GLOBAL FRAUD ATTACK INDEX™

A PYMNTS/Forter Collaboration

FORTER

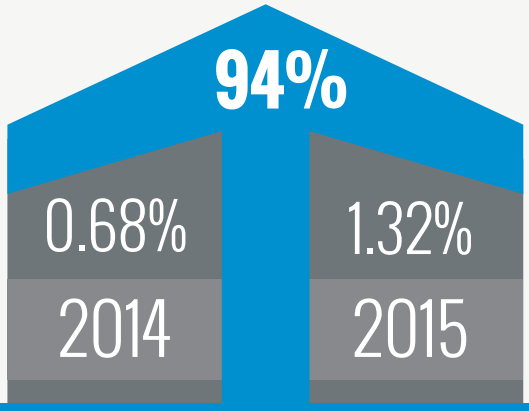
PYMNTS.com

FIRST QUARTER 2016

ATTACK INDEX: 163%

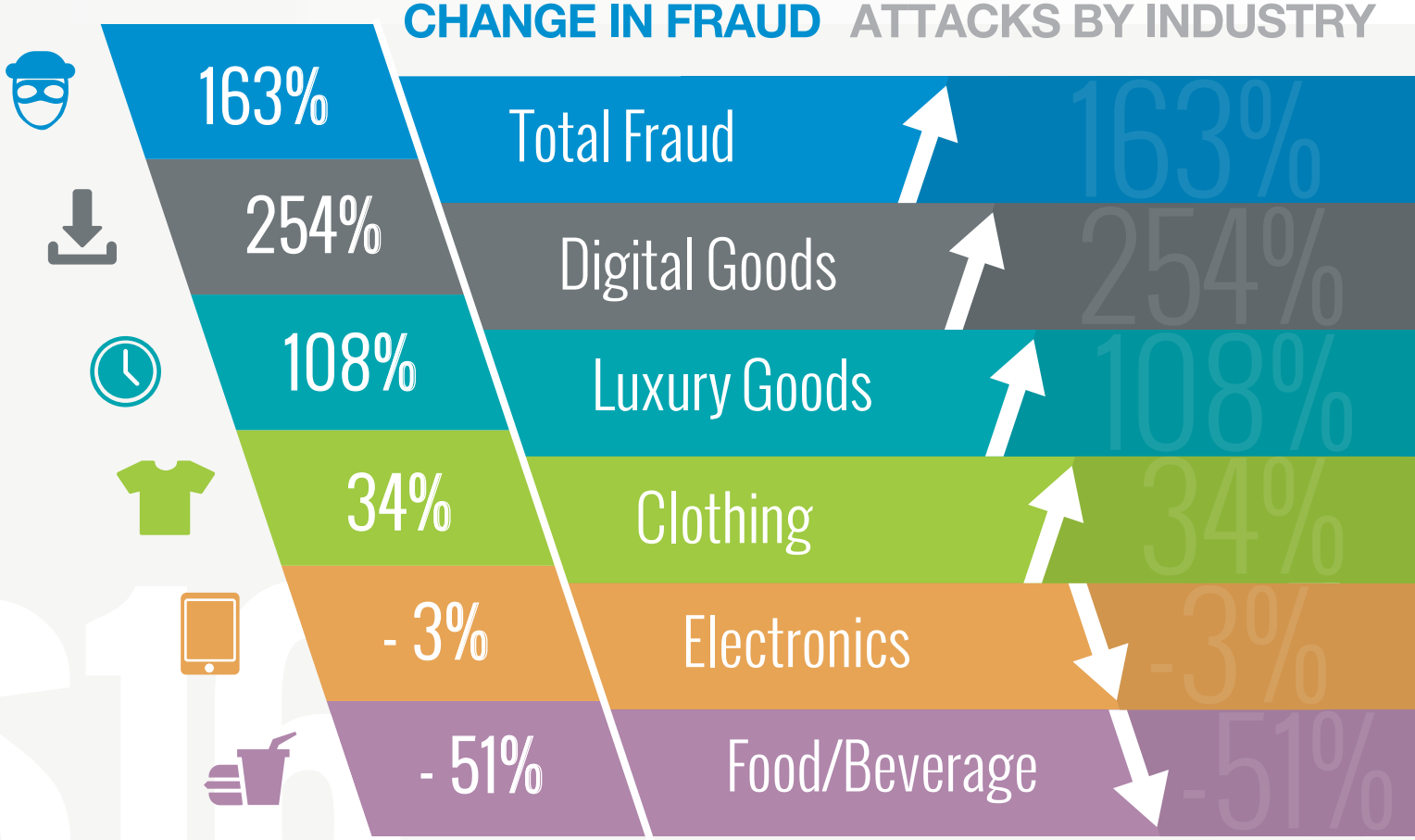
$16 Billion

TOTAL COST OF CREDIT CARD FRAUD WORLDWIDE[1]



FRAUD AS A PERCENTAGE OF RETAIL REVENUE[2]

CHANGE IN FRAUD ATTACKS BY INDUSTRY



[1] http://www.nilsonreport.com/publication_chart_and_graphs_archive.php?1=1&year=2015

[2] https://www.lexisnexis.com/risk/downloads/assets/true-cost-of-fraud-2015-study.pdf

THE GLOBAL FRAUD INDEX REPORT

Fraud. The sheer word alone sends shivers up and down the spines of executives, risk managers, 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 retailers reached $32 billion in 2014. $32B.

It's estimated that retailers lost 1.32% of revenue in 2015[1], more than double the rate of 2014. And up to 25% of declined sales transactions for eCommerce merchants were actually good sales to start. Not only does actual fraud "sting," but making inadvertently wrong decisions to avoid fraud costs merchants plenty as well.

