

8 INDUSTRIES. 8 QUARTERS.

ECOMMERCE FRAUD INDEX

An In-Depth Study of Global Ecommerce Fraud

Table of Contents

INTRODUCTION	3
TYPES OF ECOMMERCE FRAUD	4
KEY LEARNINGS	6
TOTAL FRAUD BY INDUSTRY	9
ALCOHOL, TOBACCO & CANNABIS	11
APPAREL	14
CONSUMER ELECTRONICS	17
COSMETICS & PERFUMES	22
DEPARTMENT STORES	25
FURNITURE, APPLIANCES & HOME IMPROVEMENT	28
HEALTH, LEISURE & HOBBIES	33
JEWELRY & WATCHES	36
ABOUT SIGNIFYD	39
METHODOLOGY	40
DISCLAIMER	41
FOOTNOTES	42

INTRODUCTION

Every ecommerce merchant remembers their first fraudulent chargeback. It usually arrives soon after they've launched their site, at a time when every sale is critical. The betrayal of this first chargeback can be devastating.

Before that initial chargeback, most merchants had never heard of ecommerce fraud, or simply assumed they were protected. Chargeback losses really hurt, because they're a cash loss and are often unexpected or simply unpredictable.

Determining fraud as an individual merchant is a daunting task. Fraudsters have evolved from individual criminals to international syndicates operating with advanced technologies and disciplined organization. Fraudsters hope merchants will act alone, with only the data available to them from each transaction. This works to the fraudster's advantage. For this reason, there is no lone wolf strategy for cybersecurity. Evaluating orders alone, with limited data, is a merchant's greatest mistake.

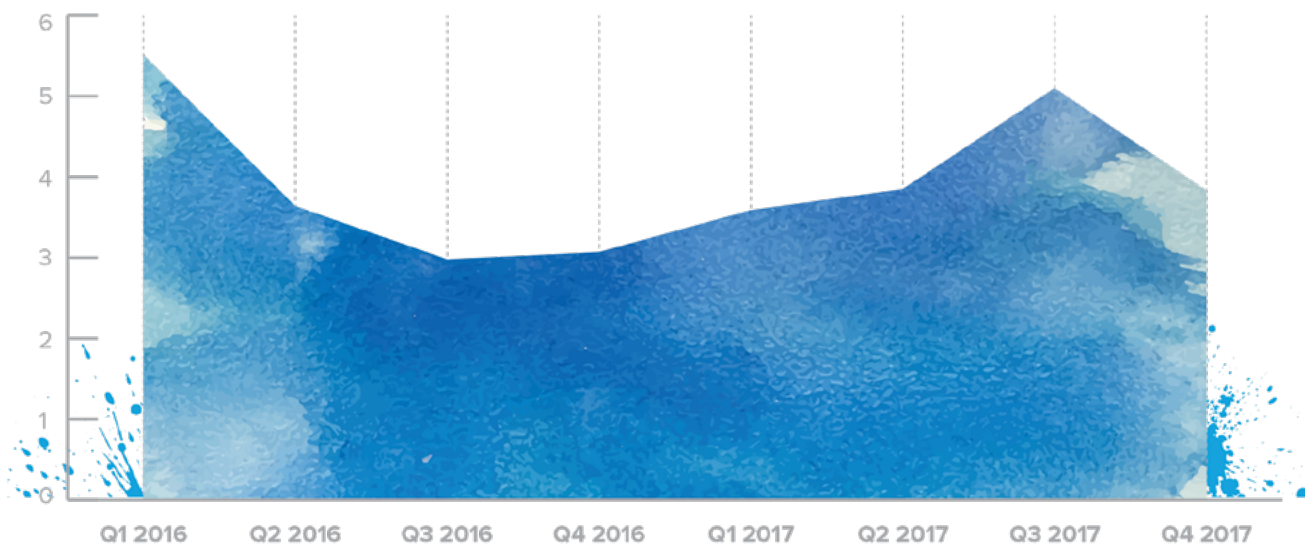
Whenever possible, merchants should leverage the data and intelligence of peers in their industry, or in the case of this report, thousands of merchants across numerous industries. This allows fraud analysts to see larger trends and a greater variety of threats so they can accept more orders while minimizing fraud losses.

To help ecommerce merchants everywhere, Signifyd is releasing the Ecommerce Fraud Index with data culminated from billions of transactions from thousands of merchants spread across the world. The data covers an 8 quarter period from Q1 2016 through Q4 2017 and is organized across 8 major ecommerce industries.

As the world's largest provider of Guaranteed Fraud Protection, Signifyd provides a 100% financial guarantee against fraud and chargebacks for thousands of ecommerce merchants. With liability for fraudulent chargebacks on a global scale, we have a first hand view of fraud everywhere, which is what we're making available what we've made available through this report.

While some fraud prevention platforms attempt to scare their customers with constant reports of increasing threats and insurmountable fraud losses, Signifyd has opted for transparency to allow merchants to see where they stand in relation to their peers.

TOTAL FRAUD (%)



TYPES OF ECOMMERCE FRAUD

Fraud losses are calculated by the total amount of orders rejected, due to suspicion of fraud, and the total amount of fraudulent chargebacks received (from accepted orders). This combined amount is represented as a percentage of total orders received. Each fraudulent chargeback has been classified in to one of the following categories.

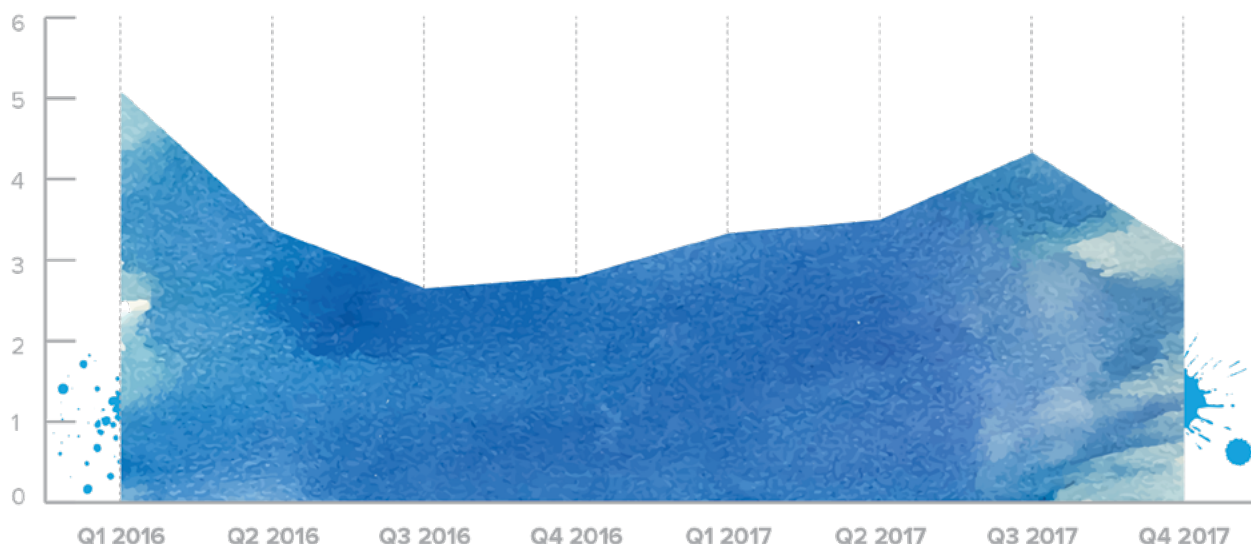
Stolen Financial Fraud

The most common type of ecommerce fraud, stolen financial fraud occurs when a fraudster uses someone else's credit card details to make a purchase, with no intention of ever paying the merchant.

Once a credit card has been tested it can be used by fraudsters across numerous merchants and can even be used to create new accounts on merchant sites, for future fraudulent purchases.

This type of fraud has historically made up the bulk of merchant fraud losses, though it now appears a new threat is emerging with the rise of account takeover fraud.

STOLEN FINANCIAL (%)



Account Takeover Fraud

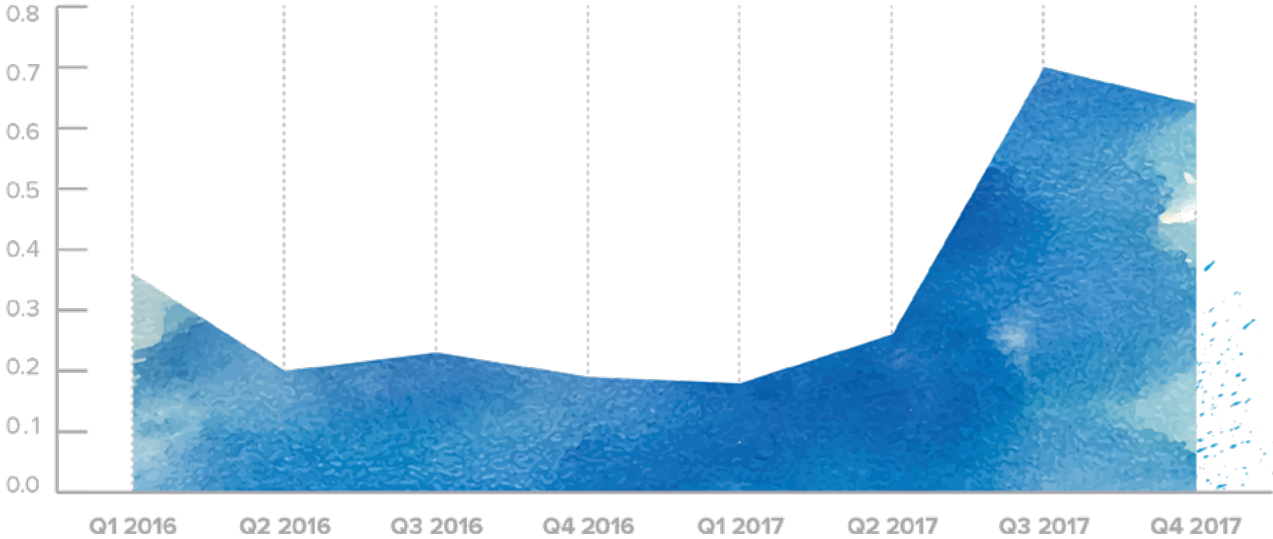
Account takeover fraud occurs when a fraudster logs in as an existing user on a merchant's site and uses pre-existing payment options to place purchases, usually shipped to a new address.

Fraudsters obtain login credentials with social engineering, by hacking databases, or by simply buying them on the Dark Web. Phishing is a common method for fraudsters to collect login credentials directly from users. The more a fraudster knows about each user, the more successfully an email can be crafted that convinces the user to follow a link to login to their account on the fraudster's replica site.

Given an overwhelming majority of people reuse passwords across most of their online accounts, fraudsters need not steal, hack or buy the credentials for a merchant's site. Instead, they can target a person's least secure account and, once they've confirmed the username and password, reuse those details across every merchant site for that person.

As the data shows for every industry we've analyzed, the massive amounts of personal data that have been hacked over the past few years have finally come back to haunt ecommerce merchants through rising account takeover fraud losses.

ACCOUNT TAKEOVER (%)

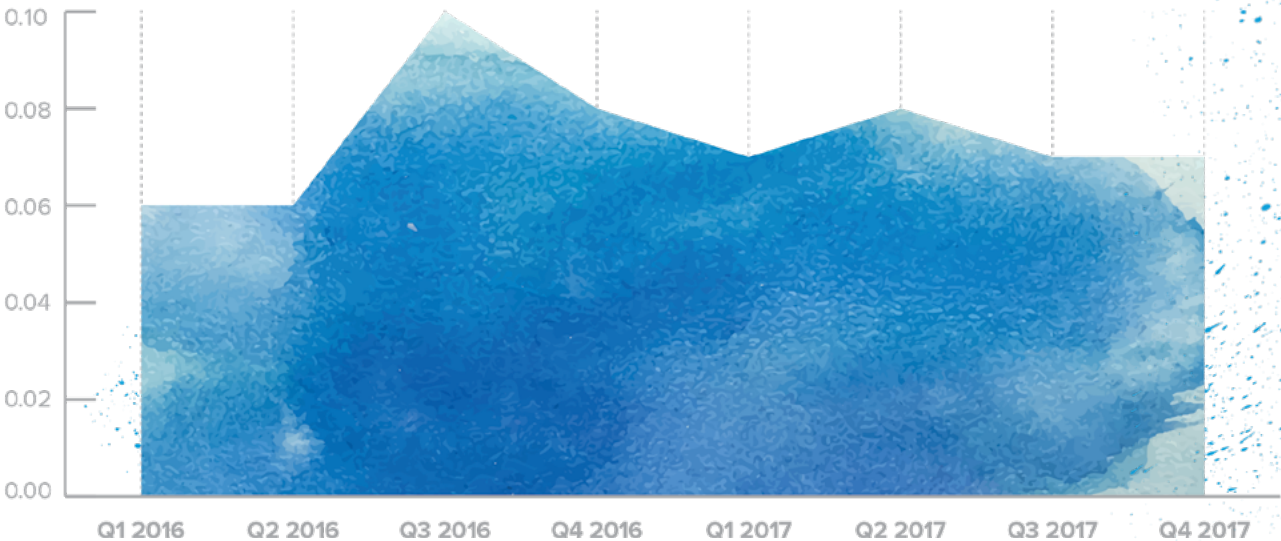


Friendly Fraud

Unlike stolen financial fraud or account takeover fraud, friendly fraud is less likely to be committed by a fraudster, or at least not by a professional fraudster working in an international crime syndicate.

Friendly fraud occurs when a person or their family, friend or guest, uses their credit card details to complete a purchase, and then denies receiving the shipment or not receiving what they paid for. Thus, unlike our other fraud types, friendly fraud is often committed by legitimate customers who are, for some reason, being dishonest.

FRIENDLY FRAUD (%)



KEY LEARNINGS

Along with the data itself, a few key learnings have emerged from this analysis, hundreds of conversations with merchants, and related studies from our fraud prevention partners.

Rising Fraud Losses, By the Numbers

7%



Total fraud losses increased 7 percent from 3.80% in 2016 to 4.09% in 2017.

24%

Losses during the holiday season were higher, with fraud increasing 24 percent from 3.07% in Q4 2016 to 3.83% in Q4 2017.

102%

The beauty industry was hit hard, with fraud increasing 102% for online cosmetics and perfume retailers from 2.52% in 2016 to 5.10% in 2017.

48%

Online department stores saw fraud increase 48 percent from 1.47% in 2016 to 2.18% in 2017.

30%

Jewelry and luxury watch merchants saw fraud increase 30 percent, from 10.43% in 2016 to 13.56% in 2017.

Account Takeover

The rising threat of account takeover fraud can be seen across every industry as it constitutes a larger portion of total fraud losses.

80%

Account takeover fraud losses increased 80 percent from 0.25% in 2016 to 0.45% in 2017.

285%

For online department stores account takeover fraud increased a whopping 285%, from 0.06% in 2016 to 0.23% in 2017, representing more than 10% of total fraud losses.

271%

For cosmetics and perfume merchants account takeover fraud increased 271%, from 0.26% in 2016 to 0.96% in 2017, representing almost 19% of total fraud losses.

194%

For jewelry and luxury watch merchants account takeover fraud increased 194%, from 0.42% in 2016 to 1.24% in 2017.



