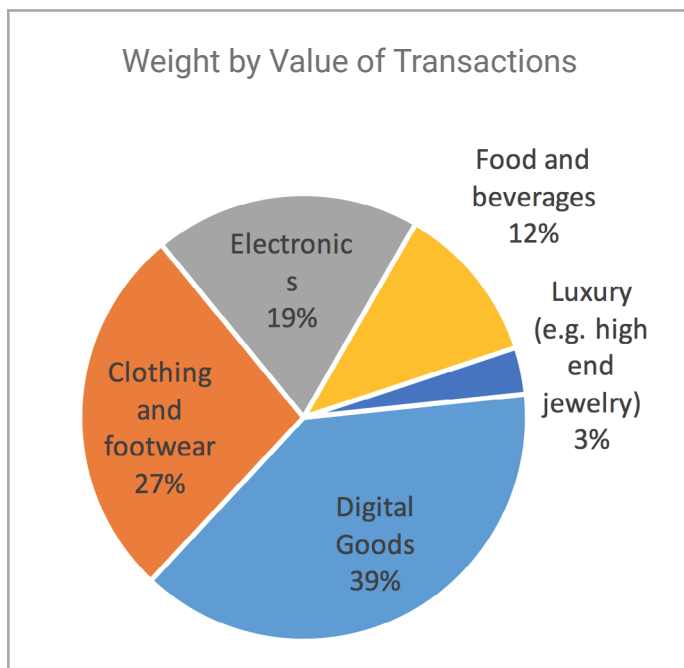
With regard to attacks on U.S. merchants from transactions that ship to Europe, the cost of fraud nearly doubled: it went from 9.5% in Q4 2015 to 18.9% in Q1 2016. With regard to attacks on U.S. merchants on transactions that ship to the ROW, attacks increased by 69%: the cost of fraud rose from 8.5% in Q4 2015 to 14.4% in Q1 2016. Attacks on domestic transactions remained below the average with a cost of fraud of just 7%.

Industry Segments

To get a deeper look into the nature of fraud attacks, we analyzed them by the following industries: digital goods, clothing, electronics, food and luxury.

In 2016 Q1 the average transaction value for digital goods was \$27, compared to \$126 for clothing; \$279 for electronics; \$88 for food; and \$712 for luxury goods, which includes high-end jewelry.

We also accounted for smaller transactions in each of these industries and found that nearly 77% of transactions in the digital goods industry; 12% in clothing industry, 4% in electronics, 7% in food and 0.3% in luxury fell in the category of smaller transactions with less dollar value.

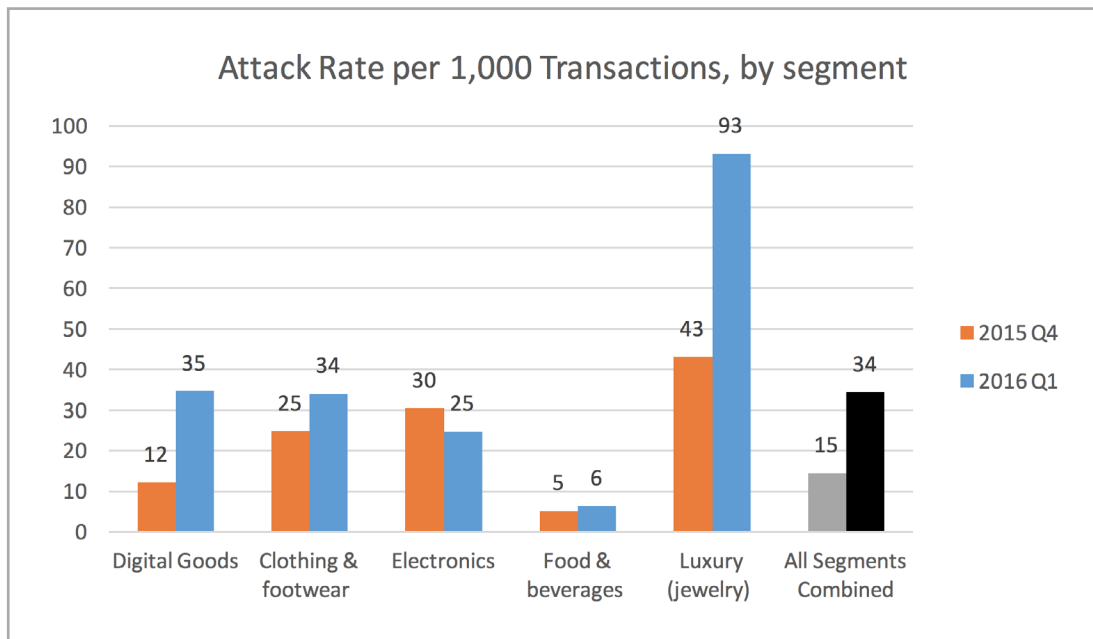


For the first quarter of 2016, the overall product weights by number and transactional value are shown below. Digital goods accounted for 77% of transactions, but only 39% of the dollar value of transactions. On the other hand, jewelry accounted for only 0.3% of the number of transactions, but represented 3% of the total dollar value.

The attack rate (attacks per 1,000 transactions) varied considerably across these segments – from a high of 93 in luxury to a low of 6 in food & beverage. In addition, attack rate trends have changed drastically over the past year.