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 another and exploit it.

If that sounds a bit depressing, let's envision a different world. One where merchants employ sophisticated tools themselves – not for bad, but for good. Innovations like machine learning offer the potential to react much faster, and be proactive as well as reactive.

Fraud prevention, instead of rejecting good orders and frustrating legitimate customers with delays and demands for further information, can become real-time and far more accurate – contributing to more sales and better customer experience.

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. With the latest technology and access to the latest information about fraud and fraudster trends, retailers can be far better prepared to cope with the challenges of fraud prevention.

Enter the Global Fraud Attack Index™, a PYMNTS/Forter Collaboration. 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. Every quarter we will monitor how fraud attempts, reflected as a percent of U.S. sales transactions[2], on U.S. merchant websites are trending. Up? Down? Stable? Time to panic? Hopefully not.

We have developed an actual Index metric which measures how the rate of fraud attempts on U.S. online merchants change over time. The base of this Index is 100, and is defined as the average attack rate for the first 3 quarters of 2015. For the 3rd quarter of 2015, the index is 148. This means that for the 3rd quarter of 2015, the rate of fraud attempts is nearly 50% higher than the current 2015 average[3].

We will also explore different aspects of fraud. How are different merchant segments affected by fraud trends? Does it matter where fraudsters originate? Do U.S. fraudsters tend to use Location Manipulation more than those emanating from Europe? Are the average attack amounts increasing or decreasing at a faster rate than the transaction volume? What can be done to help stop or slow down these trends?

We hope you find this information interesting and enlightening and we welcome your feedback at globalfraud@pymnts.com. Identifying and understanding the root cause of fraud is half of the battle!

[1] LexisNexis® True Cost of Fraud℠ study
[2] The rate of fraud attempts is measured as the percentage of sales transactions that are fraudulent in nature. This combines both successful and unsuccessful attempts.
[3] We plan to update the baseline for the Index when a full year of data becomes available.

ARE WE HEADING FOR A MELTDOWN?

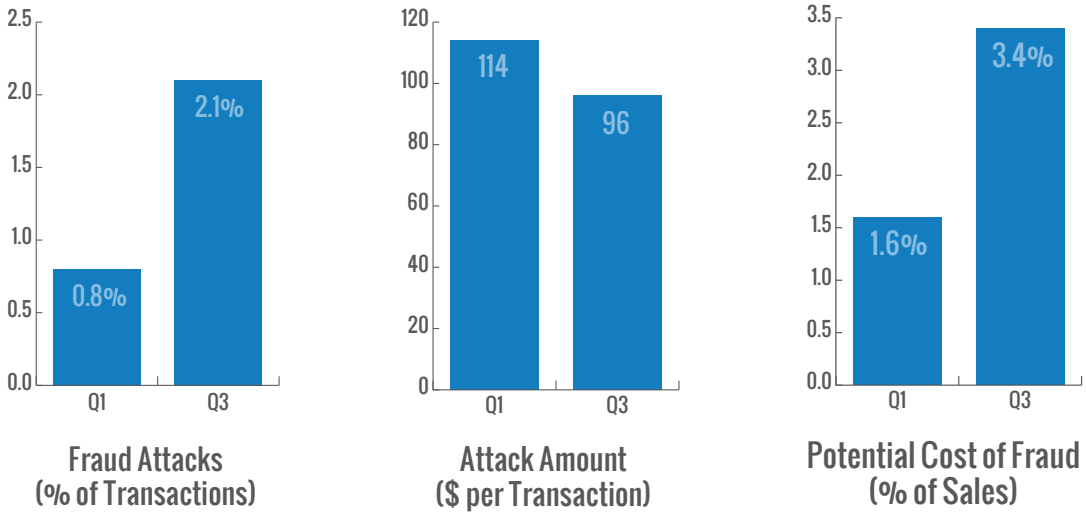
Not exactly — but we are starting to see a pattern of increasing fraudulent activity.

In the U.S. overall, clearly there are more frequent attacks on eCommerce sites. The number of fraudulent attempts, as reflected as a percent of sales transactions, has grown two and half times in a mere three-quarter period from 0.8% to 2.1% of all transactions. That should be concerning to almost any merchant selling on the Web.

On the good news front, the average attempted attack amount has actually decreased from $114 to $96 per transaction.

The net effect is that, if undetected, prevented or otherwise addressed, these attempts would translate into a huge jump in the bottom-line cost of fraud to merchants. Reflected as a percent of total sales, the cost would have doubled from first quarter 2015 to third quarter 2015 – reaching 3.4%.

U.S. ECOMMERCE FRAUD[4] (Q1 AND Q3 2015)



[4] For business segments studied. See Methodology section for additional details.

DOES FRAUD AFFECT MERCHANT SEGMENTS DIFFERENTLY?