Address Unknown

Over time, fraud prevention teams develop a bias for delivery addresses, zip codes, cities, or even entire regions that just don't "feel" right. With practice this "intuition" can be honed or suppressed to remain objective.

As more consumers are buying online than ever before, there are often circumstances under which a high value order is being delivered to a seemingly odd or unfitting location. Merchants relying too heavily on delivery addresses for their evaluation are rejecting legitimate orders and losing revenue to false positives.

For example, Signifyd protects merchants shipping high end bathtubs to empty lots and U.S.-based jewelry merchants shipping diamond jewelry to Nigeria – all without fraud losses.

Size Does Matter

When compared side-by-side, larger merchants outperform their smaller counterparts with higher acceptance rates and lower fraud losses. While larger merchants generally have more budget assigned for fraud prevention measures, and obviously more data for analysis, the advantage appears to be due to a more human effect.

As merchants grow, they attract more experienced fraud prevention experts. These experts are better equipped to test new technologies and apply multiple methodologies, such as machine learning and liability shift options. This, in turn, provides larger merchants with dynamic defenses, despite being larger targets for international fraud syndicates.

So Popular It Hurts

Fraudsters prefer popular products with brand recognition since they sell for higher prices on the resale market. When merchants

Merchants relying too heavily on delivery addresses for their evaluation are rejecting legitimate orders and losing more to false positives.

with "hot" products increase their marketing efforts, they may inadvertently be driving more consumers to fraudsters offering these products on Amazon or eBay.

One example of product fandom that creates spikes in fraud are flash sales for limited edition items. Such flash sales are common in the cosmetics and apparel industries, where a brand will release a new item with limited supply. Thousands of units will sell out in minutes and their value can rise quickly. For merchants without machine learning, accepting thousands of orders in minutes can lead to hours of manual reviews and a great deal of chargebacks for fraudulent orders accepted during the flash sale rush.

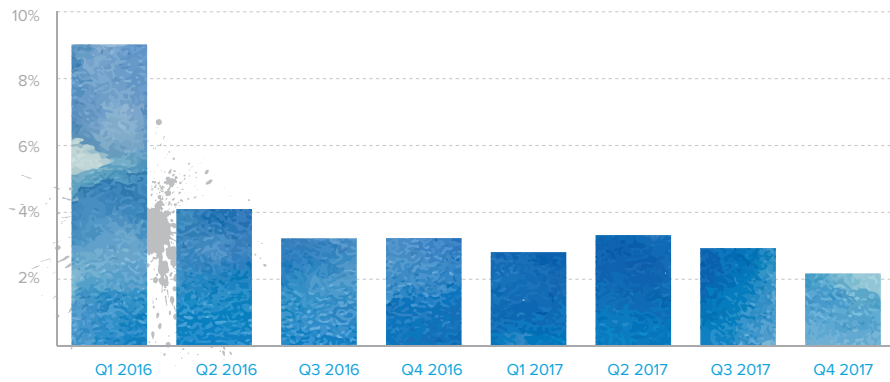
Since consumers are aware of the potential value for these limited edition items, flash sales can also increase friendly fraud losses since the opportunity for a quick profit can test the honesty of some legitimate buyers.



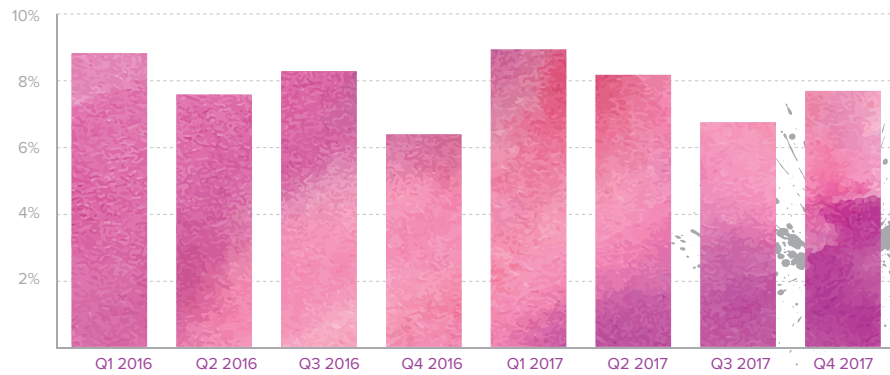
FRAUD BY INDUSTRY

TOTAL FRAUD BY INDUSTRY

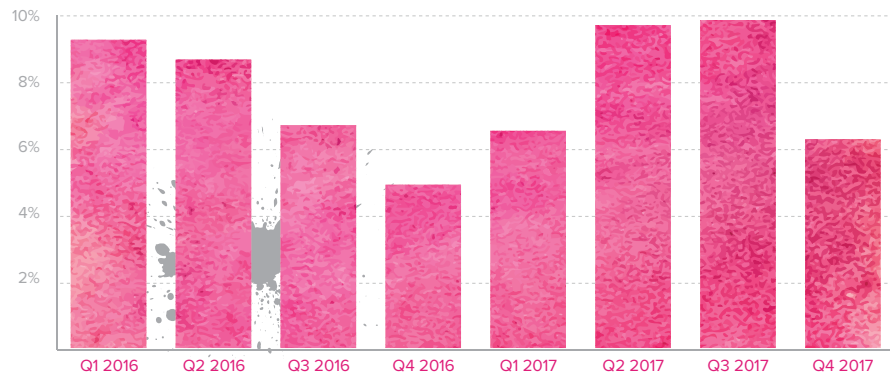
ALCOHOL, TOBACCO & CANNABIS



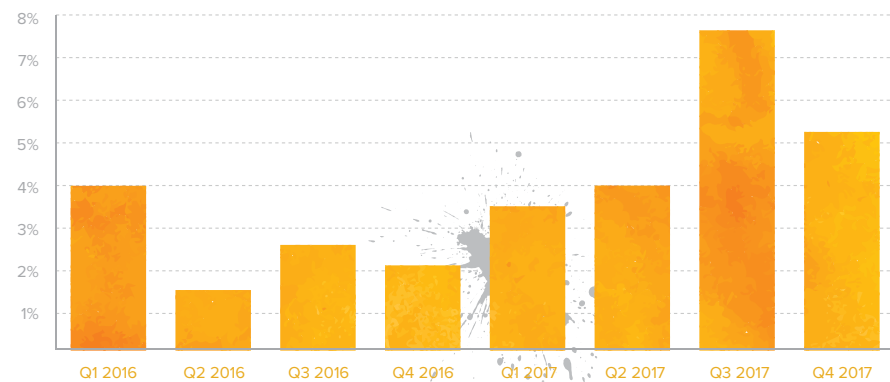
APPAREL



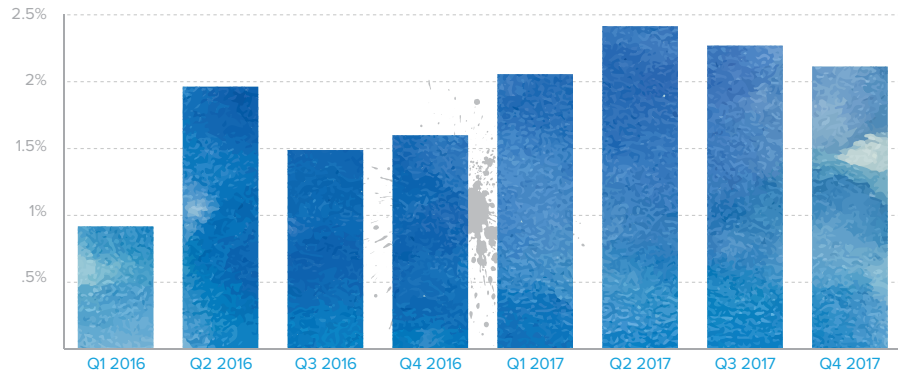
CONSUMER ELECTRONICS



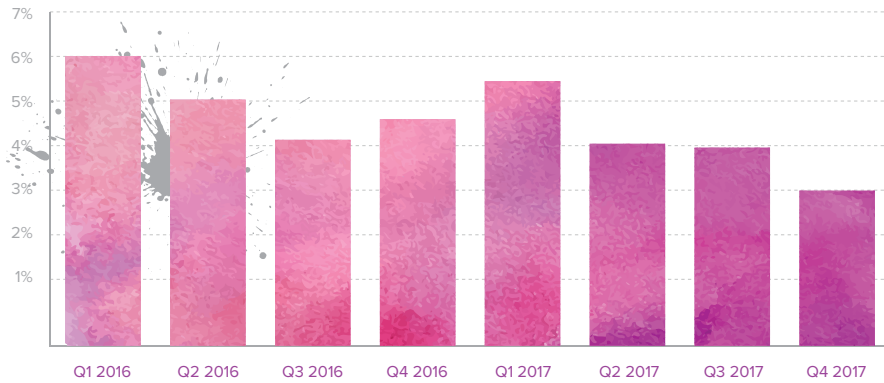
COSMETICS & PERFUMES



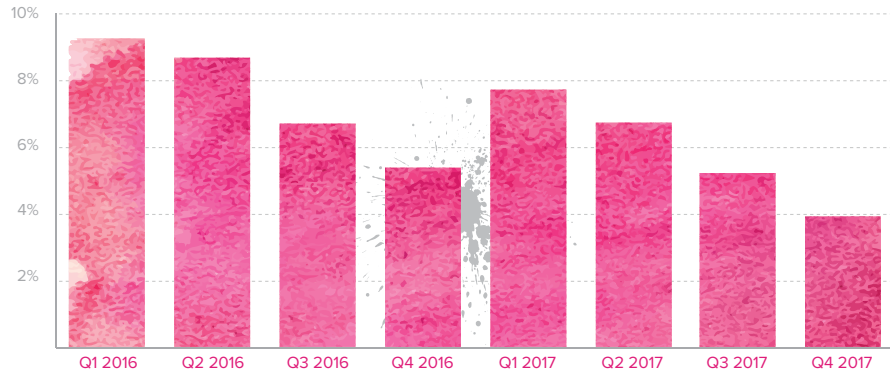
DEPARTMENT STORES



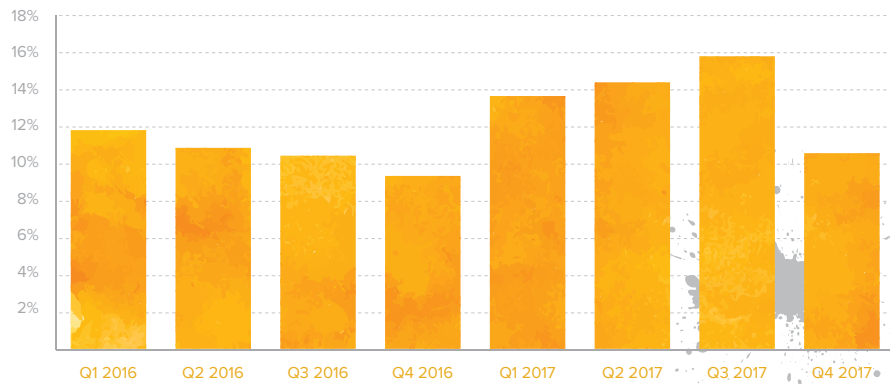
FURNITURE, APPLIANCES & HOME IMPROVEMENT



HEALTH, LEISURE & HOBBIES



JEWELRY & WATCHES





ALCOHOL, TOBACCO & CANNABIS

The alcohol, tobacco and cannabis industry includes merchants selling these substances and their related accessories and paraphernalia. For cannabis specifically, the data was heavily sourced from vendors selling accessories/paraphernalia, as there are more of these vendors online than vendors selling the dry herb or its derivatives.

Online retailers selling alcohol, tobacco and cannabis products (and related accessories), have made tremendous progress against ecommerce fraud, bringing total fraud losses down 42.6% from 4.89% in 2016 to 2.81% in 2017.

However, a large proportion of relatively safe orders below \$100 are masking the impact of rising fraud for

orders between \$100 and \$500. While total fraud for these industries was recorded at 2.93% in Q3 2017, total fraud for orders between \$100 and \$500 rose to 4.47% in the same quarter.

Globally, most alcohol is still purchased at brick-and-mortar supermarkets as part of a consumer's grocery trip. However, online alcohol sales have boomed worldwide over the past few years. In China, online sales for wine now make up a significant share of total wine sales, and Amazon Japan offers a staggering 150,000 different choices for alcoholic beverages.

For ecommerce merchants, the shift to buying alcohol online represents a significant opportunity, led by millennials predominantly buying wine and spirits. Online shopping cart totals are often higher than what they would purchase in a single visit to the liquor store and online shoppers prefer better known brands.¹

A combination of buyers with rich digital footprints and urban billing and shipping addresses has helped online merchants identify fraud accurately.

Meanwhile, the global e-cigarette and vaporizer market is expected to experience double-digit growth over the next 10 years, particularly in China and India. However, this growth will be shaped by regulatory developments, so it's difficult to pinpoint an exact growth figure. Industry consolidation², price increases, and growing demand for tobacco-heating products (THP) have helped tobacco brands grow over the past year. In the US, it also remains to be seen how new legislation could affect online sales for THP in certain states.

43%

Decrease in total fraud losses from 2016 to 2017

23%

Account Takeover fraud as a share of Total fraud losses in Q4 2017

As can be seen across other industries in this report, the rising threat of account takeover fraud is impacting total fraud losses for alcohol, tobacco and cannabis merchants. Account takeover fraud losses peaked at 0.79% in Q1 2016 and rose again to 0.66% in Q3 2017. For orders between \$100 and \$500 account takeover fraud reached a frightening 0.95% in Q3 2017. Alcohol, tobacco and cannabis merchants are advised to take precautionary measures against account takeover fraud as it represented 22.6% of total fraud losses in Q4 2017.

A combination of buyers with rich digital footprints and urban billing and shipping addresses has helped online merchants identify fraud accurately. Further reductions in fraud losses can be achieved by reducing false positives for orders from legitimate customers who are either new to buying online or simply buying in quantities larger than merchants might expect.

SUCCESS STORY

RESERVEBAR

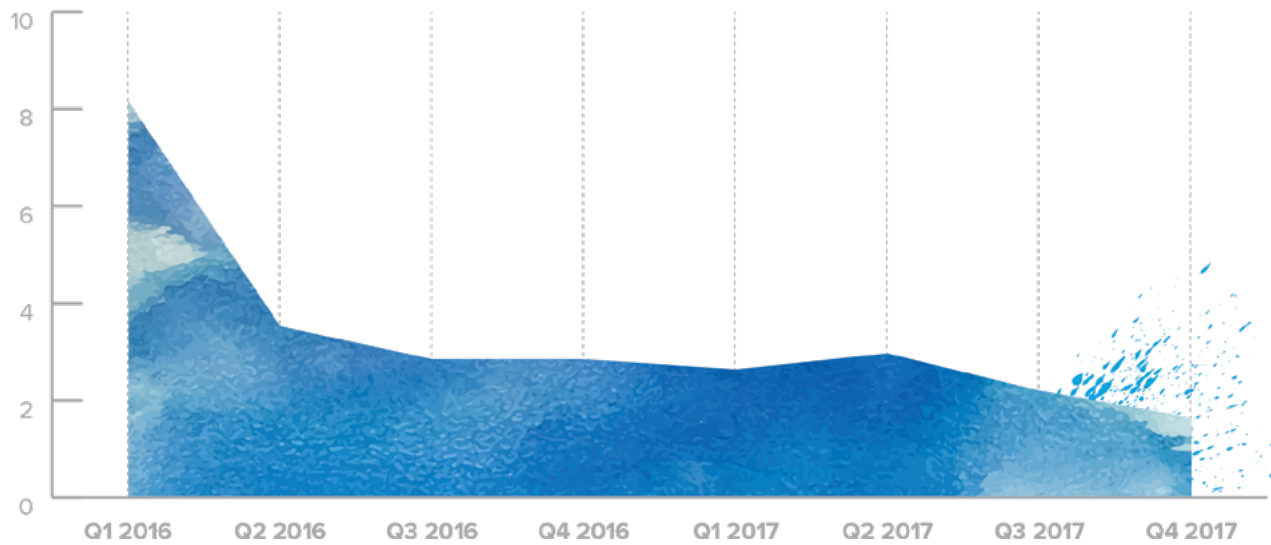


As the premier digital marketing platform for premium and luxury brand spirits, ReserveBar offers its customers limited release, special edition bottles of whiskey, vodka, cognac, tequila and wine. Customers can have each bottle custom engraved to create one-of-a-kind gifts for their personal and professional connections, or for self-consumption. As the official ecommerce partner for the world's leading spirits brands, ReserveBar is committed to delivering a premium experience with every purchase.