Digital Goods, which had a relatively low attack rate in Q2 2015, now has the second highest attack rate. In luxury, the attack rate increased dramatically from 43 per 1,000 transactions to 93 per 1,000 transactions. Overall, the attack rate across segments is 34 per 1,000 compared to 15 per 1,000 transactions in Q2 2015.

The Global Fraud Attack Index Report



A comparison of the fraud attack rate for 2015 Q4 and 2016 Q1 broken out by segment. Below is an examination of fraud attack rates, since Q1 2015, 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	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016
Digital goods	7	12	25	29	35	0.6%	1.8%	6.3%	7.8%	10.8%
Clothing & footwear	15	25	20	20	34	3.1%	9.6%	4.1%	3.6%	7.2%
Electronics	20	30	20	17	25	2.9%	5.4%	1.8%	2.6%	3.9%
Food & beverages	5	5	3	3	6	0.3%	0.3%	0.2%	0.2%	0.4%
Luxury (jewelry)	31	43	65	60	93	4.9%	5.7%	9.0%	8.6%	9.5%
All segments combined	9	15	24	27	34	1.9%	4.8%	4.2%	4.8%	7.3%

Methods of Attack

Fraud attacks have surged to new levels. In part this is because the types of attacks fraudsters launched are changing. Last year, botnets (collections of computers that had been taken over by fraudsters, unbeknownst to the owner) accounted for 34% of attacks, followed by account takeovers at 17% and location manipulation at 10%. Friendly fraud accounted for 15%.

In the first quarter of 2016, botnets account for a staggering 79% of all fraud attacks. Meanwhile, account takeovers have dropped to from 17% to a mere 4%.

Fraud type	15.1	15.2	15.3	15.4	16.1
Account takeover	17%	8%	3%	3%	4%
Botnets	34%	47%	81%	82%	79%
Friendly fraud	14%	10%	2%	2%	3%
Location manipulation	11%	6%	2%	2%	4%
Other	17%	17%	7%	6%	7%
Simple fraud	3%	3%	1%	1%	1%
Sophisticated fraud	5%	8%	2%	3%	2%

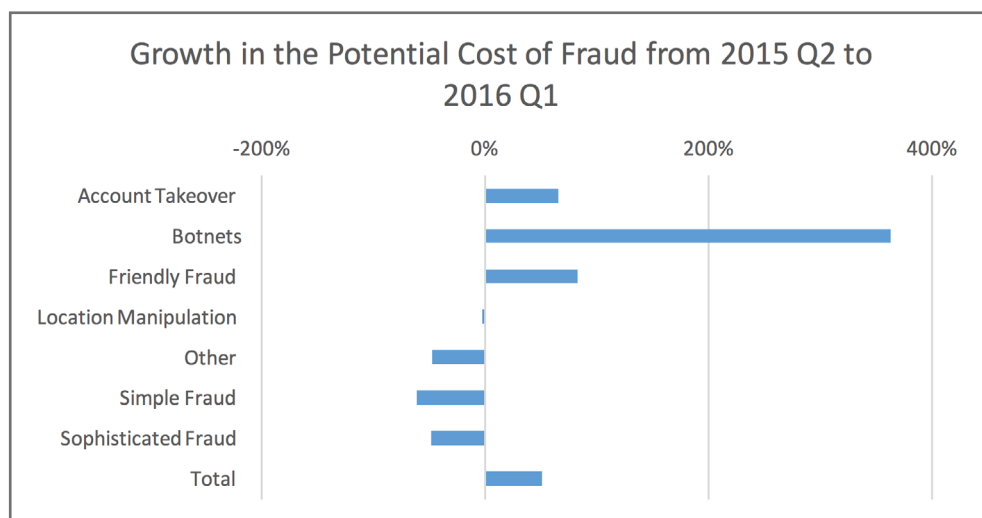
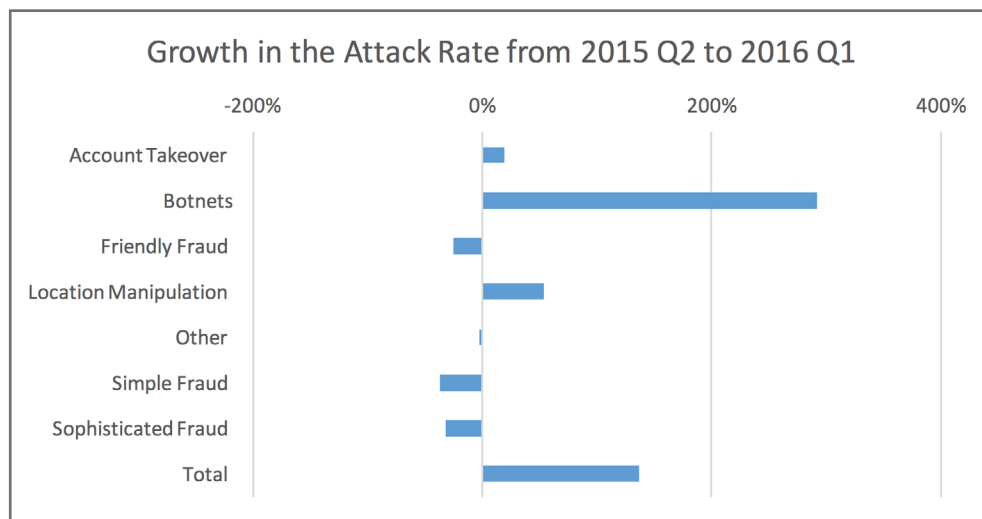
To summarize the changes over the past year, we calculated the percent increase in the attack rate for each method and the percent increase in the transaction dollars at risk, comparing Q2 of 2015 with Q1 2016. The number of attacks from botnets surged from 7 per 1,000 in Q2 2015 to 27 per 1,000 in Q1 2016.