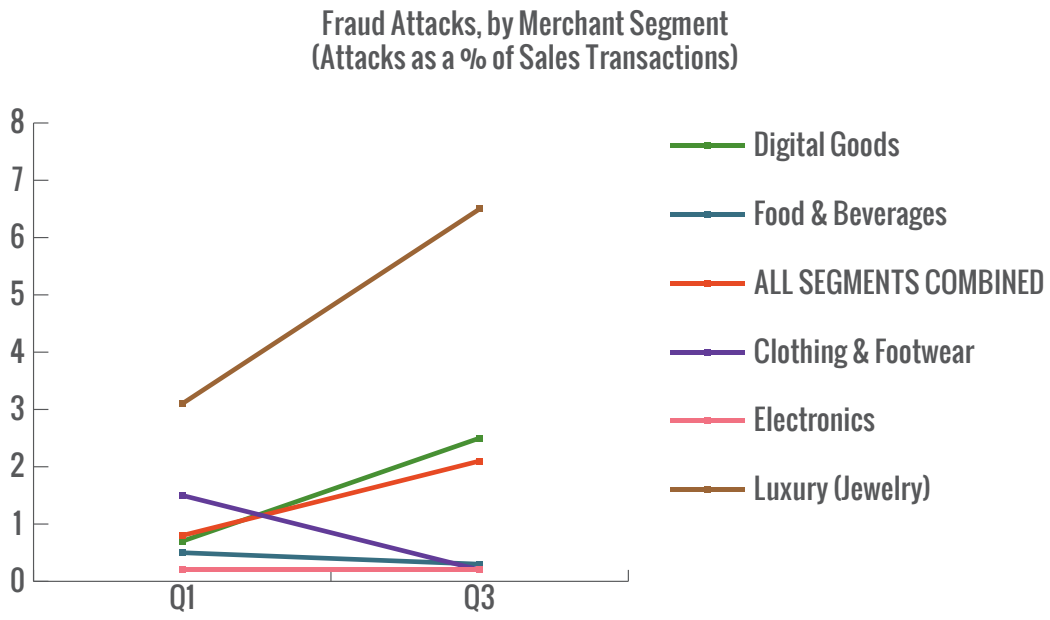
Does the rate of fraud differ by merchant segment? Is one particular category experiencing a higher frequency or incidence of fraud than another? Should a particular merchant segment be concerned about trends affecting their business?

We evaluated specific categories to understand what might be happening within specific categories. The implications are enlightening to both merchants and consumers.

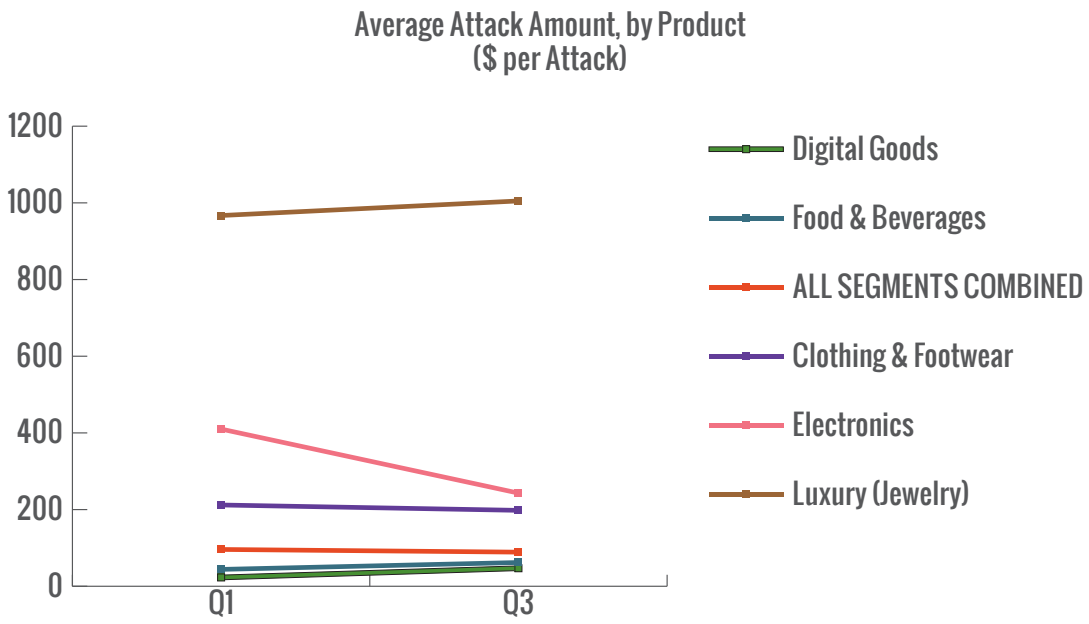
First, guess what? Fraudsters are no dummies. Shocker.

Fraudsters are continuing to hammer away in the Digital Goods and Luxury segments. While the average transaction amount appears to be stable, for the moment, the average rate of attempted fraud attacks has climbed dramatically over the three-quarter period in 2015. Fraud attempts on Digital Goods has increased by 2.5 times from the 1st quarter 2015 to 3rd quarter 2015, from 0.7% to 2.5% of all transactions. Similarly, fraud attempts on the Luxury segment (such as jewelry or high-end branded items) has more than doubled from 3.1% to 6.5% of all transactions.

The Luxury segment is also one of the few categories experiencing a rise in the average attack amount. For this category only, the average amount has risen 4%. Merchants in this category should be using real-time systems and concepts such as machine learning[5], avoiding, or at least minimizing as much as possible, the use of manual reviews.



[5] Forrester, Stop Billions in Fraud Losses with Machine Learning, April 2015



WHAT IS HAPPENING BY TYPE OF FRAUD?

We did further analysis to understand if certain types of fraud attacks are on the increase, are contained, or are potentially eliminated, due to superior tools and fraud detection techniques on the market today.