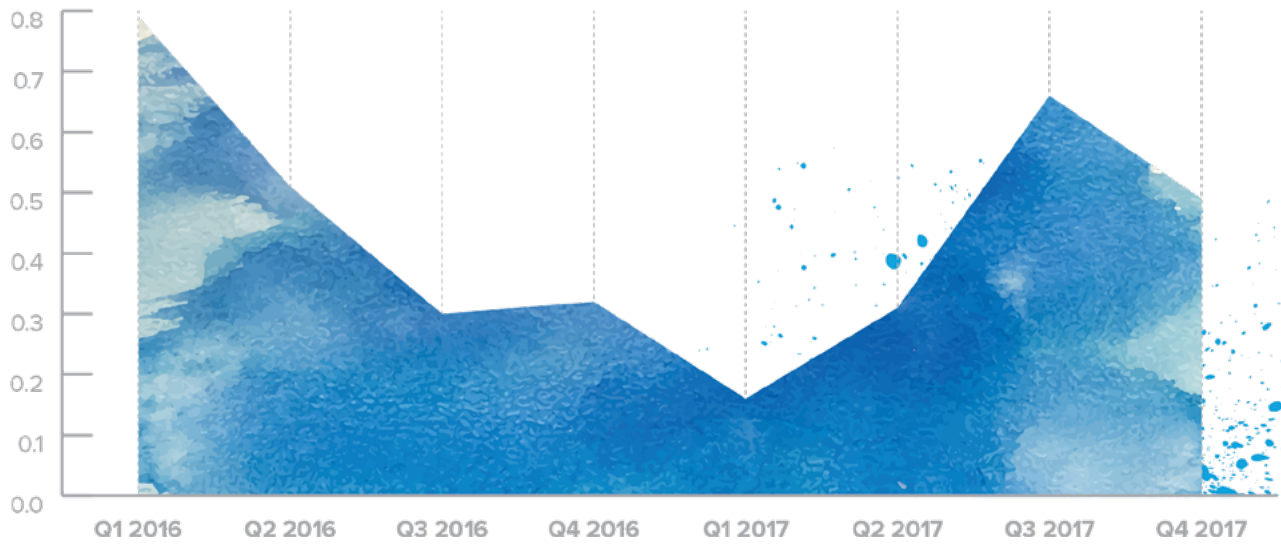
When ReserveBar launched, co-founder and president Lindsay Held was surprised by how quickly fraudsters began attacking the site. Held took these losses personally, as they were stealing his products to resell on their own. Held's team quickly began noticing patterns to identify some of these fraudsters so their orders could be promptly declined. But legitimate customers also demonstrated some of these patterns and their orders were inadvertently cancelled. Even with a defensive approach, the ReserveBar team was unable to stop their fraud losses from chargebacks each month, which is when Held sought a different solution.

Frustrated with the prevailing attitude among payment processors and other online retailers who claimed ecommerce fraud was simply an unpredictable cost he would have to bear, Held opted for Guaranteed Fraud Protection, which offers a 100% financial guarantee against fraud and chargebacks. By shifting fraud liability to Signifyd, Held was able to accept more orders without fraud losses, while freeing up his team to focus on acquiring new customers and delivering orders faster. This has helped ReserveBar scale tremendously, facilitating faster growth and new partnerships with other premium gift brands.

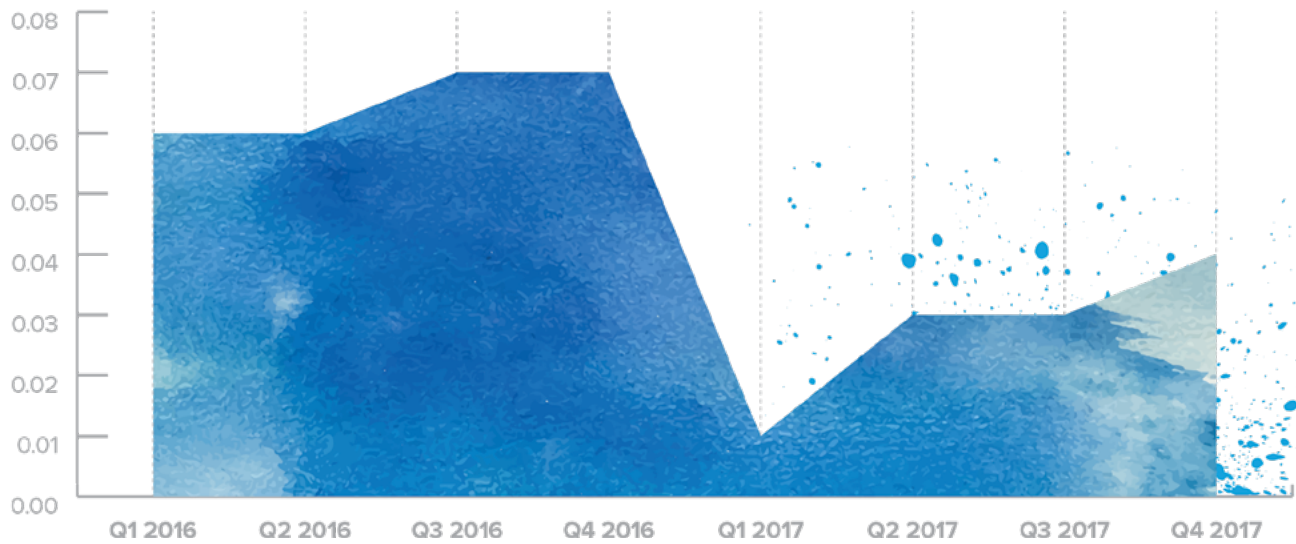
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)





APPAREL

Apparel covers all clothing, shoes, and accessories such as belts, hats and sunglasses. Given the number of retail stores that closed in 2017, one might think brick-and-mortar stores were dead, or at least desperately ill. Instead, brands have made a comeback by testing new concepts and innovating their in-store and online shopping experiences.

In particular, the luxury sector is evolving with “affordable luxury” and celebrity-designed fashion attracting larger audiences. “Athleisure,” which combines athletic and leisure wear has had impressive growth, fueled by millennials’ more relaxed dress code standards and the busy lifestyle of the modern worker. Lululemon, Under Armour and Nike are among the brands that brought athleisure to prominence. Other brands have jumped on the bandwagon, too, including Gap and J. Crew.

McKinsey estimates the category will maintain 6.5 to 7.5 percent sales growth in the next year. Athleisure is growing even faster in countries like China, Japan and India, where industry estimates say the category is growing at a rate of 20 to 25 percent annually. 2018 is likely to be the first year the United States and Europe will account for less than half of apparel sales worldwide as emerging markets continue to flex their consumer muscles.

Growing demand and a constant supply of new online buyers is the perfect mix for fraudsters, unfortunately. In luxury apparel, a growing trend of luxury manufacturers releasing limited numbers of highly coveted products is creating hotspots for fraud. Resellers charged upward of \$1,500 for designer, limited edition sneakers, more than seven times the original retail price. Numbers like these, combined with short supply, create a strong incentive for perpetrators.

At the end of 2017, total fraud losses for merchants with orders between \$100 and \$500 was at 7.36%, but it more than doubles to 16.53% for merchants with orders above \$500.

The rising threat for merchants selling higher end clothing and shoes is account takeover, which ranges from 1.35% for orders between \$100 and \$500 to 6.04% for orders above \$500.

With Amazon and its marketplace sellers accounting for about 40 cents of every dollar spent online for shoes and clothing, progressive retailers are embracing new technology to keep up with consumers, while holding their own with Amazon.

“For those leaning forward and willing to help design the new features of the modern fashion system, the opportunities at hand to truly connect with fashion consumers across the globe have never been greater,” says “The State of Fashion 2018,” a report prepared by McKinsey and the Business of Fashion, or BoF.³

21%

Increase in total fraud losses for the holiday season from 2016 to 2017

49%

Increase in account takeover fraud from 2016 to 2017



WATCH THE VIDEO

SUCCESS STORY

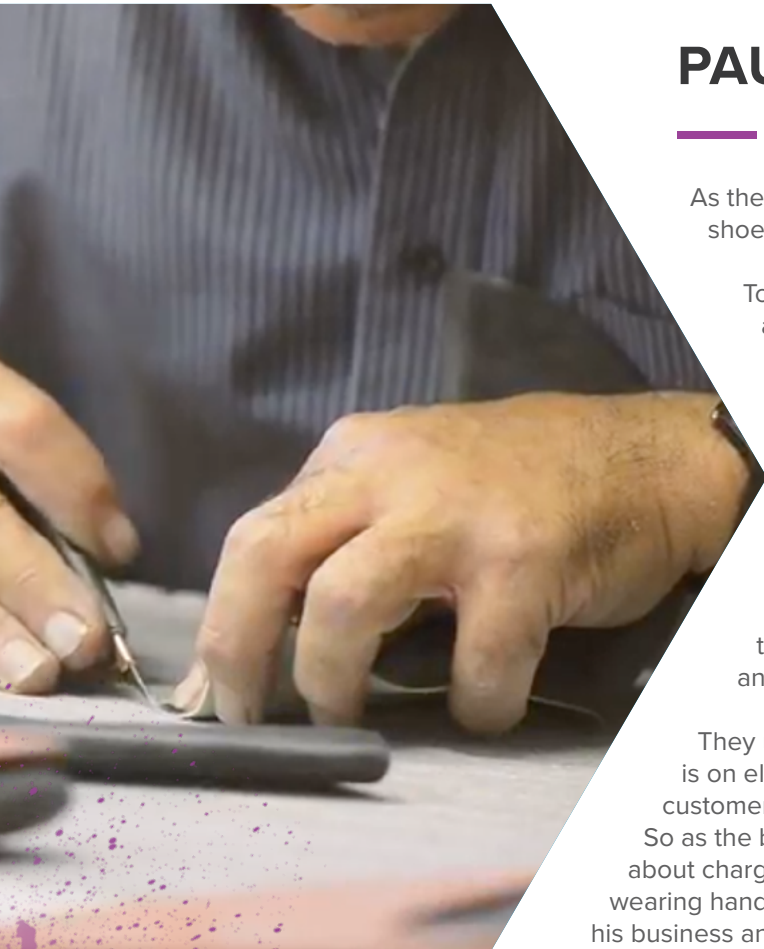
PAUL EVANS

As the CEO of Paul Evans, Evan Fript is designing more than just shoes, he's designing a business.

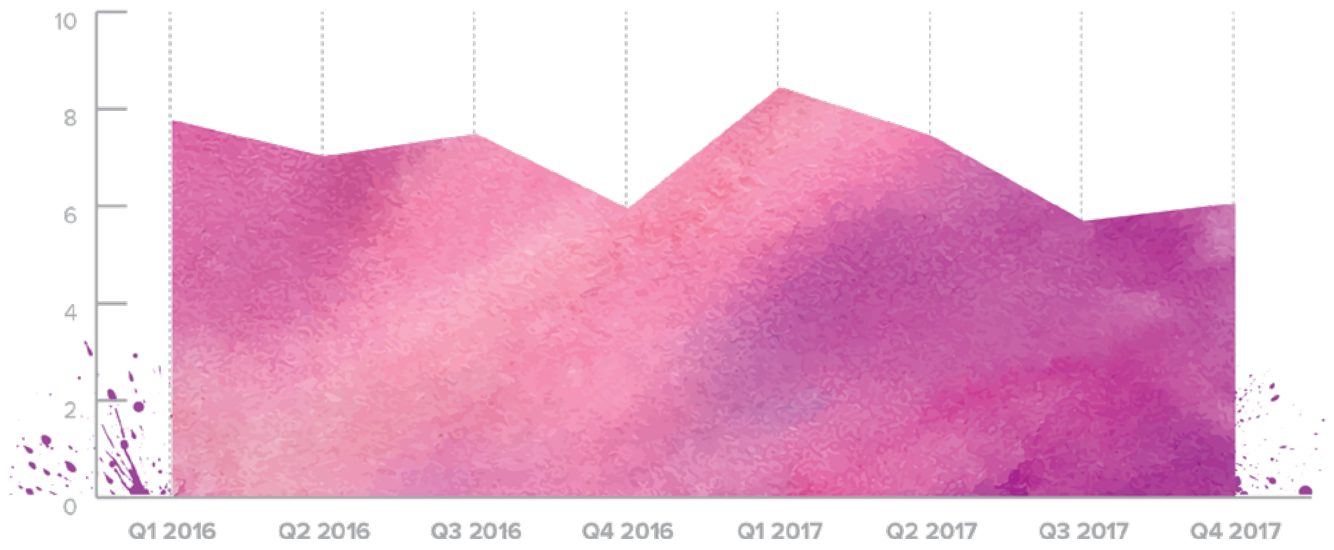
To do this right he needs to focus on just a few things, all of which provide value to his customers. He starts by sourcing the best product. Paul Evans was founded on the goal of producing the world's best shoes at the best possible price. They provide a seamless experience for online shoe buying because men don't want to shop for shoes, they want to buy them.

Paul Evans drives growth by removing the middleman and reaching customers directly in over 50 countries. Their shoes are sourced directly from Naples, Italy, and they provide free international shipping with an unparalleled 365-day return policy.