Location manipulation, the second largest cause of fraud, also grew in popularity among fraudsters. During Q2 2015, it was used in 9 out of every 1,000 transactions, but in Q1 2016, it was used in 14 out of every 1,000 transactions.

The Global Fraud Attack Index Report

The fraud rate also decreased in a few categories. The highest decreases were for simple fraud (a 37% decrease) and sophisticated fraud (a 32% decrease).

Although the attack rate has decreased for friendly fraud, the potential cost of fraud has increased over the period. This can be attributed to the fact that overall the average attack amount more than doubled over the period, from 101 in Q2 2015 to 256 in Q1 2016, increasing costs all around.

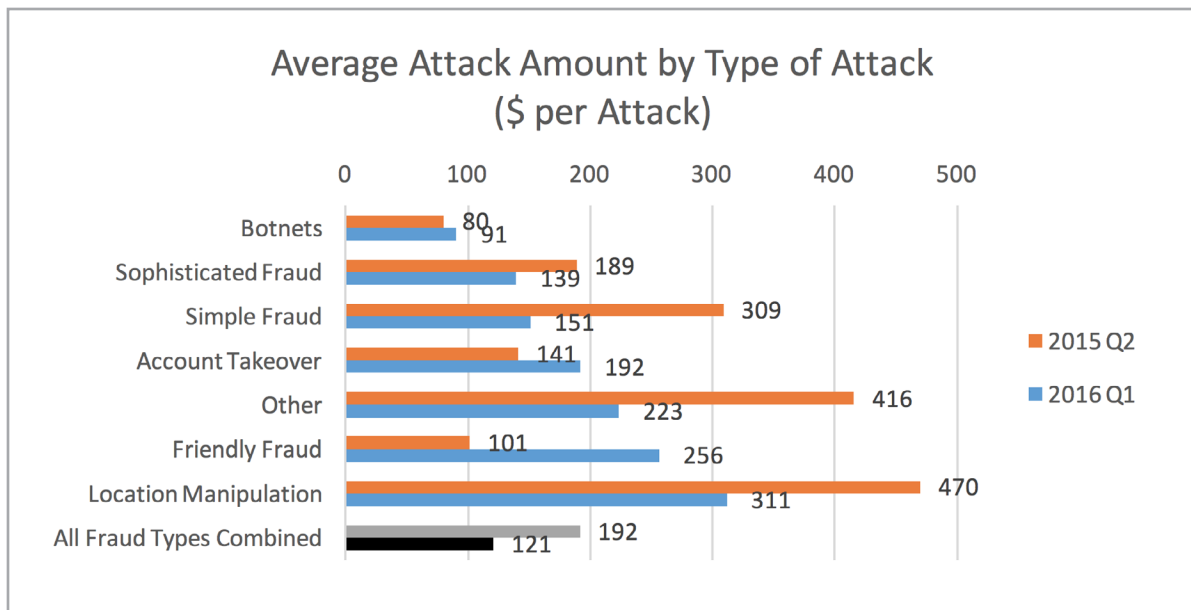


The average size of the transaction targeted varies considerably for the type of attack. As the chart above shows, botnets have the lowest average attack amount of all the types of fraud. Because the average attack amount is lower than other types of fraud, it offsets some of the potential transaction dollars at risk. One potential reason why botnets target lower dollar transactions is because fraudsters realize merchants scrutinize high value transactions more carefully.

The Global Fraud Attack Index Report

The overall dollar amount of an average transaction has decreased over the last year, from \$192 in Q2 2015 to \$121 in Q1 2016. We saw a corresponding significant decrease in the average value of fraud attacks for some of the fraud types. For instance, average value of simple fraud went down from \$309 to \$151, and location manipulation decreased from \$470 to \$311.

In fact, the average attack amount has only increased for botnets (\$80 to \$91) and friendly fraud (\$101 to \$256). One reason for the difference in the scale of the increase is, botnets are hoping to pull off large amounts of fraud undetected and targeting lower amounts en masse. Friendly fraudsters, on the other hand, are probably thinking on a much smaller scale, and hoping to get away with one-off frauds for a larger amount.



The Global Fraud Attack Index Report

When botnets represent 79% of fraud attacks, their average transaction value is lower than the rest of the fraud types. As a result, botnets accounted for 58% of transaction dollars subject to attack during Q1 2016.

	15.1	15.2	15.3	15.4	16.1
Account takeover	5%	6%	2%	4%	7%
Botnets	28%	19%	62%	66%	58%
Friendly fraud	15%	5%	2%	4%	6%
Location manipulation	20%	16%	6%	7%	10%
Other	26%	41%	18%	12%	14%
Simple fraud	4%	5%	2%	1%	1%
Sophisticated fraud	3%	7%	8%	5%	3%