The fraud types we tracked and analyzed were[6]:

- Account Takeover
- Suspected Botnets
- Friendly Fraud
- Location Manipulation
- Simple Fraud
- Sophisticated Fraud

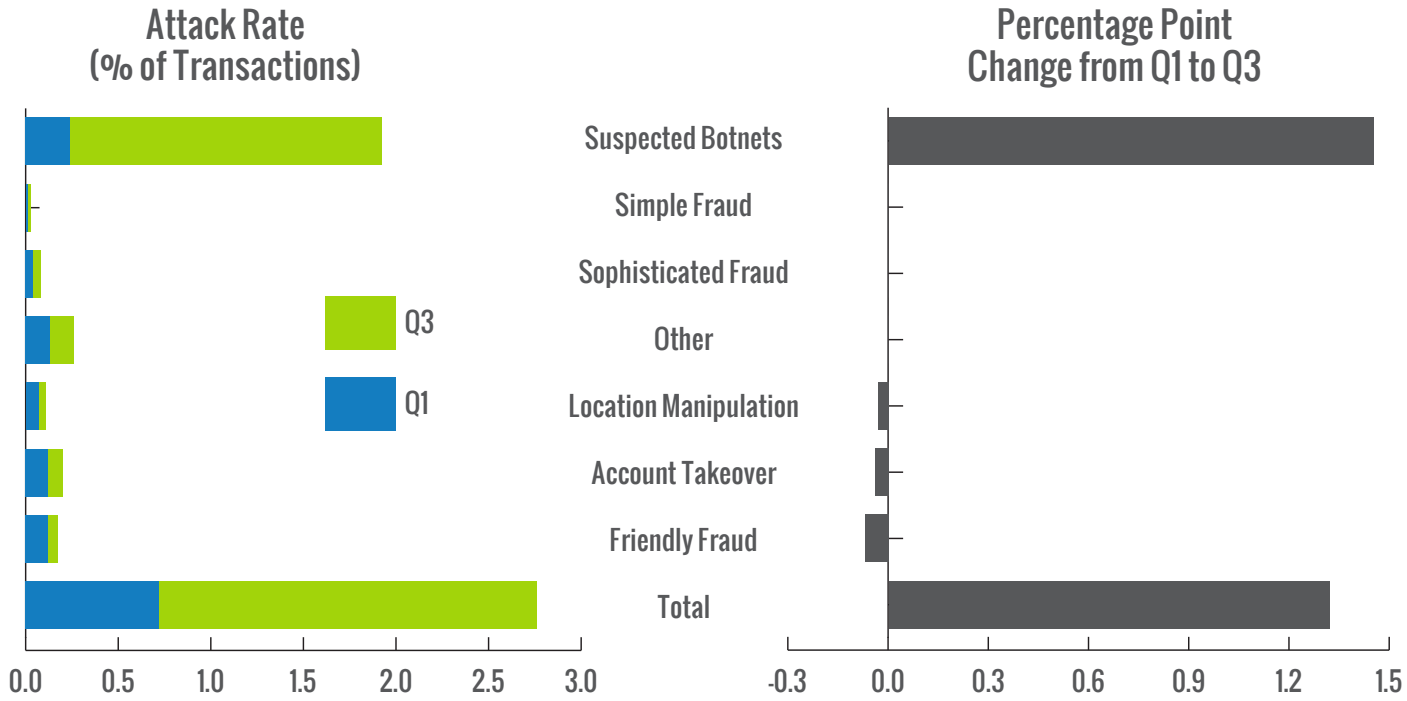
The increase in fraud attacks that originated in the United States were driven by the fraud type "Suspected Botnets."

This conjures up the particularly menacing picture in the mind of what fraud looks like – sneaky machines lurking in dark rooms somewhere, running wild with complex algorithms that calculate ways to encroach, replicate and penetrate vulnerable merchant systems faster than anyone can detect, let alone stop, their malicious attacks.

Sounds like something straight out of "i, ROBOT." Perhaps a bit stretched, but it is what this fraud type represents at its core.

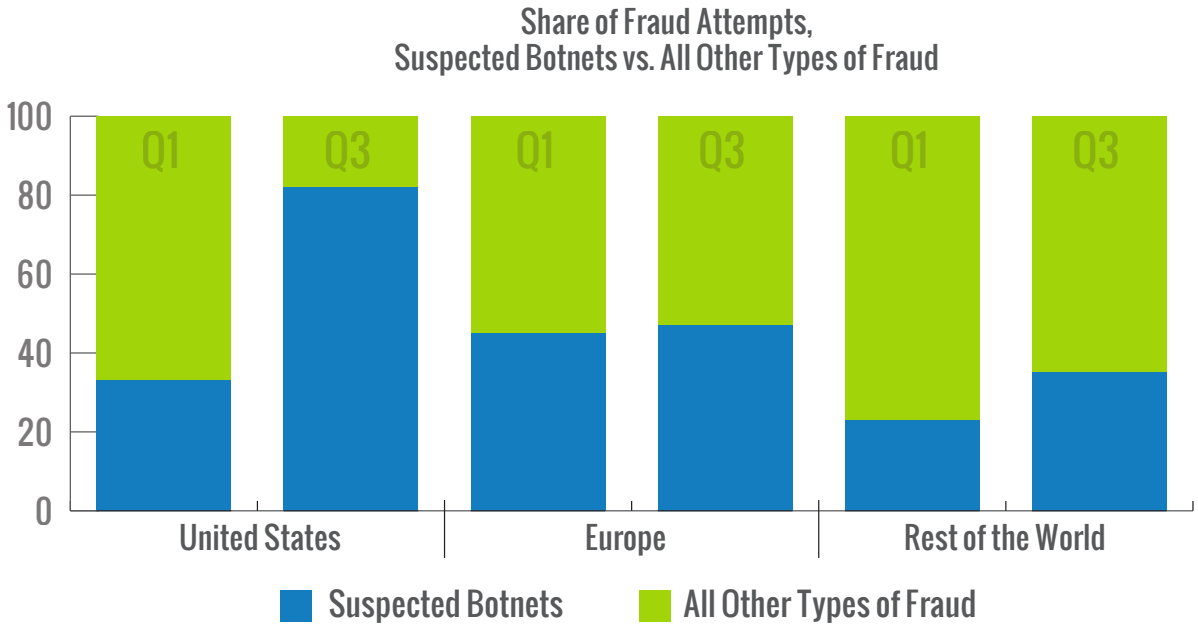
The scary part is that it's growing – and really fast. The rate of attacks has increased sevenfold in a nine-month period.