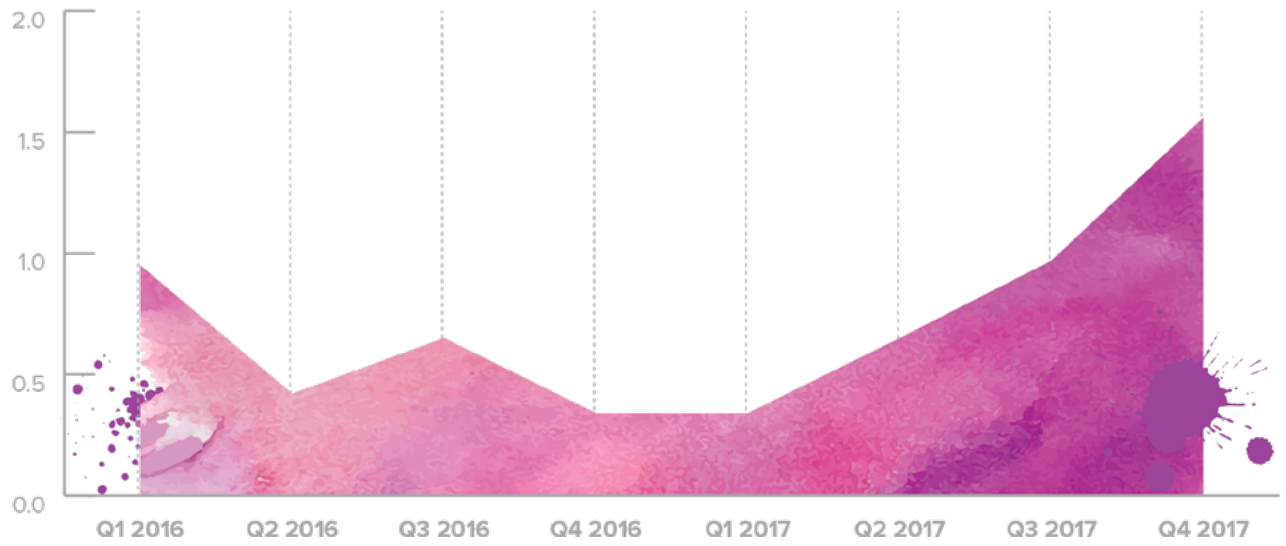
They use Signifyd for the same reasons. Signifyd's focus is on eliminating fraud by verifying all of Paul Evans' potential customers, which allows them to easily accept more orders. So as the business continues to grow, Fript doesn't need to worry about chargebacks or fraud. Focusing on growth means more men wearing handcrafted shoes, which allows Fript to focus on building his business and growing the Paul Evans brand.



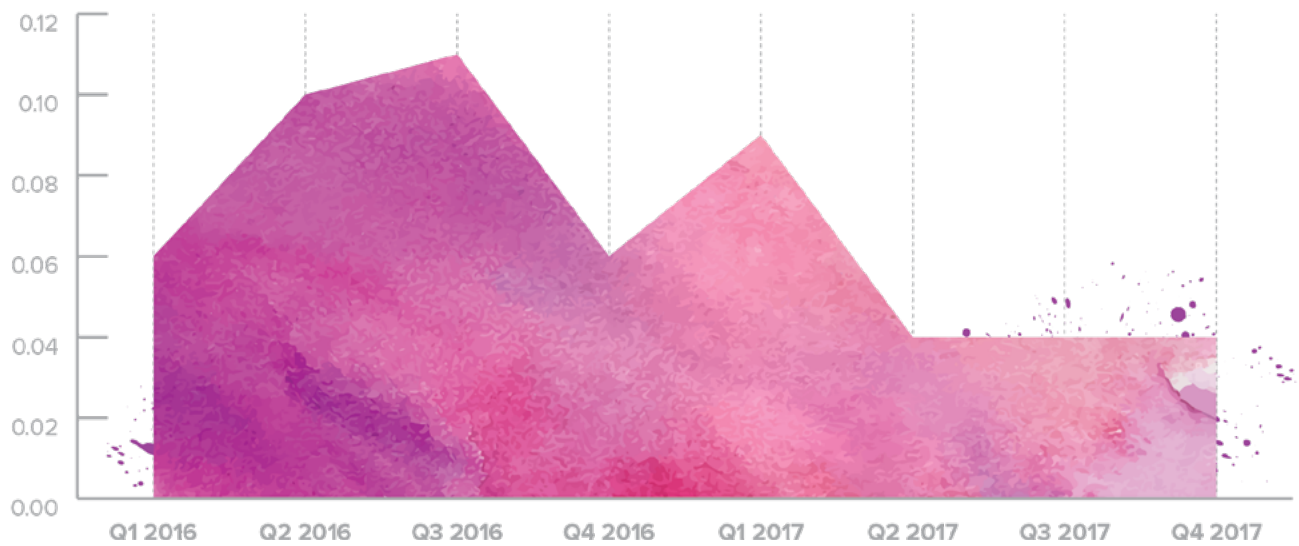
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)





CONSUMER ELECTRONICS

Consumer Electronics covers items as varied as televisions, laptops, digital cameras, flash drives, drones, electric scooters, hoverboards and wireless earbuds. Excluding automobiles, if it's powered by batteries, it'll likely fall into this category.

For the past few years, ecommerce merchants in the consumer electronics industry have been waging war with fraud syndicates with heavy losses on both sides. As merchants make progress in one quarter, with stolen financial fraud for example, they need to be prepared to lose that advantage the next quarter as fraudsters evolve their attack methodologies.

Total fraud increased 9.54% from 7.34% in 2016 to 8.04% in 2017. Account takeover has emerged as a rising threat, climbing 100.79% from 0.28% in 2016 to 0.56% in 2017.

With growing global demand, sales for consumer electronics will be multiplied by the rapid growth of the middle class, led by China and India, the world's most populous countries. McKinsey says 1.4 billion people will join the global middle class by 2020, and 85% will be in the Asia-Pacific region.⁴

One study predicts the value of the global consumer electronics industry will be \$1.6 trillion by 2022 as a result of this trend.⁵

In particular, gizmos driven by artificial intelligence will be more prominent in homes around the world. At the top of the list are voice-enabled speakers, such as Amazon's Alexa, Google's Assistant and Apple's HomePod. The market for the speakers/home assistants should reach \$2.68 billion in 2018, setting off a gadget rush that is expected to climb to nearly \$12 billion by 2023.

101%

Increase in account takeover fraud from 2016 to 2017

10%

Increase in total fraud losses from 2016 to 2017

21%

Increase in total fraud losses for the holiday season from 2016 to 2017

And smart speakers are just the start. Homes are also being rapidly transformed by connected devices via the Internet of Things (IoT). IoT features have gone mainstream and manufacturers are connecting smart locks, refrigerators, washing machines and televisions, to name just a few.

IHS Technology says that demand for connected goods will experience triple-digit growth over the next few years. And by 2020, the number of internet connected goods shipped annually will reach 223 million.⁶

The signs point to a growing pie, now it's up to retailers to figure out how to best win their share.

[WATCH THE VIDEO](#)



SUCCESS STORY

PRECISION CAMERA & VIDEO

Precision Camera & Video was founded by Jerry and Rosemary Sullivan in 1976 in Austin, Texas. It's probably the biggest camera and video store between New York and LA.

It's also one of the few places where you can buy, rent and get equipment repaired in one place.

Precision Camera & Video has extended their in-store hospitality to their online business with free shipping for orders over \$200, free in-store pick up and free local delivery. Their goal is to take care of customers online as if there were right there in the store. That's why real humans pick up the phone to answer questions when customers call.

Because of their wide variety of products, Precision Camera & Video sees customers come to their site from many different channels, including search, social and their outbound special offers. But this is also why they hate turning down customers or being unsure of whether they should or shouldn't ship an order, especially when the customer is asking for rush delivery.

Signifyd has helped Precision Camera & Video eliminate fraud and chargebacks so they can accept a lot more orders and ship them out immediately, knowing they're covered by Signifyd's financial guarantee against fraud and chargebacks.

The team at Precision Camera & Video used to do hours of manual review on orders, especially higher value orders, but now they get an immediate decision, backed by a financial guarantee.

So they're able to serve more customers online and in-store and scale their business significantly with the same great service that drives their customer satisfaction and loyalty.

And that's important, because that's why Jerry and Rosemary started the business over 40 years ago.



SUCCESS STORY

ALEPH OBJECTS

3D printer manufacturer Aleph Objects, Inc. signed up with Signifyd and put the service to the test during the holidays (a peak sales period for the company).

“Signifyd actively caught a case of fraud for us, after going through our standard pre-transaction fraud prevention policies and procedures,” recalls Megan Garber, the company’s sales support supervisor. “We never had this happen before, where we actually caught a case of fraud after an order was placed.”

The story began when the company realized a customer was returning to an abandoned or “cold” cart. This triggered a routine email along the lines of, “Hi we see you have some products in your cart. Is there anything we can do to help you?” Garber said. “He contacted us and we spoke with him on the phone. He said he had been having problems checking out through the website, so he wanted to try to place the order directly with us over the phone. But when the sales rep put his credit card information in and pushed it through, Signifyd flagged it as fraud,” she said.

“About a week later we got a call from another person saying they had received a charge from our company on their card. They were confused and they were checking into things because they had never ordered from



us,” said Garber. Aleph Objects was able to match the transaction details with those from the “cold” cart fraud incident. Fortunately, the charge was already voided on the woman’s credit card, Garber said. Fraud containment staff at Aleph said because of Signifyd, in this case, it made the process much simpler.

Since 2011, when they began selling 3D printers online to hobbyists, educators, engineers, and more, the company has grown exponentially, as has its exposure to fraud. Online sales now make up over a third of Aleph Objects’ business. “I’ve been here since November of 2015 and when I started there were 99 employees. At last count there were 144 employees and that was February of this year,” said Garber. “We went from \$15 million to over \$20 million dollars in one year alone.” K-12 and higher education institutions, manufacturers, and resellers make up the bulk of Aleph’s online business through LulzBot.com. Across all sales channels, the company has customers in over 85 countries around the world.

Prior to signing up with Signifyd, Aleph lost \$50,000 – \$75,000 a year to fraud and the company dedicated two full-time staff members to contain fraud, among other responsibilities. Garber said fraudsters like to steal the more expensive of the company’s two models of 3D printers: the LulzBot Mini, which is priced at \$1,250 and the LulzBot TAZ 6, which sells for \$2,500. “They’re not trying to scam us for filament or accessories. They’re always going for the big stuff,” she said. Learn more about the LulzBot line of desktop 3D printers at LulzBot.com.

Signifyd protects Aleph Objects with real-time machine learning that incorporates extensive external data and domain expertise so merchants can accept more orders. But if a fraudulent order gets approved, which has happened for Aleph Objects, Signifyd reimburses them because every approved order is protected with a financial guarantee against fraud.

“Around New Year’s we saw a series of attempted fraud orders come through. This was new for anyone who had been on the team at that point,” Garber explains. “When we looked into it further, there were several cases that were caught and we were able to avoid shipping out the printers.” After being notified that these cases were being held for manual review, Garber says her fraud-containment staff noticed other orders that were also being held were using the same name, she said. “They were using the same name in the order but then placing it from slightly different places, slightly different addresses, but they were all tying back to the same IP address.”

Garber said she joined Aleph Objects, in part, because the company is “Committed to Free Software, Libre Innovation, and Open Source Hardware. This means we are open and encourage people to make changes and make things better so that we share those improvements. That allows us to put out the best product and the best things for our customers. That’s what really intrigued me. Being somewhere that was so open to that.”

Garber said today her greatest challenge when screening orders for fraud is “trying to make sure I’m soft enough and do it with an understanding point of view. So the customer isn’t put off and wants to return it or be done with it. But I’m still making sure we’re not letting people attempting fraud through, even though we have Signifyd.”

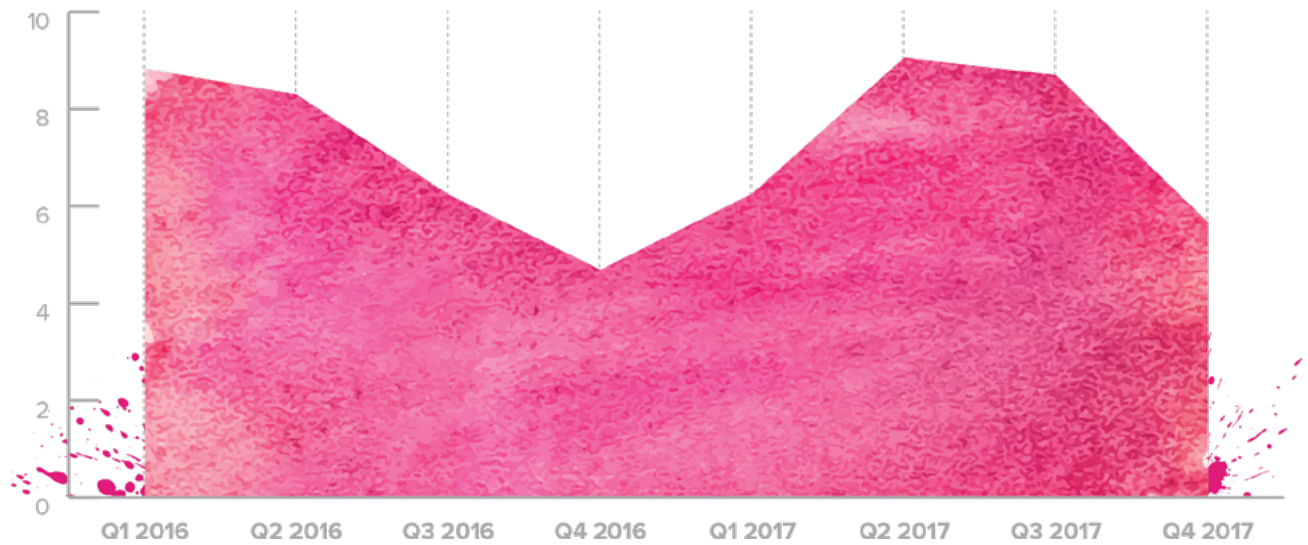


“They were using the same name in the order but then placing it from slightly different places, slightly different addresses, but they were all tying back to the same IP address.”

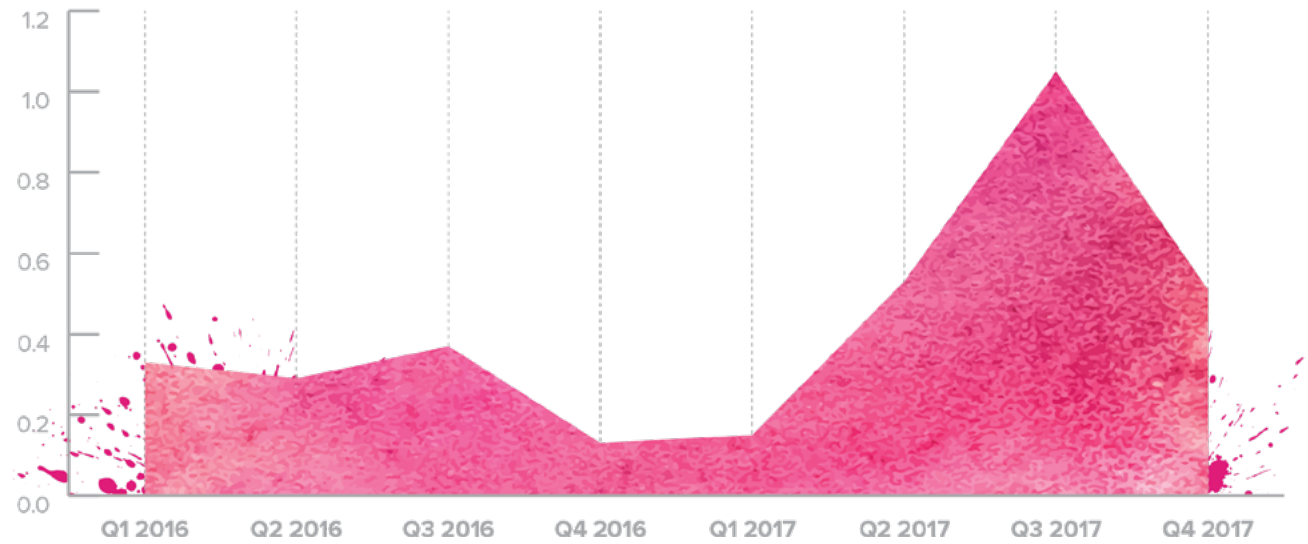
The customer experience remains top of mind for her. “Anytime somebody gets the email that says their order is being held for manual review, they get a little on edge. So I’m making sure we’re working through the process to get them approved and that we’re selling to a real person who’s really buying this with their own money.”