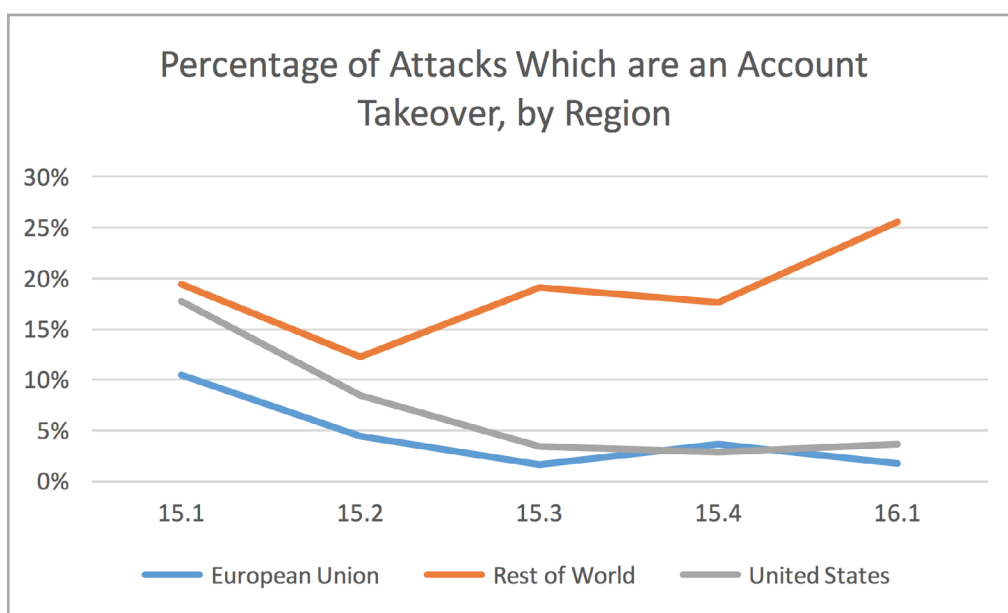
Deep Dive – Account Takeover

Customer account takeover is a major challenge for financial services and eCommerce organizations. Criminals use credentials stolen from victims via phishing and malware attacks to gain unauthorized access to customers' accounts.

Once inside the compromised account, criminals can transfer money, execute fraudulent purchases, or exploit relationships with other customers.

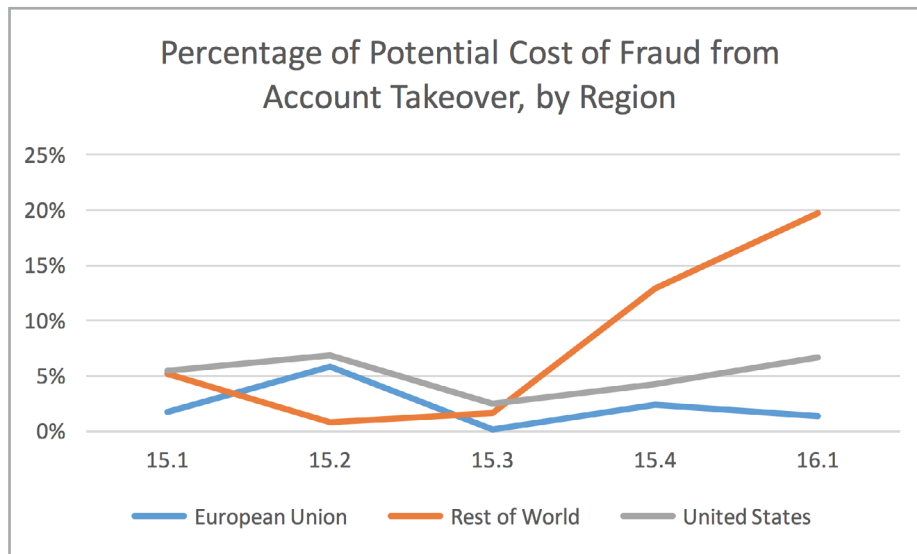
While the percentage of attacks stemming from account takeovers has been diminishing both in Europe and in the United States, they have shown a surprising growth in the ROW over the last year and in the first quarter of 2016.

As of Q1 2016, account takeover as a fraud type represented 2% of fraud activity on transactions shipping to Europe, 4% for domestic transactions, and 26% for transactions from the ROW.

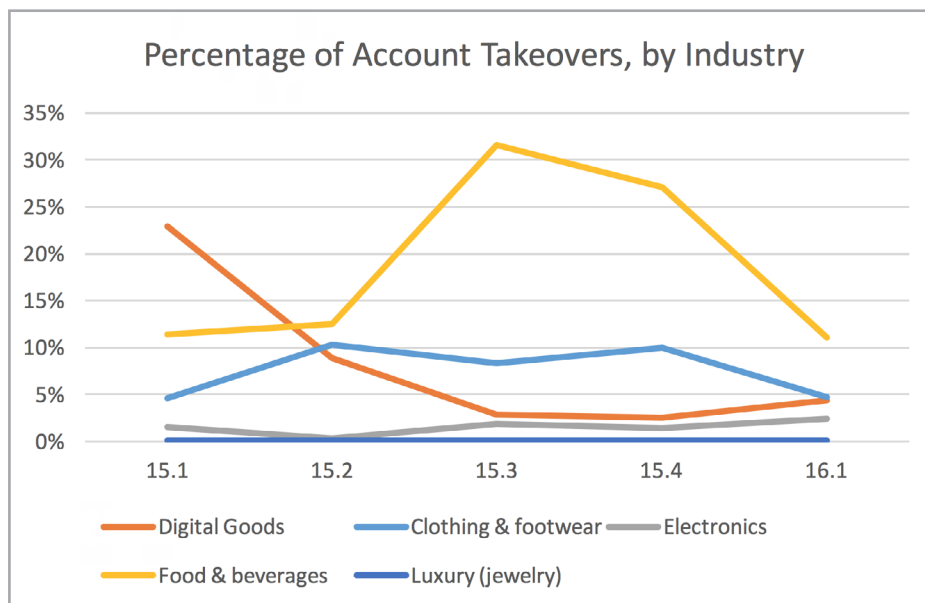


Until the third quarter of 2015, the rate of fraud attacks in the rest of the world was similar to the levels seen in Europe and the United States. Since then, account takeover has grown to represent a higher percentage of the attacks and thus has a bigger price tag for ROW transactions than for European transactions and domestically.