[6] See Methodology Section for fraud type definitions



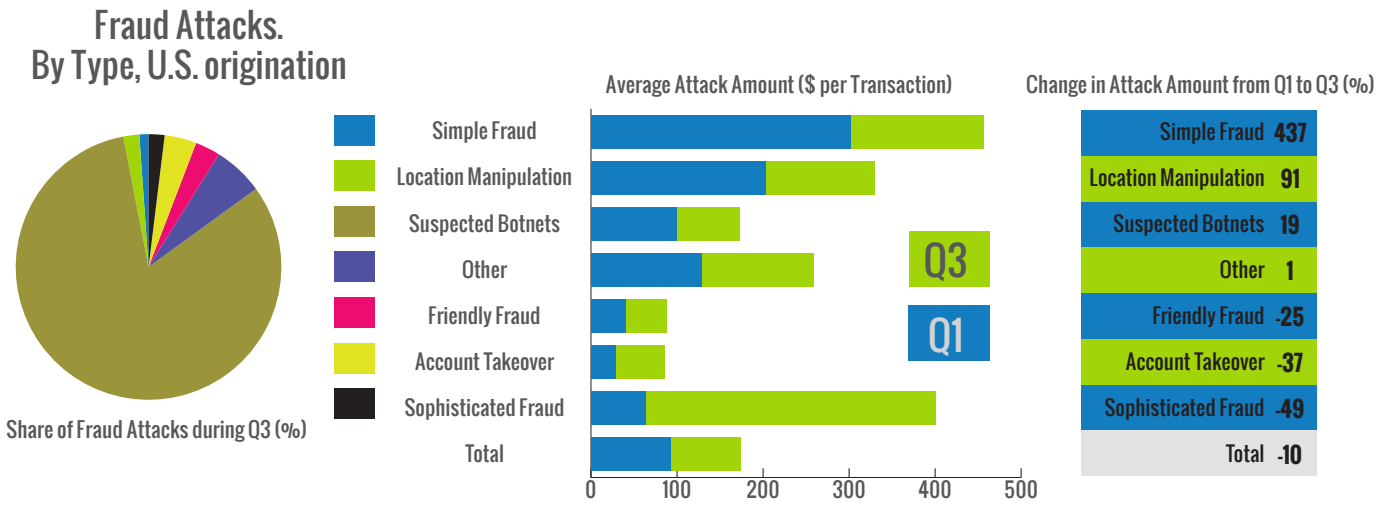
This type of attack represented 33% of all fraud attempts in the 1st quarter of 2015 and by the 3rd quarter, suspected Botnets had risen to an astonishing 82% of all fraud attempts.

Further, it's the largest fraud type for any fraud origination coming from other parts of the world as well.



Some good news please? The average attack was decreasing rapidly for botnets. Since botnets are such a huge portion of overall fraud, this reduces the average attack amount for fraud overall.

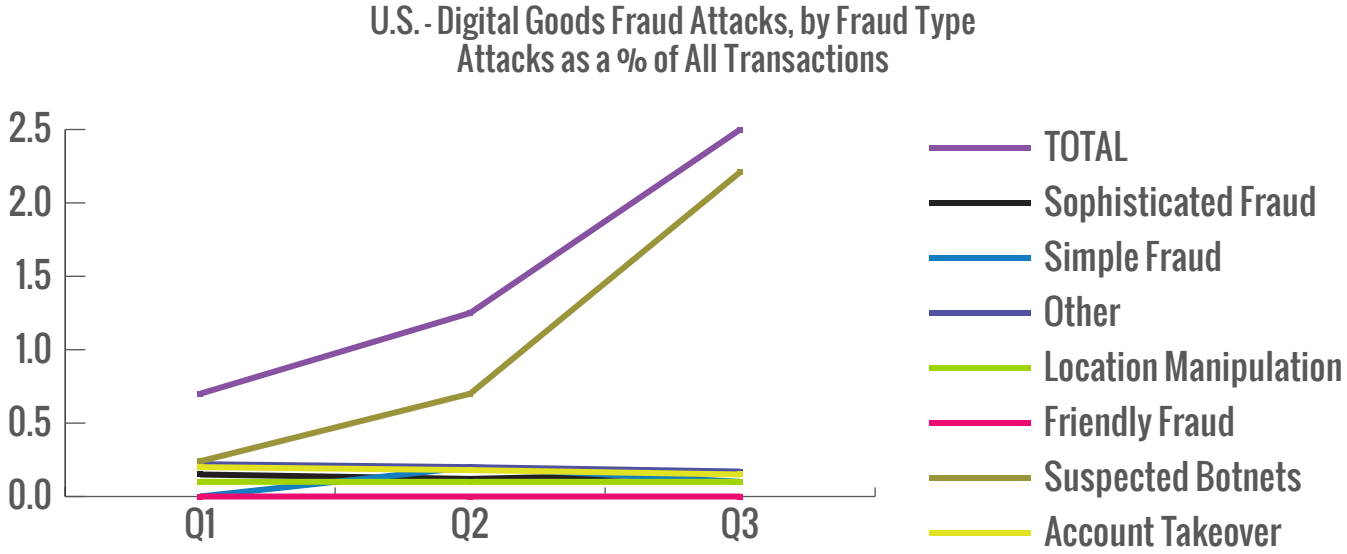
Yippee?