READ THE CASE STUDY

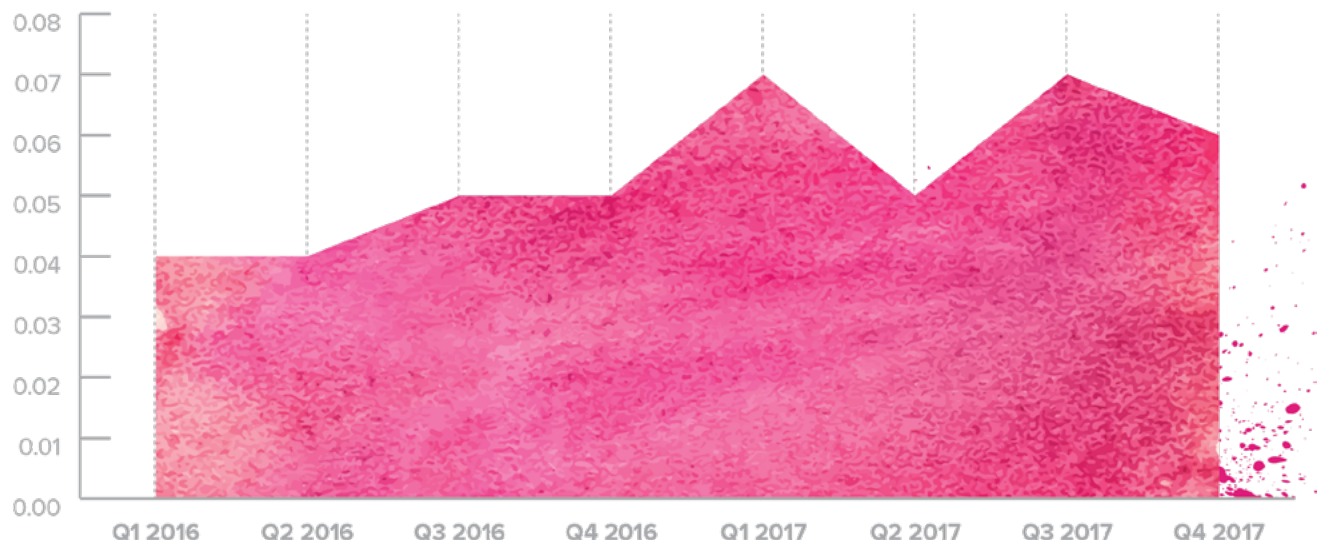
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)





COSMETICS & PERFUMES

Cosmetics and perfumes includes fragrances, makeup, wigs and skin care for men and women. Traditionally, shoppers considered cosmetics and perfumes to be products that had to be tested in-person. However, thanks to beauty tutorial videos and Instagram influencers, the divide between in-store purchasers and online shoppers is narrowing.

There's the constant introduction of new brands, new products and rapidly evolving trends, as well as the ongoing need to educate consumers about how to use products correctly. Then there's consumers' desire for hassle-free repeat purchases which paved the way for subscription services such as Birchbox and its regular deliveries of preselected products.

The beauty industry is facing an uphill battle with ecommerce fraud. While gains were made throughout most of 2016 and the early part of 2017, total fraud rose to an all-time high of 7.48% in Q3 2017 before settling down to 5.34% at the end of 2017.

At 1.48% in Q4 2017, account takeover fraud represented a devastating 27.7% of total fraud losses. This rise in account takeover fraud reverses the progress online beauty retailers had made against stolen financial fraud.

The beauty industry
is facing an uphill battle
with ecommerce fraud.

The pace of the cosmetic and perfume segment has picked up considerably with startups blossoming and consumers demanding that they be catered to as individuals, not demographics. Digital technology has given shoppers the tools to try on looks and find the specific one that reflects the person they know themselves to be.

103%

Increase in total fraud losses from 2016 to 2017

271%

Increase in account takeover fraud from 2016 to 2017





Consumers can buy kits that enable them to make everything from their own signature scents to specialized serums for their particular type of skin. This trend is similar to what people expect from their technology: personalization and customization. So we may be entering the era of “iMakeup.”

For younger buyers, limited edition beauty products and flash online sales are all the rage. Such flash sales are common in the cosmetics industry, where a popular brand will release a few new colors or an entire mini-collection on a particular theme. These flash sales sell out in minutes, and once completed, these products may not be available for some time - or ever again - depending on the brand’s strategy. For individual merchants without machine learning, accepting thousands or tens of thousands of these orders in less than 30 minutes can lead to hours of manual reviews and a great deal of chargebacks for fraudulent orders accepted in the rush to ship orders out on time.

Meantime, beauty entrepreneurs are fueling their own growth by taking a page from the digital revolution and

turning to venture capitalists to fund their innovative companies. The number of beauty startup deals jumped from 86 in 2012 to 150 in 2016 with a five-fold increase in investment, reaching \$608.9 million.

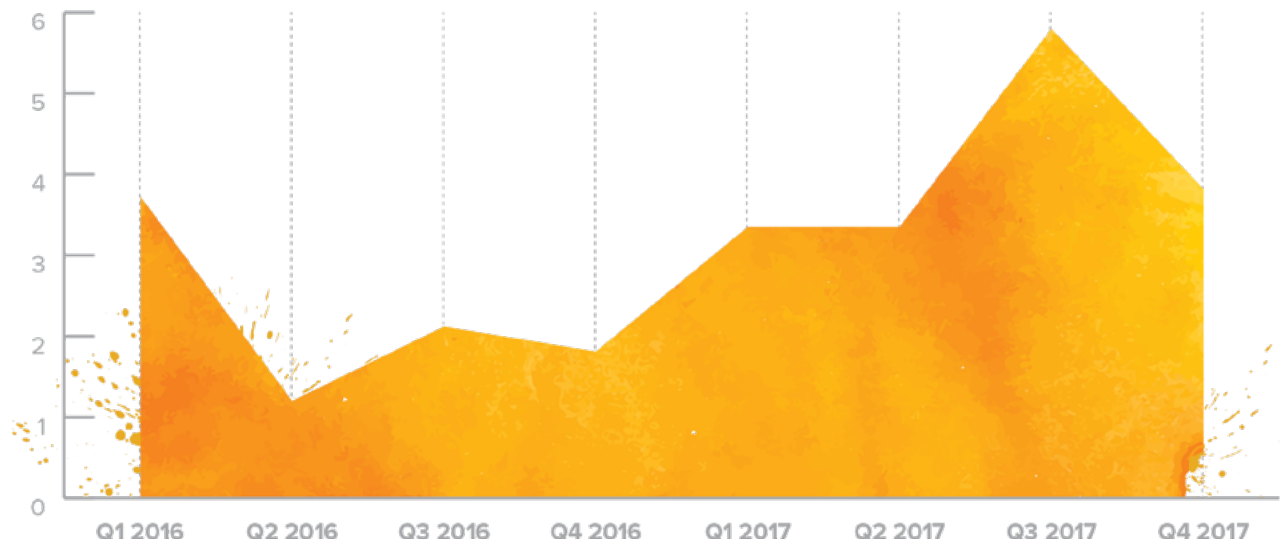
These young, hungry companies are supported by labs, like the Cosmetic Laboratories of America and Ariel Cosmetics Laboratories, where they can team up with chemists to develop new products. And they are finding sales channels at retail leaders such as Sephora and Ulta, which are willing to give shelf space to small companies producing high-quality products.

Hot new products also come with a 21st century twist. “Clean beauty” is the buzz phrase as products made with natural ingredients are gaining both mindshare and market share.

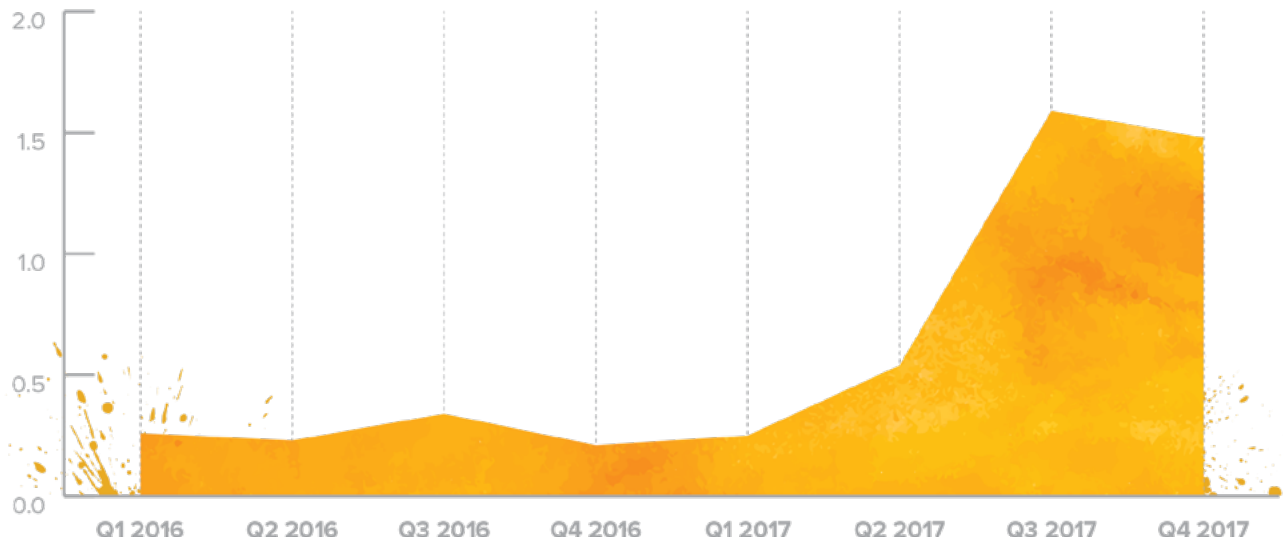
Which is not to say that traditional brands have been totally upended, as evidenced by the other hot category in cosmetics and perfume: Luxury. Sales of high-end products are growing at a rate that eclipses the industry as a whole.



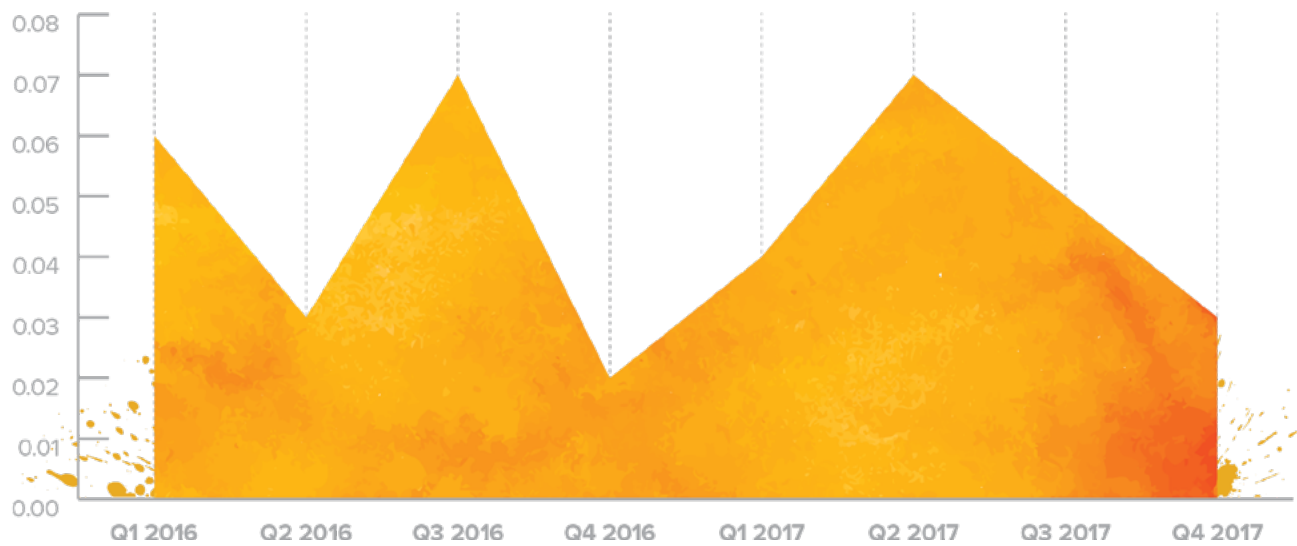
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)





DEPARTMENT STORES

Department Stores are classified here as ecommerce merchants selling a wide variety of household products intended to save the consumer a trip to his or her local grocery store and/or the department store. As such, the products sold may overlap with merchants in the Apparel, Cosmetics and Perfumes, Consumer Electronics, or Furniture, Appliances and Home Improvement categories.

With expert fraud prevention teams, more varied transactions, and very large customer bases, online department stores and grocery sites have had an impressive track record for managing fraud effectively. By Q4 2017 total fraud losses rose to 2.09% from 1.61% a year earlier. However, this was still lower than total fraud losses in Q2 and Q3 in 2017.

One area where department stores are struggling with ecommerce fraud losses are higher value transactions. Merchants need these higher margin orders to make up for their competitive pricing on lower-priced groceries and household items.

Total fraud losses for orders above \$500 spiked at 10.32% in Q2 2017 and ended the year slightly lower at 9.32% in Q4 2017. False positives are partially responsible for these higher fraud losses as online department stores are more likely to reject suspicious orders for higher priced goods.

Another area of growing concern for these merchants is the rise of account takeover fraud which represented 16.3% of total fraud losses in Q4 2017.

Online grocery and department stores have been featured repeatedly in headline news since Whole Foods was acquired by Amazon. Every major brick-and-mortar department store and grocery chain has a strategy in place for the acquisition of online customers, and further consolidation appears imminent.