The Global Fraud Attack Index Report



In particular, account takeover has impacted the food and beverages industry. The number of account takeovers in the food and beverage industry has been very volatile. In Q1 2015 it accounted for 11% of total fraud in the segment, reached 32% in Q3 2015 and lowered again in 2016 Q1 to 11%.

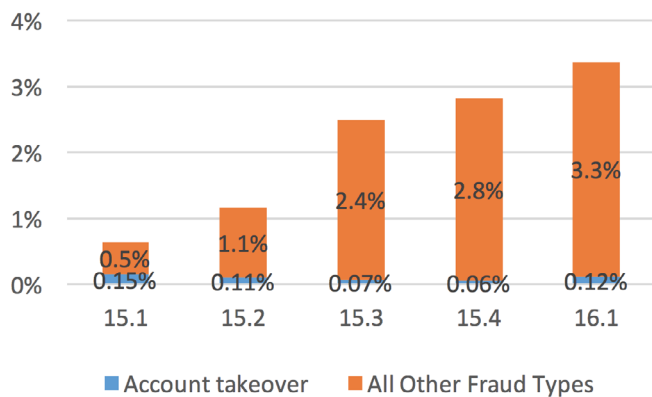


The Global Fraud Attack Index Report

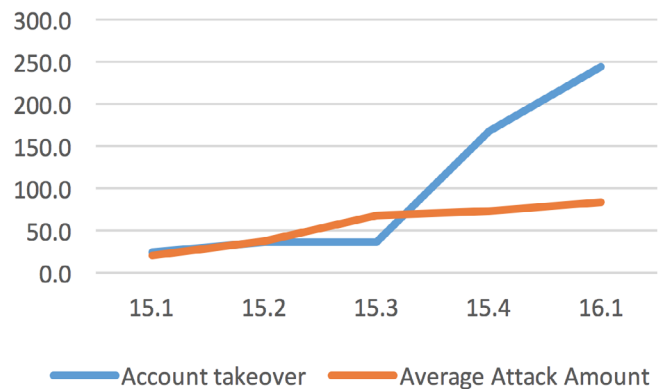
Digital goods in the United States

Over the course of 2015, account takeovers saw a decrease, with a slight uptick during the first quarter of 2016. Account takeovers for digital goods dropped from 0.15% in Q1 2015 to 0.06% in Q4. However, in Q1 2016 takeovers doubled from Q4 2015. In addition, the cost associated with account takeovers has almost tripled. This is in part because of a sharp increase in the average amount of account takeovers for digital goods. By comparison, the potential cost for other types of fraud increased 30% over the last quarter.

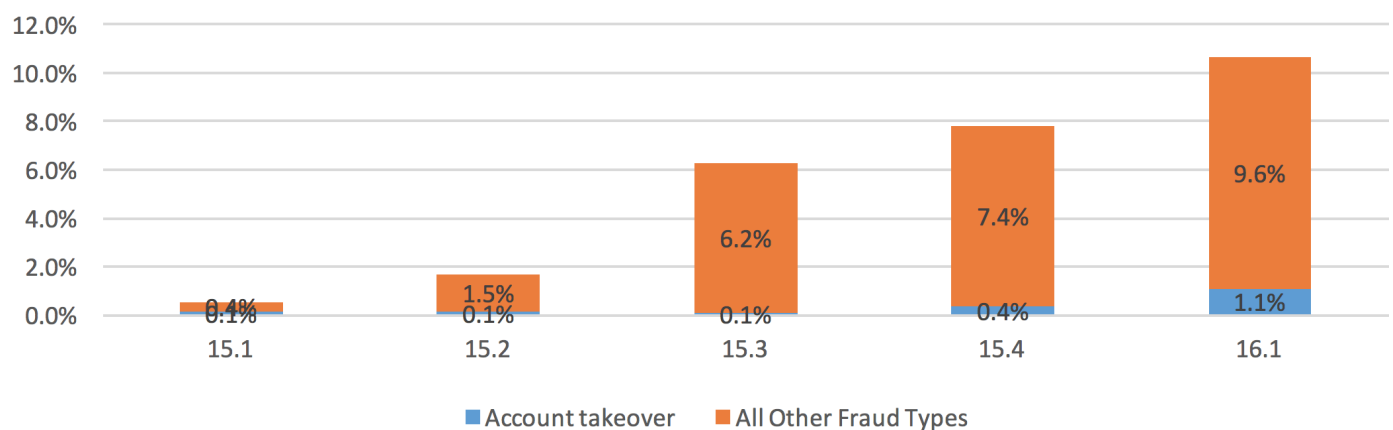
Attack Rate for Digital Goods in the United States