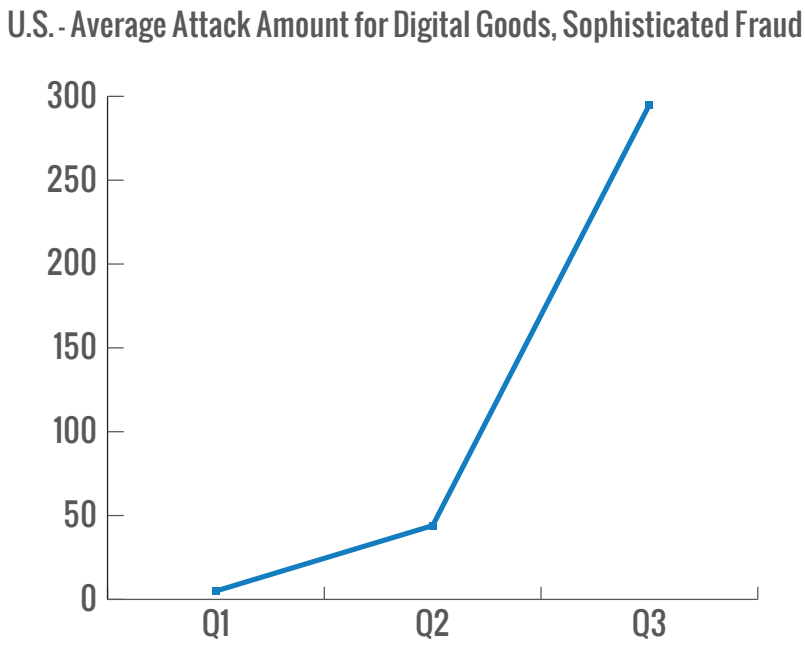


WHERE ARE OTHER SPECIFIC AREAS TO WATCH?

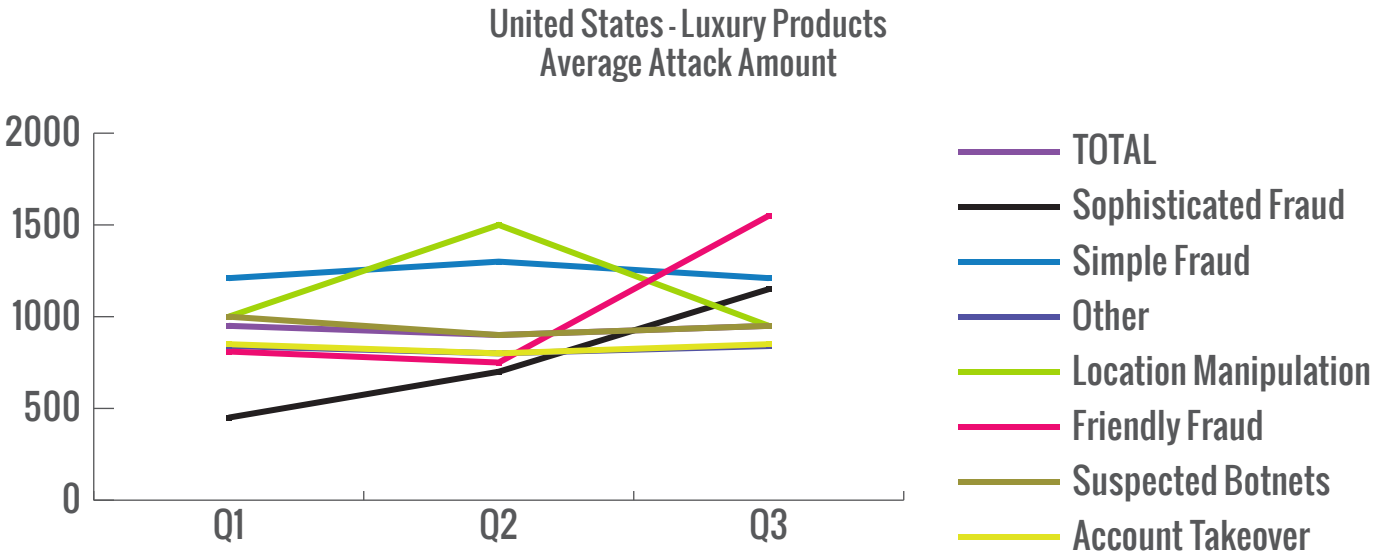
By far the biggest driver of overall fraud is Botnet attacks on Digital Goods. Botnet attacks within the Digital Goods segment accounts for 75% of all potential fraud losses overall, by far the largest of all fraud combinations. The total fraud attempt rate for Digital Goods is increasing fairly dramatically, and that is exclusively driven by Suspected Botnets.

One other item to note in this category: Sophisticated Fraud. When it comes to average attack amount for Digital Goods, Sophisticated Fraud has grown much more significantly than other types – nearly six fold in one quarter alone. While it's early to label it as a permanent trend, this is also cause for concern and definitely something to keep watching.