48%

Increase in total fraud losses from 2016 to 2017

16.3%

Account takeover fraud as a share of Total fraud losses in Q4 2017

Learning from the pace of digital adoption by department stores in the UK, early adopters appear to be faring better than those who took a wait-and-see approach – until it was too late and store closures ultimately led to chains shutting down entirely. On the flip side, successful chains are managing a careful balance of online deals and digital engagement with the advantage of proximity to their customers for in-store pick ups.⁷

In China, the world's largest online consumer market, the story is quite different. By 2020, an estimated 24% of all retail purchases will be made online.⁸

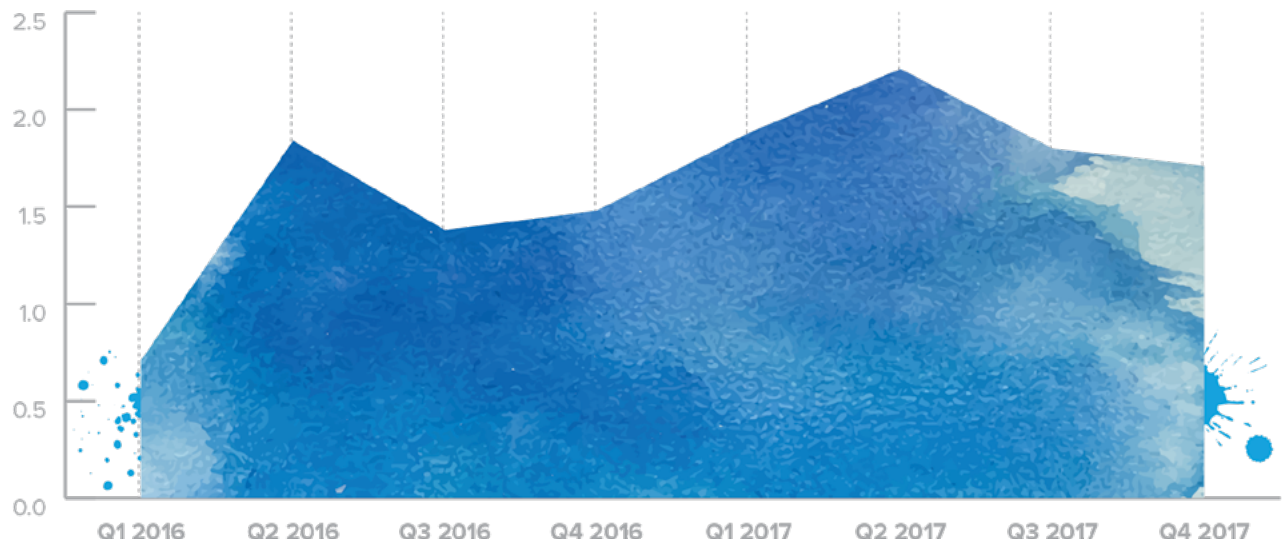
With the broad set of commerce, communications, media and payment services offered by China's 3 largest online marketplaces, Alibaba, Tencent and JD, online consumer spending appears unstoppable. Especially as consumers outside major cities begin adopting the online buying habits of their urban neighbors and peer-to-peer transactions continue to grow.

Going forward, online department stores and grocery sites need stronger methodologies for validating higher value purchases and better techniques for identifying account takeover fraud before shipping orders.

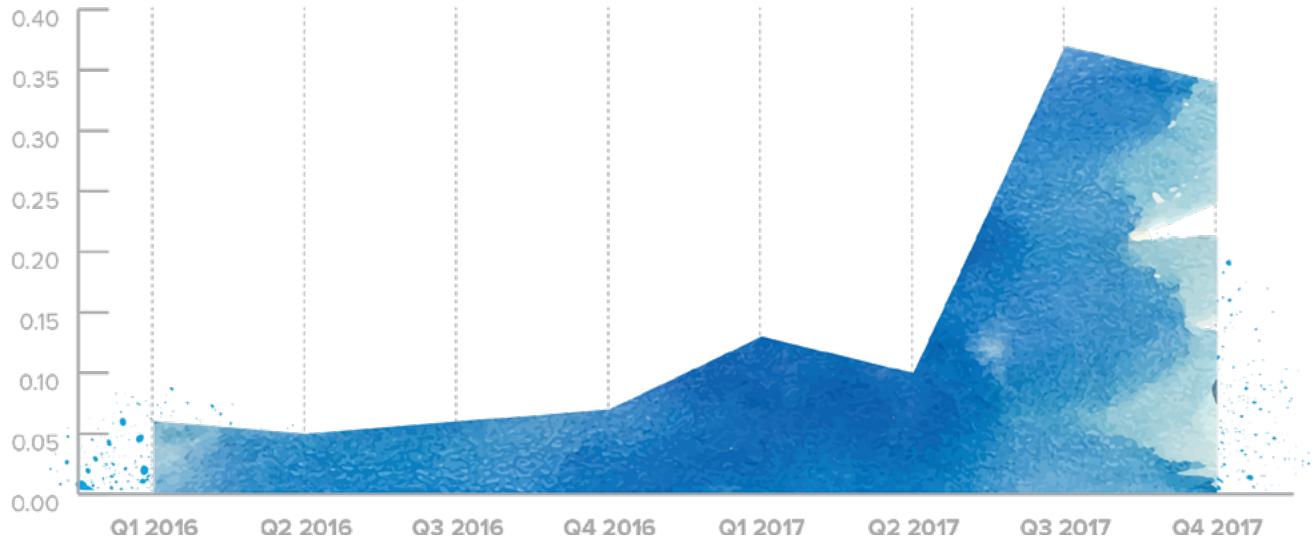
By 2020, an estimated 24%
of all retail purchases in
China will be made online.



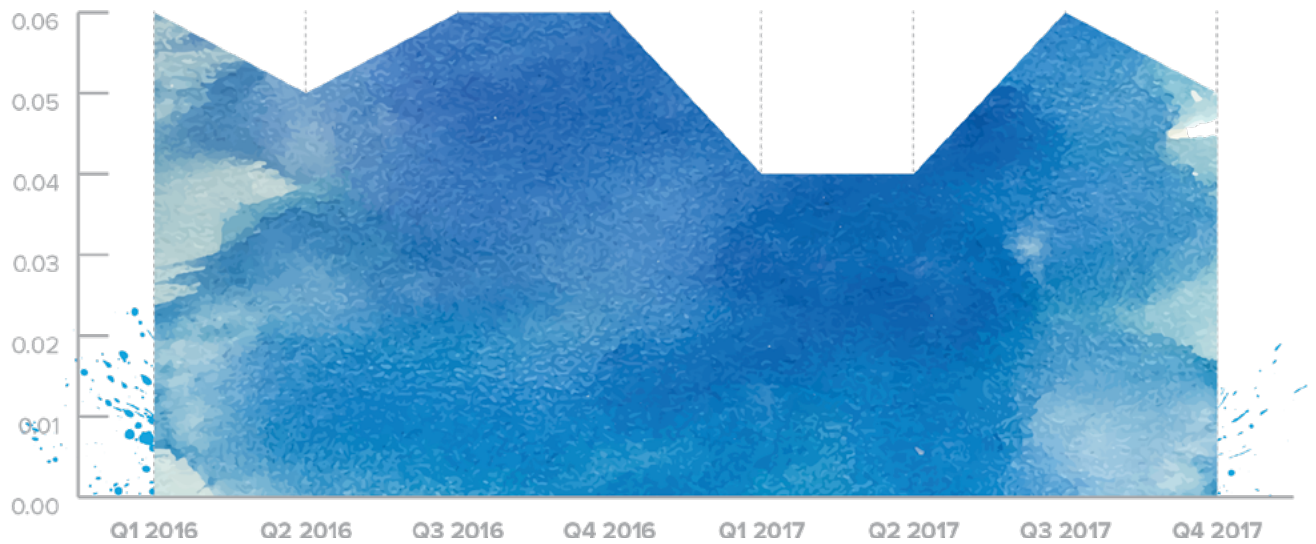
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)





FURNITURE, APPLIANCES & HOME IMPROVEMENT

Furniture, Appliances and Home Improvement includes all major purchases for the home or other properties, as well as purchases intended for the repair or improvement of such properties.

It's little surprise that these retailers were slow to move online. High-touch items that are big and bulky are not ideally suited to digital commerce. But consumers are changing and the industry is changing with them.

The furniture industry is still in transition to online sales. According to Furniture Today, 70 percent of furniture retailers have yet to try ecommerce, but things are changing.

Furniture is the second fastest growing segment of online retail in the United States. In fact, the only industry growing faster is online grocery. Furniture is projected to surpass even electronics in online sales by 2018, and higher-end retailers like Williams-

Sonoma and Restoration Hardware are investing substantial sums into their online businesses.

Brick-and-mortar stores that aren't going multichannel are losing market share to those that are, and Wayfair is the only publicly traded online pure-play furniture company that has achieved significant size and continued growth — 66 percent growth from 2015 to 2016.

Appliance sales are doing splendidly, benefitting from a replacement cycle thanks to the 2004 to 2006 boom in sales. Meanwhile, “aspirational” and forward-looking “smart” products are prompting consumers to buy new appliances. Online sales have seen double digit growth from 2015 onwards.

Internationally, Vietnam recorded the largest growth globally, as online retailers worked hard to solve delivery challenges. Online is an attractive option for consumers in both Vietnam and India because appliance prices cost 15 to 20 percent less online than at brick-and mortar shops. Meanwhile, in China, online sales of consumer appliances has grown 37 percent over the last five years.

For home improvement, ecommerce has also been a major success story. According to the NPD Group, almost every online category within home improvement saw double-digit increases, and the largest growth was seen in plumbing pipes and fittings, light bulbs and ceiling fans.

16%

Decrease in total fraud losses from 2016 to 2017



As merchants shift to selling online, they are quickly attacked by sophisticated fraudsters who know furniture, appliances and home improvement products can be sold over a longer duration than more perishable goods or those that can go out of style quickly.

However, these early losses are negated by the dramatic improvements merchants have made with their fraud prevention strategies.

By leveraging machine learning and fraud liability shift solutions, merchants have been able to reduce their losses from false positives, as consumer purchases across other (less risky) industries support a greater willingness to ship valuable, and sometimes bulky, orders to new customers.

This reduction in false positives is most visible in the reduction of stolen financial fraud losses, which dropped from 5.65% in Q1 2016 to 2.74% in Q4 2017.

One example, from a longtime Signifyd customer, helps illustrate how false positives in the home improvement industry can be avoided. For most merchants, shipping a bathtub to an empty lot seems like a terrible idea. However, for a family business that makes high end bathtubs in the U.S., this is a normal practice since the luxury home where the tub will be installed is in the process of either being built or significantly remodeled. Judging from the delivery location alone would be a mistake in their business, which is why they know their premium bathtubs are often shipped to seemingly unfitting addresses where a stunning home has yet to be built.

For furniture, appliances and home improvement merchants, building an omnichannel experience is key. Digital sites and apps are great for pricing and comparing features — and they might be sufficient for some consumers. But some will still want to sit on that couch or stick their head into that fridge before buying. This desire to touch and feel is leading retailers to pioneer the use of augmented reality to help online shoppers see what a piece would look like in their home. It's also encouraged some retailers to offer buy-online-pickup-in-store, or BOPIS, which is a huge sales channel for a store like Home Depot, for instance.

Leveraging the in-store experience also helps many retailers compete against Amazon, which is making its own push into furniture, appliances and home improvement. The online giant is reportedly building warehouses made to handle bulky household items and it's launching a custom furniture design service.

For home improvement, ecommerce has also been a major success story. According to the NPD Group, almost every online category within home improvement saw double-digit increases, and the largest growth was seen in plumbing pipes and fittings, light bulbs and ceiling fans.

SUCCESS STORY

STRUCTUBE

Founded in 1974, Structube originally sold tubular retail racking for clothing stores, hence the name “Structube”, derived from the French term “structures tubulaires”. But president and founder, Marcel Knafo, had a passion for furniture, opening the company’s first home furniture store in Montreal in 1980. Structube quickly became popular for its modern designs which were perfect for a new generation of customers shifting from larger homes to apartments and smaller houses.

The company has fueled its growth by broadening its portfolio with contemporary home furnishings for everyone, matched with lower prices that attract the largest segments of furniture buyers. “Lower prices provide greater affordability to more consumers in Canada and other markets,” explains Tony Trew, Structube’s director of marketing and ecommerce. “It’s more than an economic decision, it’s a commitment to be more inclusive, to serve more people through what we do.” Launching their ecommerce capabilities in 2015, Structube may have been late to the party but made quite the entrance. “We wanted to ensure our underlying infrastructure was in place before we launched, so we could offer our entire inventory and provide the same service our customers enjoy in our stores.” says Trew. “We underestimated the online demand for our products and we outsold our target on the very first day.”

On that first day of online sales, Structube also experienced their first fraud loss. Trew’s team was shocked by the volume and velocity of fraudulent orders they saw online. “Once we realized the orders were fraudulent, we tried to filter them out, but had limited success and ended up turning away legitimate customers.” says Trew. “I recall how we asked for photos of driver’s licenses, and how the very first one we received was obviously fake.” The team quickly realized manual efforts to thwart online fraudsters were damaging relationships with legitimate customers, and fraudsters quickly found ways around such measures anyway.

Given their rapid growth, Structube needed a fraud protection platform that could grow with them and assume liability for their fraud as their online sales grew and matured. “Signifyd was an easy choice. Protection was complete for us yet invisible to our customers, with no negative effect on conversion.” explains Trew. “We actually increased sales because we could accept more orders, since we no longer had to turn away or investigate legitimate customers we

weren’t sure about. All we needed was Signifyd’s approval to ship the order.” To streamline their process and eliminate manual order review, Structube integrated Signifyd directly in to their Magento console to enable faster delivery.



Guaranteed fraud protection isn’t the only innovation Structube has deployed to its award-winning website. Since its launch, the site has been a shining example of omnichannel shopping capabilities designed around the customer experience, earning it a “Commerce Marketer of the Year” nomination in 2017 from Magento, it’s ecommerce platform provider. Design and digital marketing expertise for the site were provided by Absolunet, including numerous features that enable growth while enhancing customer satisfaction. One such example is the tripling of orders almost overnight when the team introduced its “Ship to Store” feature to online buyers.

“

“Signifyd was an easy choice. Protection was complete for us yet invisible to our customers, with no negative effect on conversion.”

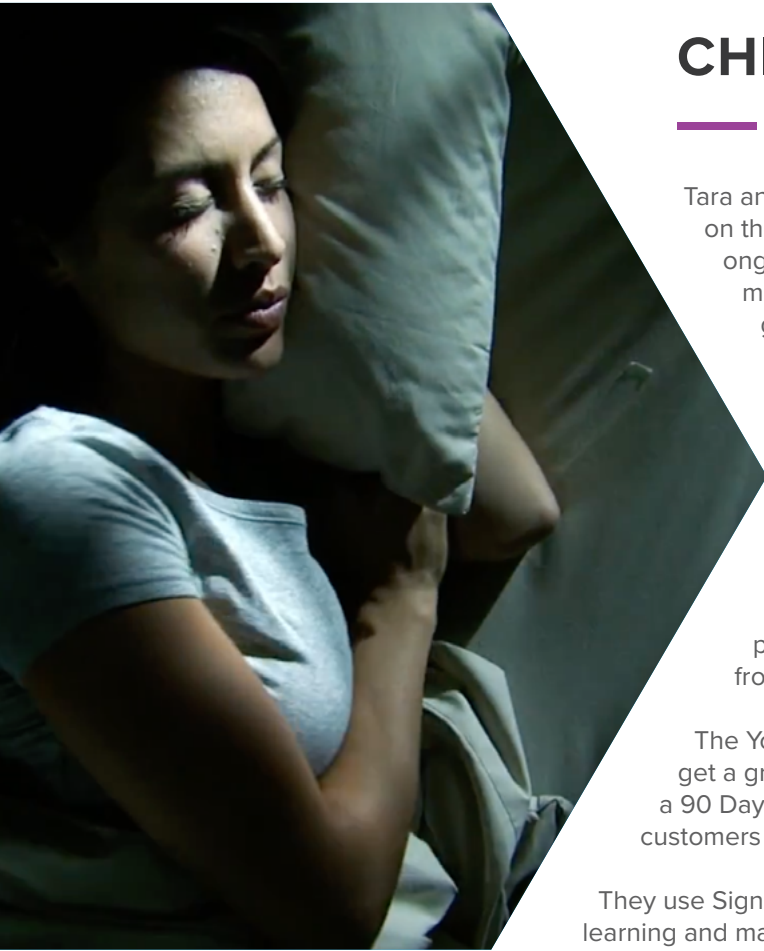
This serves as a reminder of why Structube has been successful all along – understanding and catering to their customer’s needs, instead of the company’s. “It’s important to ‘get out of the way’ of the sale. To make buying easy, even if what you need to do to accomplish this is extremely complicated.” says Trew.