Average Attack Amount for Digital Goods in the United States



Potential Cost of Fraud for Digital Goods in the United States

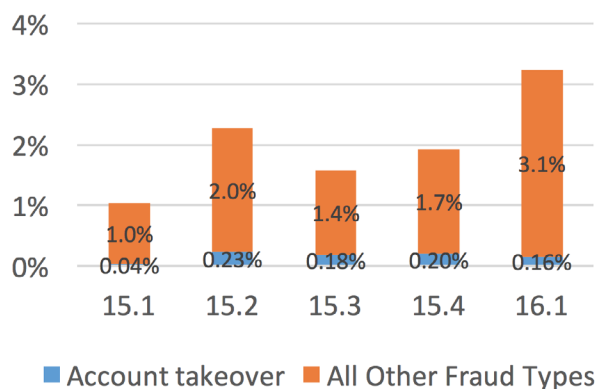


The Global Fraud Attack Index Report

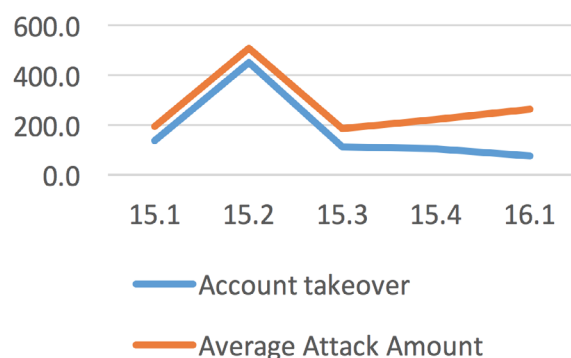
Clothing and footwear in the United States

In the clothing and footwear segment, the overall fraud attack rate increased significantly, but this is due to an increase in other types of fraud rather than an increase in account takeovers. In fact, account takeover attacks in the clothing and footwear segment decreased from 0.23% in Q2 2015 to 0.16% in Q1 2016. The potential cost of fraud in this segment peaked in Q2 2015, and then saw a sharp decrease afterwards. Don't celebrate too soon though: even if overall costs have lowered in the segment, costs are climbing back up. Costs experienced 109% growth during the last two quarters.

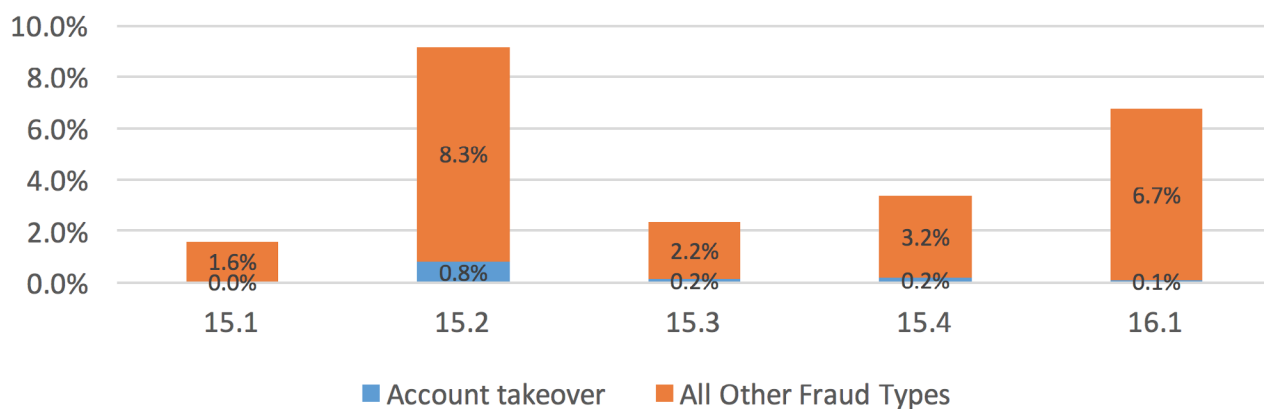
Attack Rate for Clothing & Footwear in the United States



Average Attack Amount for Clothing & Footwear in the United States



Potential Cost of Fraud for Clothing & Footwear in the United States



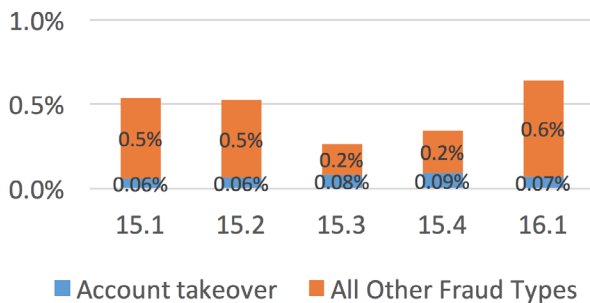
The Global Fraud Attack Index Report

Food and Beverages in the United States

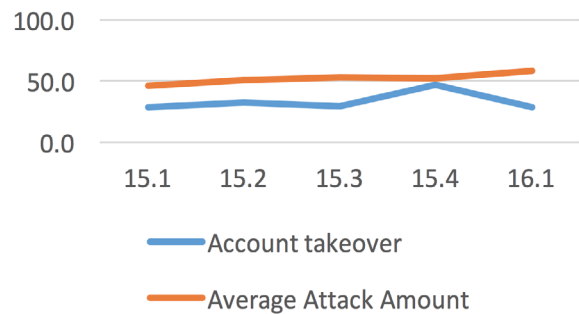
The sector most attacked by account takeovers is food and beverages. The rate of account takeovers remained pretty flat in 2015, and oscillated between 0.06% and 0.09% in the first quarter of 2016. By comparison, the attack rate for other types of fraud has tripled since last quarter from 0.2% to 0.6%.