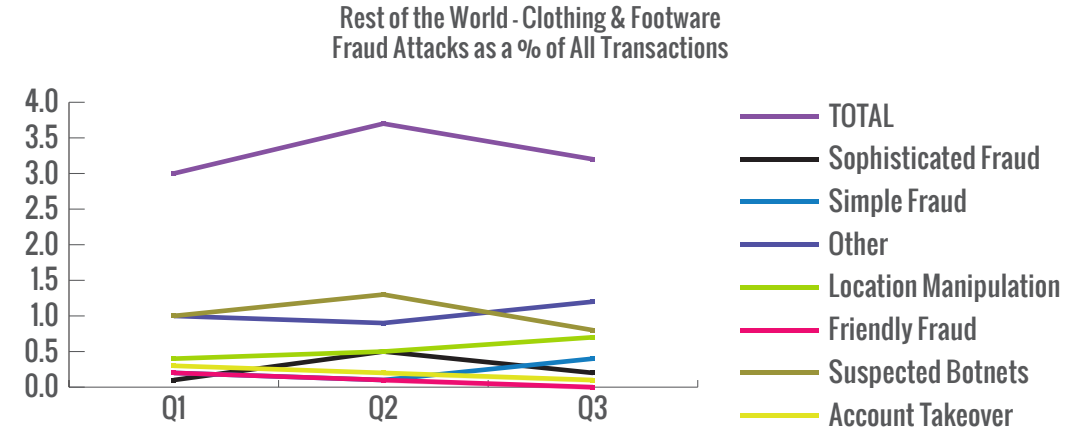


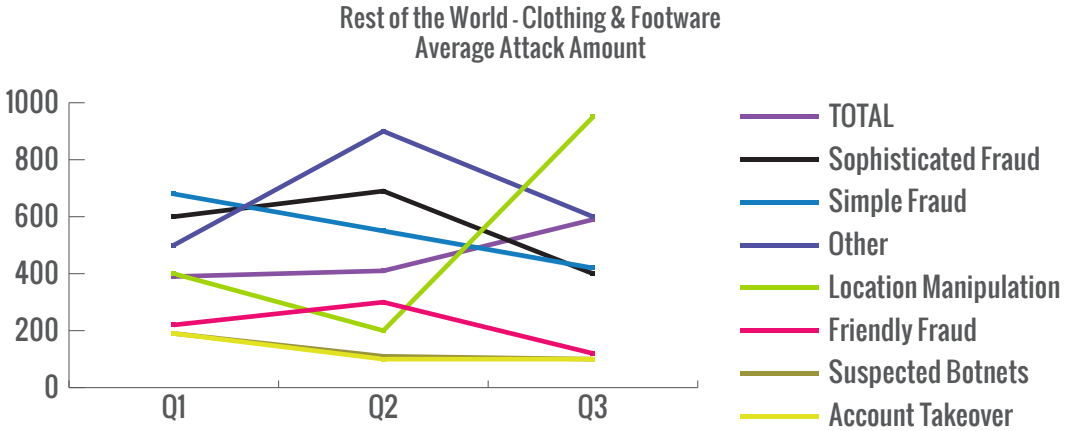
Turning to the Luxury segment, attack amounts are up for almost all fraud types, but most notably Friendly Fraud and, again, Sophisticated Fraud. The average attack amounts for both of these types have nearly doubled. Again, this is something to monitor closely in the coming quarters.

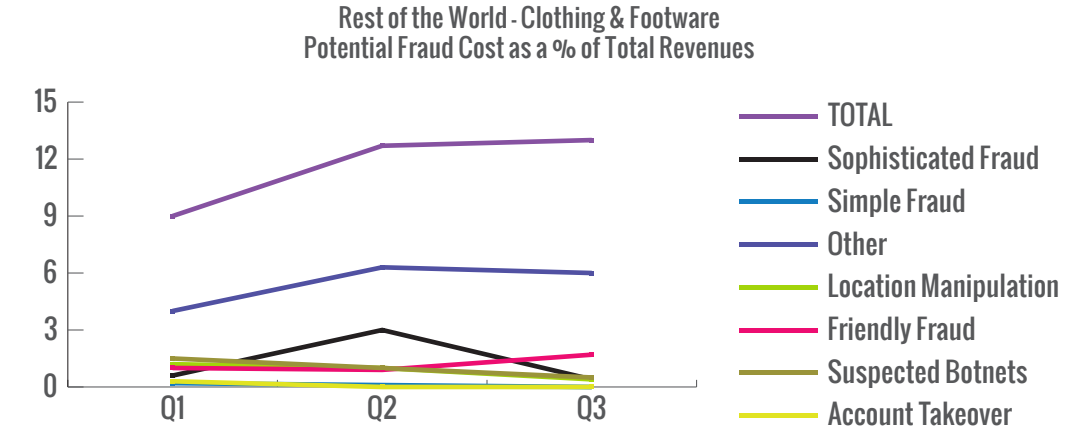


For fraud attempts originating outside of the U.S. or Europe, there is a steady and increasing trend of location manipulation, most noticeable in the Clothing and Footware merchant segment. The rate of location manipulation has doubled since the 1st quarter. At the same time, the average attack amount has increased by two and a half times. These two factors compound together and resulted in a fourfold increase in the potential cost of fraud for this category.

The impact is while location manipulation represents less then 20% of all fraud attacks in this segment, it represents over a third of the potential cost of fraud. In the first quarter, this type of fraud accounted for only 12% of the potential cost of fraud for this segment, demonstrating rapid growth if the trend continues.