Built on a tradition of accessibility, passion and innovation, Structube is positioned well for the immense growth opportunity ahead, both online and in-store. As more home furnishing customers make buying decisions online, the company is confident its comprehensive and convenient shopping options will continue to serve its existing and new customers at home and across the world.

[READ THE CASE STUDY](#)

SUCCESS STORY

CHILIPAD



Tara and Todd Youngblood, creators of the ChiliPad, decided early on they were going to design and produce products that create ongoing value for their customers. Products that got better, the more you used them, and relationships with customers that got stronger over time. These might seem like old-fashioned values, but to the Youngbloods they're not. They're simply a commitment to quality and a promise they make to their customers, a promise they back with a guarantee.

While to some it might sound dramatic, the ChiliPad has changed people's lives. They've been able to sleep through the whole night, without discomfort, without pain, without feeling too hot or too cold.

Just sleeping, peacefully. It sounds simple, but so many people are suffering from a lack of sleep and especially from the lack of quality sleep.

The Youngbloods put a lot of effort in to ensuring their customers get a great night's sleep. That's why they back the ChiliPad with a 90 Day Comfort Guarantee - ensuring this is the best sleep their customers have ever had.

They use Signifyd for the same reason. Signifyd's real-time machine learning and massive database of over 5,000 global merchants allows them to see more than 60% of their customers before they even place their first order. So Signifyd knows if each order is good or if it's fraud. And if Signifyd's wrong – which can happen – the complete cost of the chargeback is covered. Shipping, taxes, fees, everything. So it's like the loss never happened.

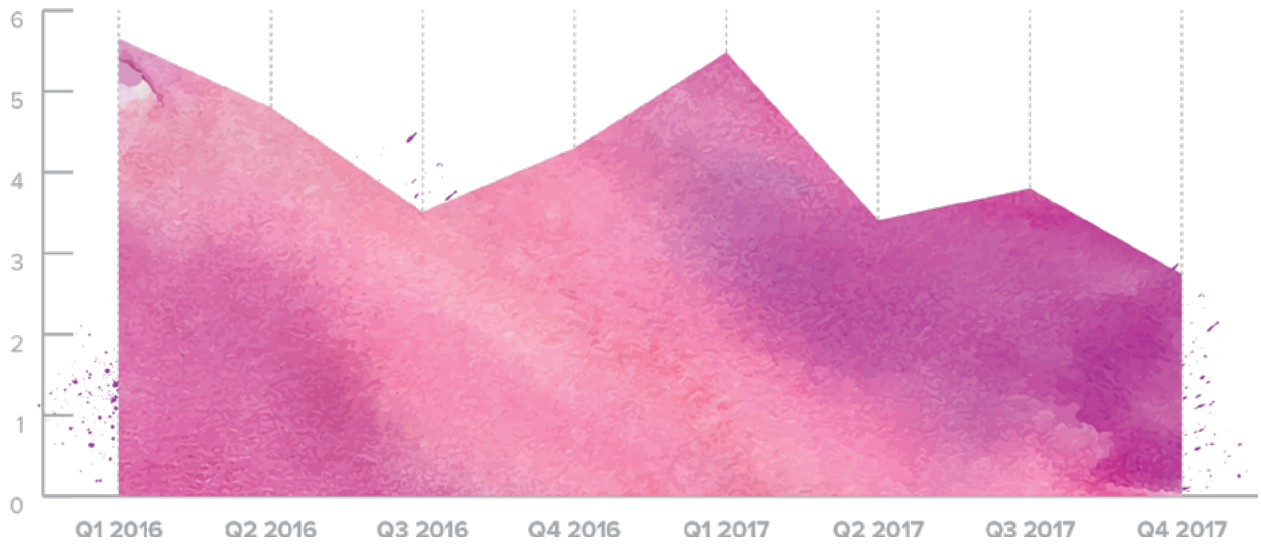
ChiliPad's relationship with Signifyd has grown over time, and they're even happier now than when they started. They're certainly not losing any sleep over fraud or chargebacks, and they can ship their products to customers faster because they don't have to review them first.

Together, Signifyd and the ChiliPad are helping customers around the world sleep better.

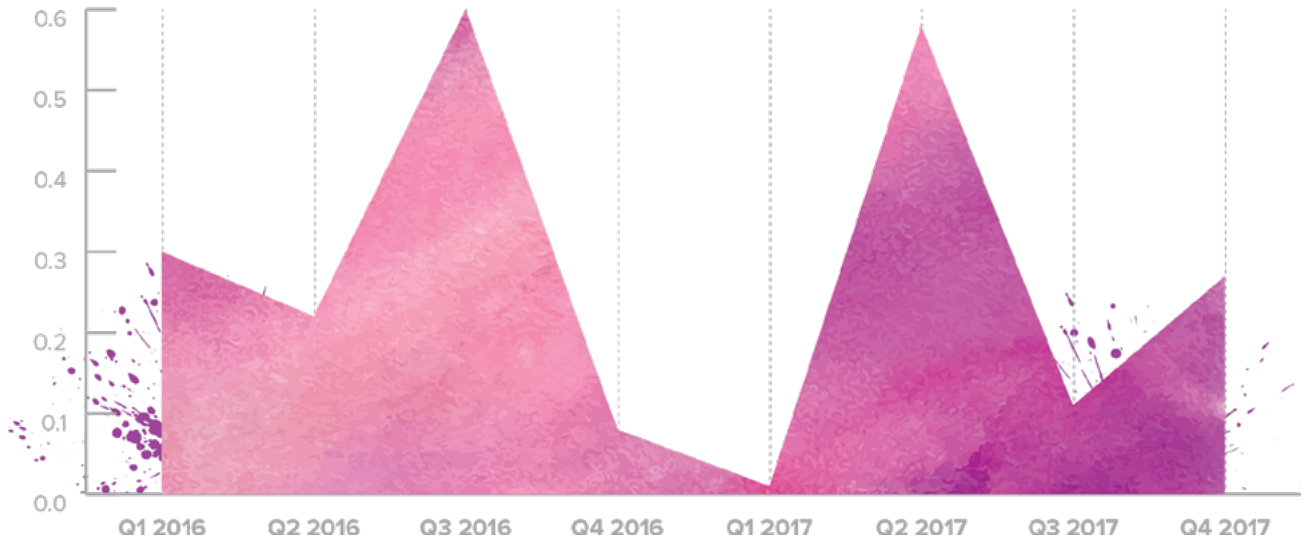
[WATCH THE VIDEO](#)



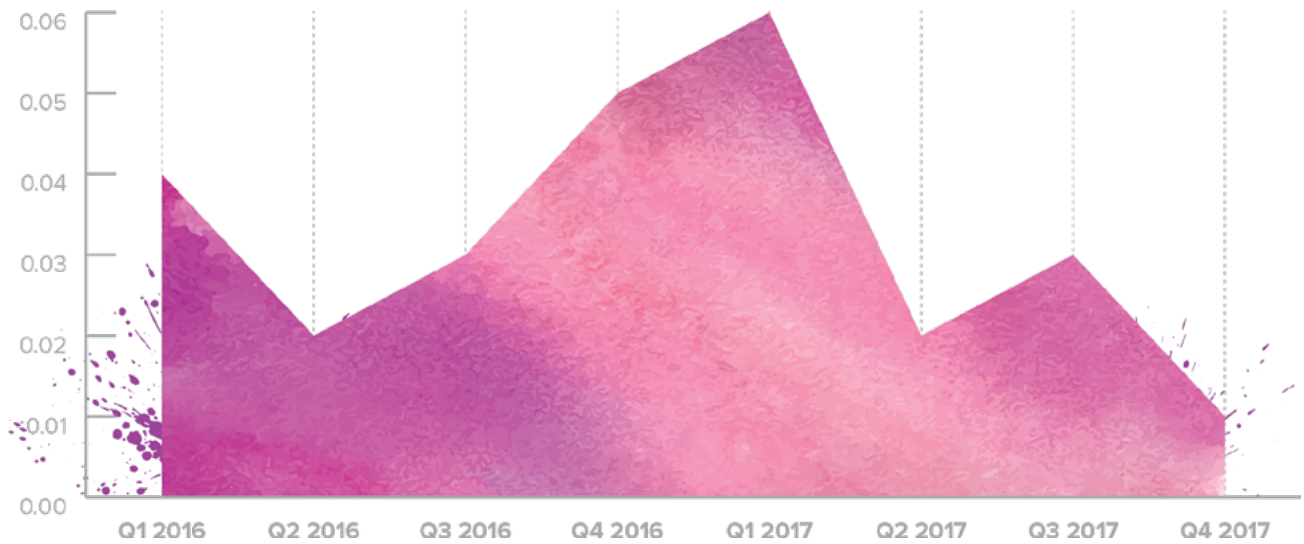
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)





HEALTH, LEISURE & HOBBIES

Health, Leisure and Hobbies (which include Outdoors, Fitness, Sporting Goods and Weapons) covers many disparate subcategories of merchants who sell items such as fishing equipment, swords, training weights and even board games.

The star of the sporting goods industry has been Dick's Sporting Goods, where ecommerce represented 11.9 percent of the company's total sales in 2016 and online sales have grown strong through 2017. Other sporting goods retailers are still catching up.

Meanwhile, the toy industry has seen significant retail changes over the past couple of years. After losing online market share to Amazon and Walmart for more than a decade, long-time giant Toys R Us filed for bankruptcy and plans to close its stores.

Toys R Us serves as an important lesson for brick-and-mortar retailers: Without aggressive online growth or a strong omnichannel strategy, it is only a matter of time before modern shoppers move their business to Amazon or other online stores.

Given the broad set of merchants covered in this category, online retailers in the health, leisure and hobby industries represent a great variety of product types, each with its own set of fraud challenges. Fraud losses vary significantly by merchant size and order value, but certain improvements can be seen across the board, as well as the emergence of certain threats.

Larger merchants have seen fraud losses fall faster than their smaller counterparts. This gain comes from a combination of factors.

68%

Increase in account takeover fraud from 2016 to 2017

24%

Decrease in stolen financial fraud from 2016 to 2017

First, larger merchants have moved faster to adopt better fraud identification technologies. In particular, machine learning has provided a notable advantage for merchants in this category with the ability to incorporate much more data than possible through manual review. Merchants in this category are often seeing customers for the first time as consumers shift towards buying these products online instead of in-store.

Second, larger merchants have shown a greater willingness to accept more orders, especially during peak seasons like the holidays. This has had a dramatic effect on reducing fraud losses from false positives as many legitimate customers in this category have orders that seem either suspicious or simply incomplete.

In particular, this strategy has reduced stolen financial fraud losses, which have come down from 9.04% at the start of 2016 to 3.39% by the end of 2017. With machine learning, merchants are accepting orders instead of canceling them, increasing revenues without a notable increase in fraud losses.

But account takeover losses have increased from only 0.09% in Q1 2016 to 0.44% in Q4 2017. Given the overall improvement in other fraud categories, account takeover fraud represented 11.3% of total fraud losses by the end of 2017.

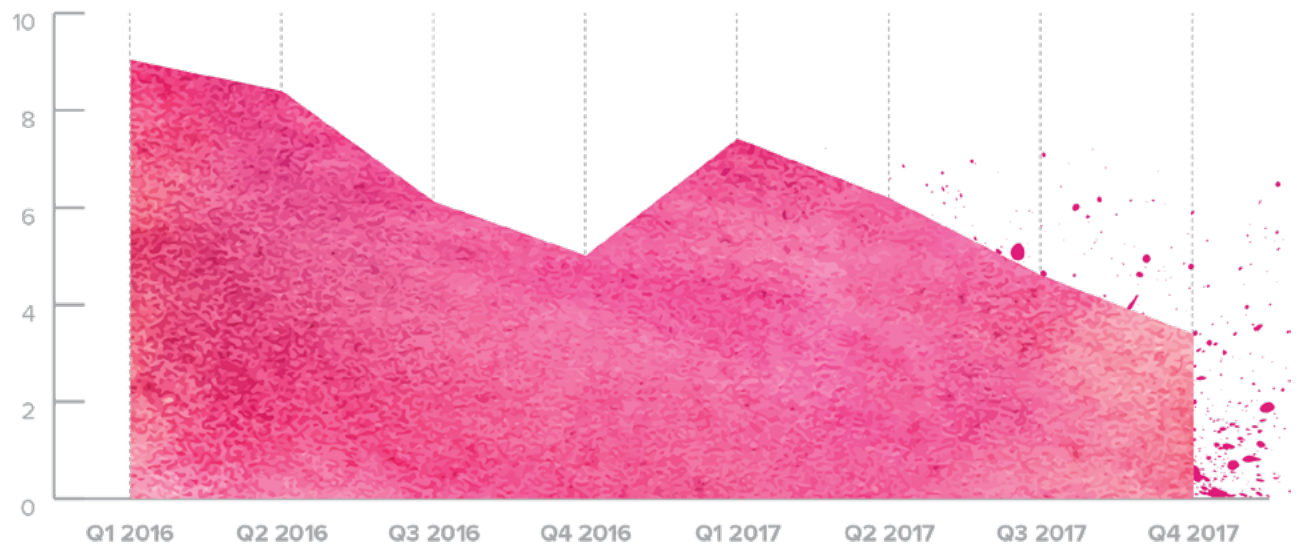
While fraud experts would expect to see account takeover losses rise for higher value orders, losses have risen across all order value ranges. This raises concerns for health, leisure and hobby merchants, since this type of fraud can be especially difficult to catch before orders are shipped.

For merchants with order values above \$500, fraud prevention techniques have provided less improvement than their counterparts with lower order values. While fraud losses have dropped for higher priced orders from 12.29% in Q1 2016 to 7.82% in Q4 2017, this represents less of a gain than the overall improvement of 57.7% across all health, leisure and hobby orders.

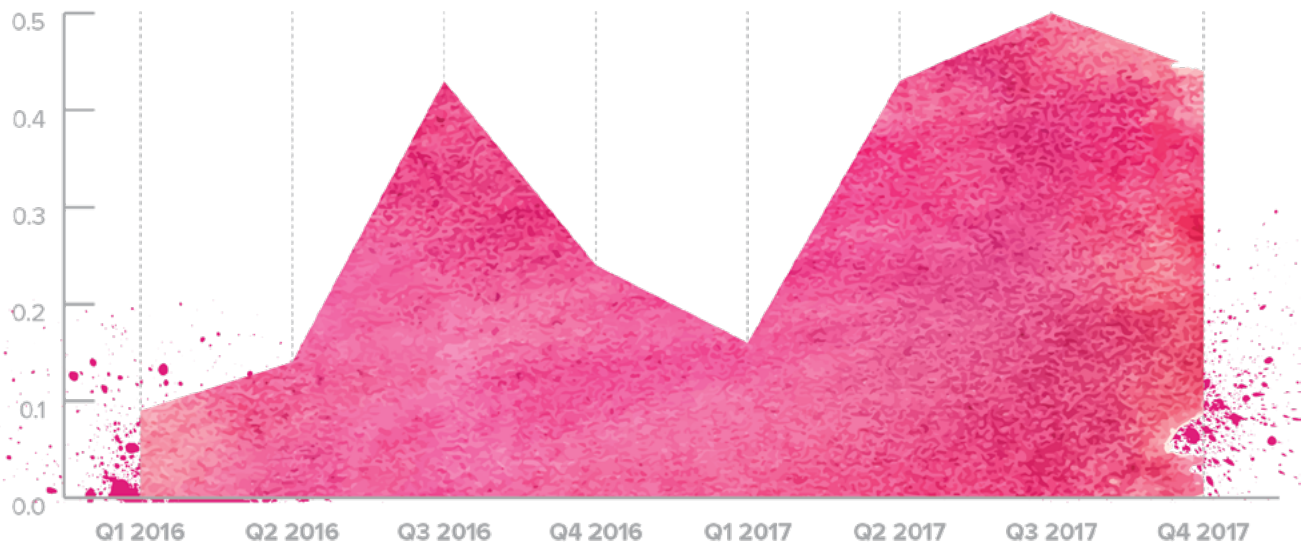
Larger merchants have
seen fraud losses fall
faster than their smaller
counterparts.