The average attack amount has also remained flat for other types of fraud. It has decreased slightly over the last quarter for account takeovers. The potential cost of fraud is down to half as of last quarter, but has doubled for other types of fraud.

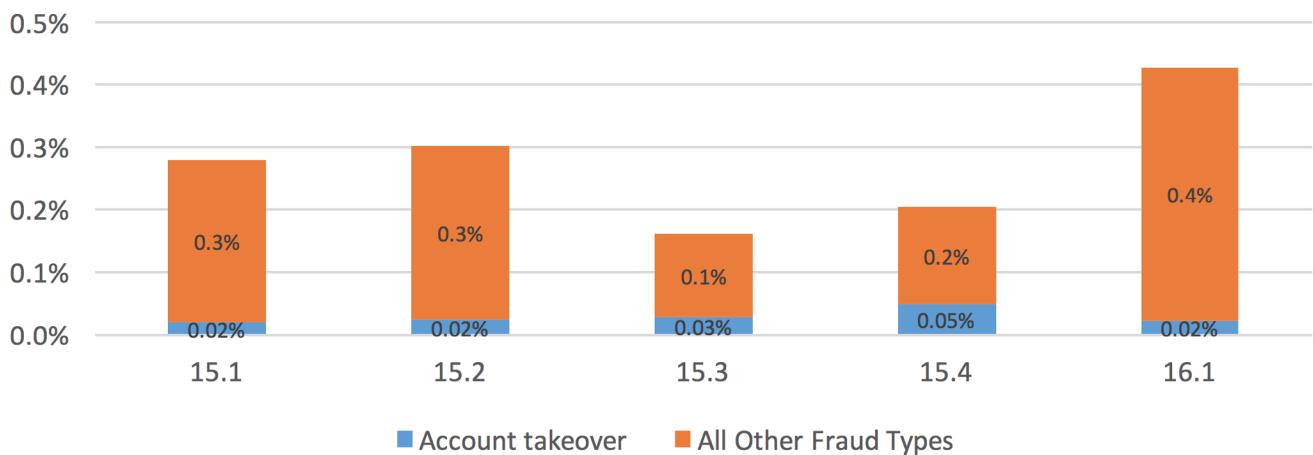
Attack Rate for Food & Beverages in the United States



Average Attack Amount for Food & Beverages in the United States



Potential Cost of Fraud for Food & Beverages in the United States



The Ever-Rising Cost Of Fraud

Fraud attempts can be time-consuming, forcing businesses to spend hours dealing with the effects of a security breach instead of serving customers and building new revenue streams. They can also be embarrassing, particularly if the incident damages customer confidence.

More than anything, though, fraud can be very costly.

According to the [Association of Certified Fraud Examiners](#), the money lost by businesses to fraudsters amounts to over \$3.5 trillion each year. And as the Global Fraud Attack Index™, a PYMNTS/Forter collaboration, illustrates, the cost of fraud is only accelerating; it's getting more expensive, it's happening more often and the number of account takeovers is rising dramatically.

As a Vice President and Vertical Leader for Financial Services at Convergys, Ron Andrews is well-versed in the latest trends in fraud and security, and knows just how damaging fraud attempts can be. PYMNTS recently caught up with Andrews to discuss the rising costs of fraud for businesses.

Andrews said that fraudsters are becoming more sophisticated and there can be a steep price to pay, both in the physical money lost and the great cost of losing customer trust and loyalty.

Fraudsters are getting smarter and attacking more often

The Q3 Global Fraud Index data indicate that instances of fraud are on the rise, growing by 126% in the last year. Fraud attacks more than doubled between Q2 2015 and Q1 2016, and attacks also rose 27 percent from Q4 2015 to Q1 2016.

Andrews noted that an increase in fraud attacks has become more visible during this period. To combat, companies are working to deal with new challenges posed by the rising amount of security breaches.

"In terms of identity fraud, we're certainly hearing about an increase in that space, and some of that is EMV related," Andrews said, noting that last September's transition to EMV security caused some complications for merchants and security teams looking to keep fraudsters out. "We're adding to the capacity of the network in order to handle the fraud increases that our clients receive."

Account takeovers are fast emerging to become one of the most common forms of fraud, according to the latest Index findings. As of Q1 2016, they accounted for 2 percent of fraud activity in Europe, 4 percent in the United States and more than 25 percent of attempts around the world.

"Account takeover is out there, and it's real," Andrews said. "There's a need for all companies, not only in this industry, but everywhere, to protect themselves and protect the transaction and protect the customer information going back and forth."

The Ever-Rising Cost Of Fraud

Fraud's growing price tag

As if an increase in the number of fraud attempts wasn't worrisome enough, the cost of dealing with those fraud attempts is also on the rise. According to the Index, the reach of fraud attacks has grown substantially from the beginning of 2015, when less than \$2 out of every \$100 was subject to a fraud attack. In Q1 2016, the reach of fraud attacks climbed to affect more than \$7 out of every \$100.

Fraud's increasing cost is, in large part, tied to the progression of fraud prevention, Andrews explained. As hackers and other bad actors become more sophisticated, merchants and security firms have to invest more money to stop them.

"This is an evolution from the early days of fraud detection systems running and catching frauds and the earliest days of authentication," he said.

Andrews also pointed out that bleeding profits at the point of sale are a big problem for merchants. Businesses are continually losing their sales revenue because protection and control measures still need to be put in place to help safeguard customers both in-store and online, he said.