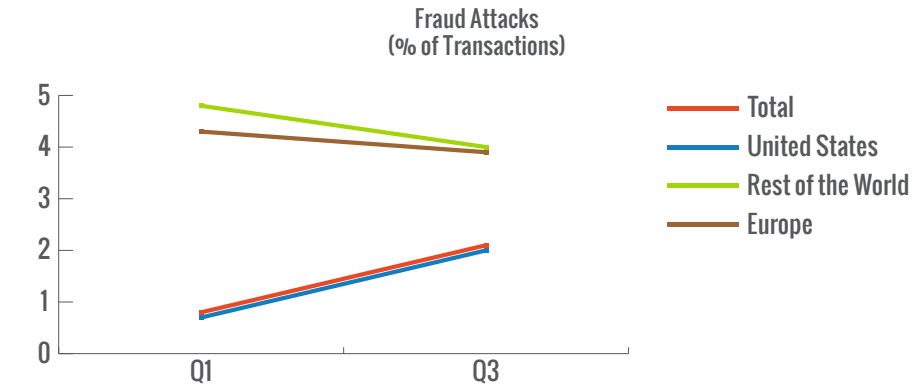


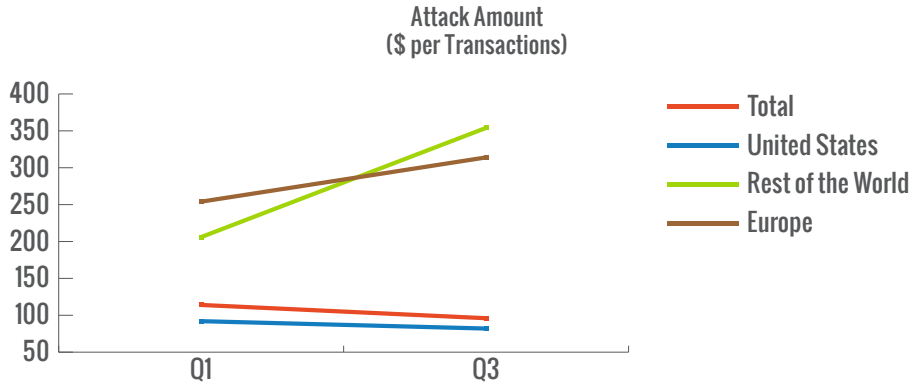
WHERE ARE THE FRAUDSTERS COMING FROM AND DOES IT MATTER?

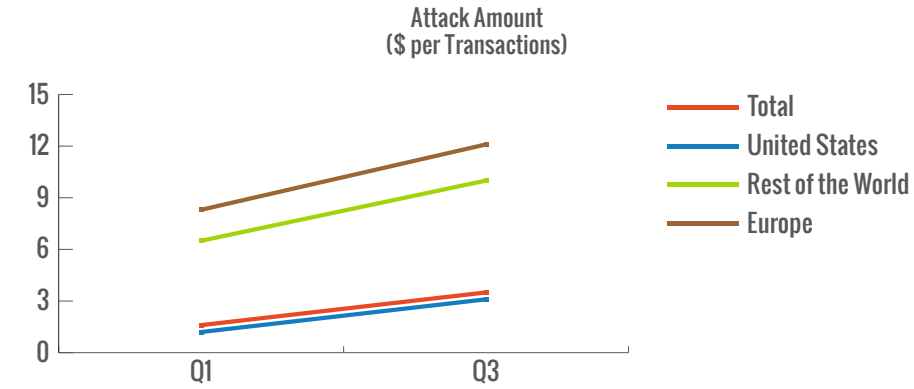
While this report focuses on U.S. eCommerce sales and attempted fraud against these sites, it is interesting to understand where fraud originates. Where are the fraudsters coming from and what are the trends?

For fraudsters originating within the U.S., their frequency of attack is increasing while the average attempted attack amount is decreasing. Conversely, when it originates within Europe or other parts of the world, the frequency of attacks are on the decline but the average attack amounts are climbing.

Given the large rise in the average amount targeted from fraudsters abroad, merchants would be smart to focus on tactics to mitigate these specific transactions to avoid fraud costs escalating dramatically.







METHODOLOGY

WHAT IS THE INDEX?

The Global Fraud Attack Index™ measures how the rate of fraud attempts on U.S. merchant websites change over time. It does so by establishing a baseline attack rate, represented as 100, which is defined as the historic average attack rate from the 1st quarter of 2015 through the 3rd quarter of 2015[7].

The report also quantifies the potential cost to merchants, left unchecked, of these attempts based on attack amounts and how these amounts are trending over time.

INDEX DEVELOPMENT

We collected data on attack rate, average attack amount and the total eCommerce revenues in the U.S. market. This data was used to evaluate trends in attack rates, amounts and the potential cost of fraud to merchants.

Attack Rate - the percent of online transactions where there was an attempt at fraud (both successful and unsuccessful)
Average Attack Amount - the average value of the transactions identified as potential fraud (successful and unsuccessful)
Potential Cost of Fraud - cost of fraud incurred by merchants as a percentage of revenues[8], assuming that every fraud attack was successful

Data was segmented and analyzed based on the geographic location of the fraudster, by primary merchant category, and by type of fraud being perpetrated.

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 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, e-books, music, gaming. Also includes business-related virtual services such as hosting and software solutions.

[7] Once data for the 4th quarter of 2015 becomes available, we will include this in the calculation of the baseline.
[8] Revenues estimated using multiple sources including Census data, Internet Retailer and PYMNTS.com analysis

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.
- Suspected Botnets - Suspected Bot describes a computer program that interacts with websites to do a specific repetitive task (legitimate or malicious). A botnet is a term used to describe an amalgamation of remote computers which were hacked and are running a "bot" for malicious activities without the knowledge of their actual users.
- Friendly Fraud - situation when the "fraudster" turns out to really 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. Can be technical or executed 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. 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.

GEOGRAPHIC LOCATIONS

The following regions were analyzed to determine different patterns of fraud based on where the fraudster originated:

- U.S.
- Europe
- Rest of the World (all countries excluding Europe and U.S.)

ABOUT

ABOUT PYMNTS.COM

PYMNTS.com is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of payments and commerce and make news.

This powerful B2B platform is the No. 1 site for the payments and broader commerce ecosystem by traffic and the premier source of information about "what's next" in payments. C-suite and VP level executives turn to it daily for these insights, making the PYMNTS.com audience the most valuable in the industry. It provides an interactive platform for companies to demonstrate thought leadership, popularize products and, most importantly, capture the mindshare of global decision-makers. PYMNTS.com... where the best minds and best content meet on the Web to learn "what's next" in payments and commerce.

ABOUT 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 analysis 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.

ABOUT THE GLOBAL FRAUD ATTACK INDEX™

The Global Fraud Attack Index™, 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 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.