Whether businesses are forced to pay more to deal with the effects of a fraud attack, lose money due to a security breach, or are unable to authenticate a customer, resulting in a lost opportunity at the point of sale, Andrews said, the rising cost of fraud gravely affects the health of a business.

"There's a real cost in terms of the call to run the authentication," Andrews emphasized. "The impacts are real, and they hit the bottom line."


The customer cost of fraud

As fraudsters have evolved to become more intelligent and sophisticated, companies have had to put sophisticated fraud prevention tactics in place to deal with an increasingly intelligent and innovative group of bad actors. That often causes frustration and even embarrassment for customers who have to deal with more stringent security, and Andrews said those feelings can also hit a company's bottom line.

"Making somebody prove they are who they say they are creates an awkwardness at the beginning of a customer service transaction," Andrews said. "It means I don't trust you until you prove to me this information and answer these questions. If you don't, I'm not going to service you."

For many consumers, the inconvenience arising from additional fraud screening steps could even change their brand loyalties. And even though such frustration might not necessarily lead customers to cancel their account right away, they can seriously affect their trust in a company, and their shopping habits, according to Andrews.

"I think it's easy to reach into the wallet, grab that second card, and not go back to the one you've been using all these years," he said.



The Ever-Rising Cost Of Fraud

Is a better way on the way?

For merchants looking to balance protection from these more expensive and frequent fraud attacks with a straightforward and pleasant customer experience, there are some good examples to follow, Andrews pointed out.

He said that companies need to work with customers so they feel confident fraudsters are being kept at bay.

“Some applications are quite good,” he said, citing methods like text messages or other alerts that ask customers to let a bank know if a particular purchase was authorized. “I think when those work well, it is likely the customer is very satisfied.”

There is also a chance for companies to differentiate themselves from competitors in the space, and establish trust and appreciation among consumers, by allowing customers a “quick path in.”

Mobile device recognition technology is one such tool that allows extension of a safe, reliable and convenient customer authentication experience. In the future, it holds the potential of allowing merchants to attach customer authentication and history information to a mobile device.

“If they could tie device reputation and actual commercial transaction data from merchants, it would be great that the network would know that this is an authenticated customer and that this is a usual transaction for them,” Andrews said. “Clearly, the best authentication is invisible to the customer. It happens behind the scenes. That’s why the industry is so excited about voice and mobile device reputation.”

So, as it turns out, companies determined to keep their profits intact and customers happy may find the best bet is relying on mobile technology.

What is the Index?

The Global Fraud Attack Index™ measures the growth (or decline) of attempted fraud⁵ 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

The Index is created by evaluating the attack rate relative to the average fraud rate during 2015. Specifically, we calculate the fraud rate for each of the four quarters during 2015. We then calculate the average of the four quarters and use that as the Index base.

Specifically, the fraud rate per 1,000 transactions for the first four quarters of 2015 were 9, 15, 24 and 27, respectively. The average of that is 18.6 and this becomes the Index baseline. Since the attack rate for the first quarter of 2016 increased to 34, it is 85% greater than the 18.6 Index baseline. We consider the Index baseline to be 100 and therefore the Index value of the first quarter of 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, by the primary merchant segment, and by the type of fraud being perpetrated.

Attack Rate

Forster 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 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 the Rest of the World, 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 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.

⁵ 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 was 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 for the Average Attack Amount were provided by Forter and described above.

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.

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:

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

The U.S. Census Bureau provides data at a three-digit 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 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)

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 eCommerce Report; Critical Facts and Insights for International Expansion, Update 2014. They PayPers, <http://www.thepaypers.com/news-and-reports/us/5>

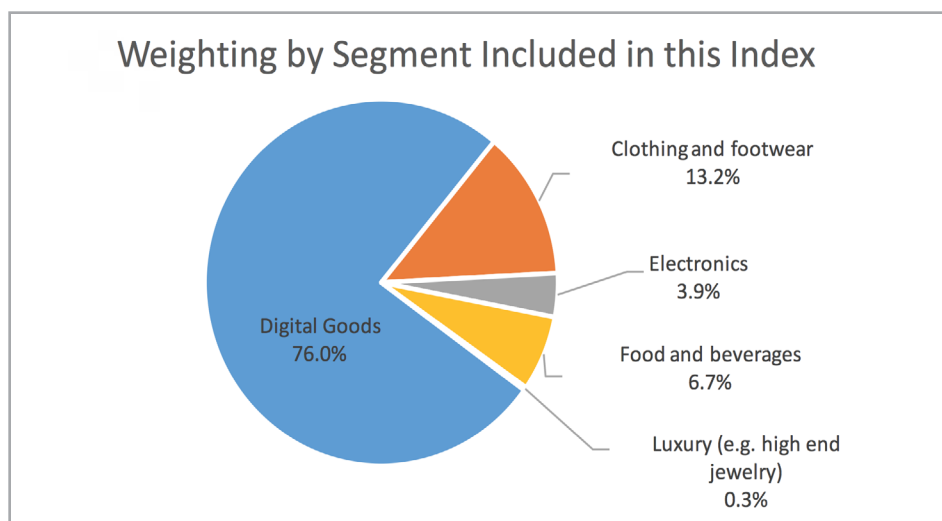
⁸ Same report.

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 722 Food service and drinking places less 7224 drinking places and 722511 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 - digital goods such as gift cards, eBooks, music, gaming. Also includes business-related virtual services such as hosting and software solutions.

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



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.

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™ 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.