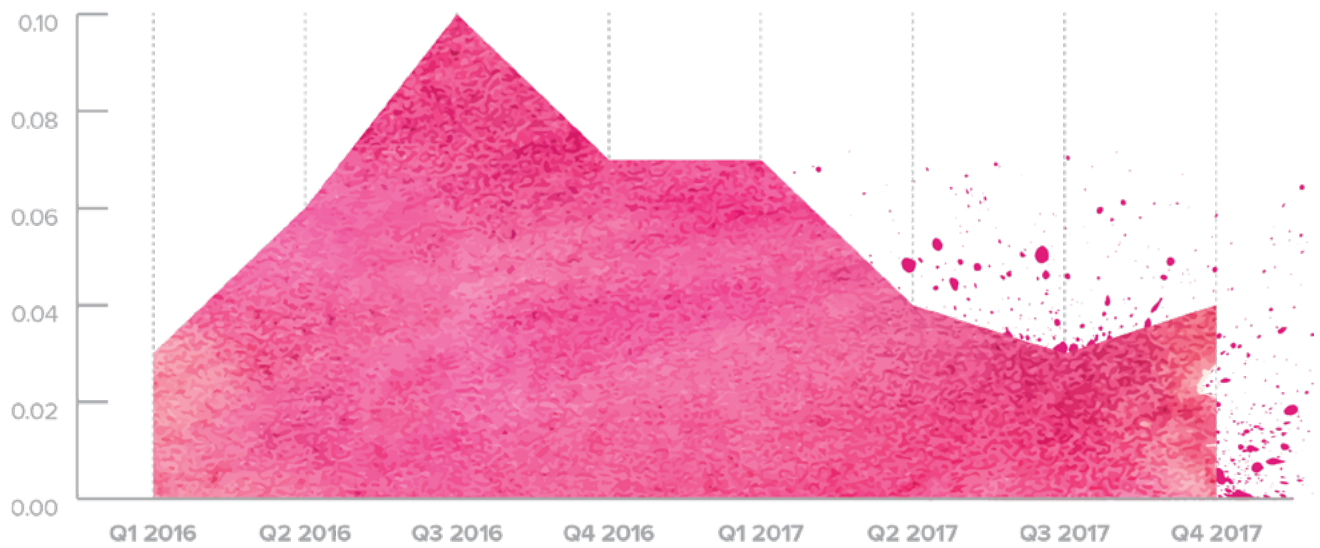
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)





JEWELRY & WATCHES

Jewelry and Watches includes designer and personalized jewelry of varying values, luxury watches, precious metals and coins for collectors.

The jewelry industry faced mixed fortunes as most traditional retailers had yet another year of lackluster sales while others got a boost from their online numbers. Larger brands, such as Tiffany & Co. and Signet — which owns Zales, Kay Jewelers and Jared the Galleria of Jewelry — saw a decline in both brick-and-mortar stores and online sales. De Beers pointed out a growing trend in which millennials are purchasing smaller diamonds, and saw an increase in self purchases for diamond jewelry.

McKinsey concluded that the portion of jewelry sales conducted online will double between 2014 and 2020.⁹ But even then, online sales will make up only 10% of jewelry sales. Digital's importance will grow immensely

195%

Increase in account takeover fraud from 2016 to 2017

in the sale of precious goods as consumers research and compare prices online and turn to social media to help with buying decisions.

Luxury watches faced similar challenges. The online resale market for Swiss watches continues to grow, though. After years of growth built upon supplying wholesalers and retailers, but without growing sales to consumers, luxury watchmakers may be forced to supply online resale sites selling genuine merchandise at steep discounts. Whenever possible, manufacturers will require sites to remove newer models from sales and ensure they're not offered at reduced discounts.

For its part, the luxury watch sector is launching online-only sales of some timepieces, while industry executives tell researchers that they see online authorized dealers as their most important revenue channel.

While total fraud losses for this category haven't changed greatly from 11.76% in Q1 2016 to 10.58% in Q4 2017, the mix of where those losses are coming from has been of great concern to jewelry and luxury watch merchants.

Despite the fear of chargebacks, merchants in this category have done well to accept more orders over the past couple of years, bringing down their false positive losses from stolen financial fraud from a high of 14.23% in Q2 2017 to a more manageable 8.78% in Q4 2017.

However, account takeover fraud has hit this category hard, rising from 0.46% in Q1 2016 to a whopping 1.74% in Q4 2017.

As merchants change how they're selling, they may also change where they're selling as McKinsey sees global consolidation coming with local jewelers becoming part of bigger retail organizations.

Luxury watch sellers are seeing the U.S. appetite for their products moderating. Meantime, consumers — especially millennials — in the UK, Italy and China have indicated in surveys that they're anxious to own luxury watches and that they view smart watches as a poor substitute.

While the jewelry and luxury watch industries are highly cyclical, fraud experts may be surprised to note the holiday peak season did not see a corresponding increase in fraud losses, with total fraud at an all-time low of 9.02% in Q4 2016 and a bit higher at 10.58% in Q4 2017.

After many years of resisting digital transformation, merchants in this category are adopting machine learning and fraud liability shift options, due in part to pressure from younger disruptors born in the cloud without physical stores and large operating costs.

For merchants willing to make the change the upside has been significant.

Most U.S.-based merchants don't jump at the opportunity to ship gold and diamond jewelry to Nigeria, simply because they lack knowledge

of the local market and consumers. However, a jeweler from New York's diamond district has been doing just that for some time now, with Signifyd guaranteeing every one of their approved orders. Nigeria offers a massive and growing consumer economy, with most major luxury brands already present in Lagos, Nigeria's largest city and one of the world's fastest growing metropolises.

Other jewelers are prospering by producing new designs and lines of jewelry targeted at urban buyers who wish to be "blinged out" like their favorite rap artists. Buyers for this type of jewelry are often located in neighborhoods where most merchants are wary to ship orders.

Such market opportunities eluded jewelry and luxury watch merchants for years due to fears of ecommerce fraud and cash losses from excessive chargebacks.

SUCCESS STORY

CROWN & CALIBER

For Crown & Caliber, every transaction is personal. Every timepiece they receive has a story and needs to be cared for to bring it back to its original self. Their certified experts evaluate every part of every watch to ensure every component is genuine. They know how each piece inside relates to every other piece and how they work together.

Crown & Caliber receives timepieces that are difficult to find from all over the world and they want to help their customers make the right choice. Signifyd helps Crown & Caliber understand the person behind every purchase and every payment. Signifyd processes thousands of points of data every minute so they can determine the customer's credibility with absolute certainty.

Signifyd has likely seen this customer and their buying activity before whereas Crown & Caliber is seeing it for the first time. Signifyd's financial guarantee against fraud and chargebacks allows Crown & Caliber to ship to customers they otherwise wouldn't have felt comfortable shipping to on their own.

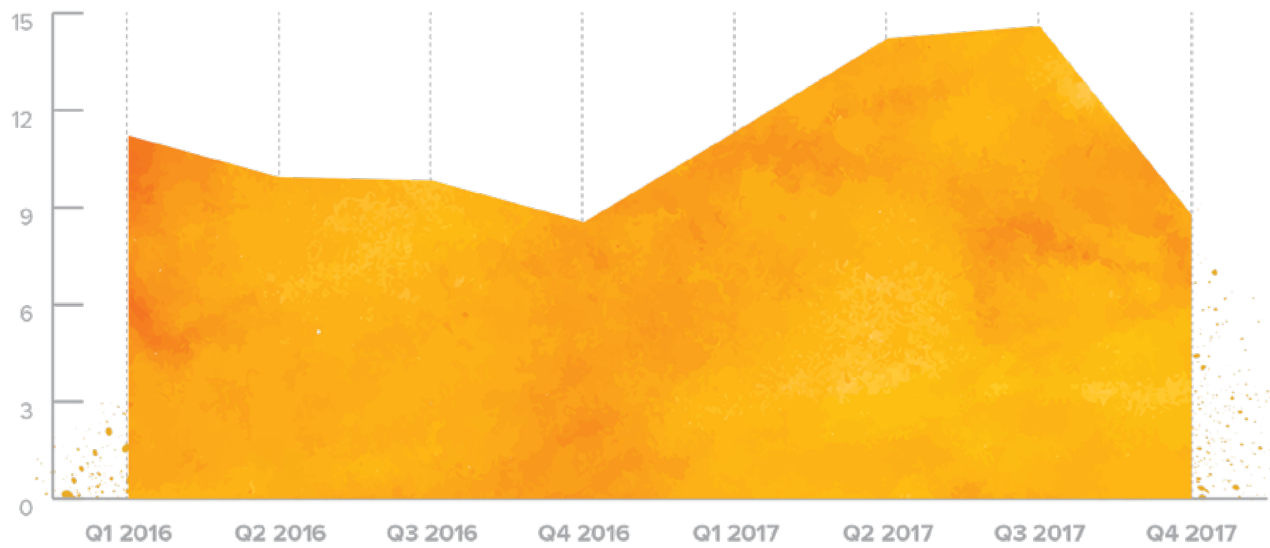
Crown & Caliber needs to understand every single timepiece, every customer and every transaction, and because Signifyd has them covered from a chargeback standpoint, it allows them to focus on what they're good at.

Which allows them to keep their business personal.

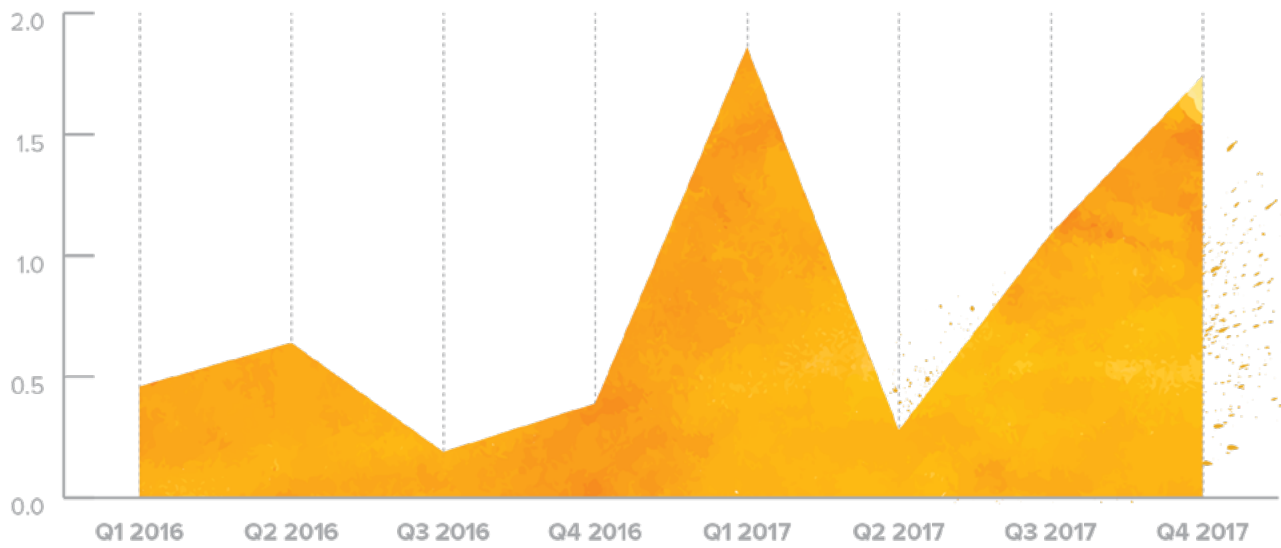
WATCH THE VIDEO



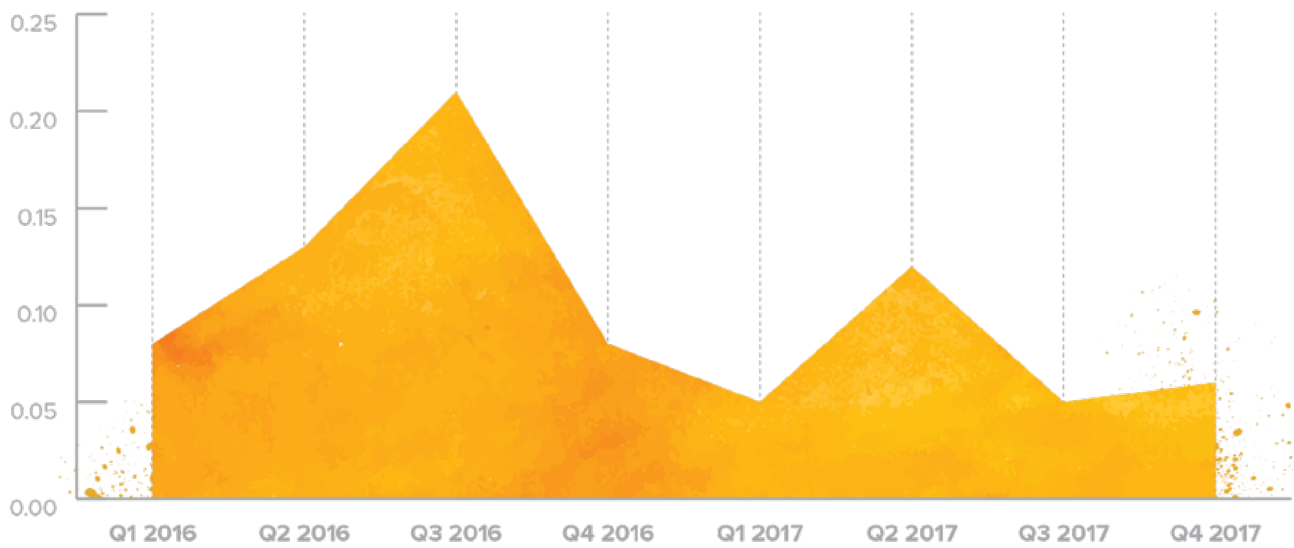
STOLEN FINANCIAL (%)



ACCOUNT TAKEOVER (%)



FRIENDLY FRAUD (%)



About Signifyd

Signifyd uses big data, machine learning and human intelligence to protect more than 5,000 ecommerce merchants from fraud. Its 100 percent financial guarantee against fraud and chargebacks on every approved order effectively shifts the liability for fraud away from ecommerce merchants. Signifyd is in use by multiple companies on the Fortune 1000 and Internet Retailer Top 500 lists. Signifyd is headquartered in San Jose, CA.

Why Guaranteed Fraud Protection?

Most fraud prevention experts know the dilemma they face at an individual merchant with limited data and transactions. They may never actually know if the orders they rejected were in fact legitimate as they may not see that consumer again for some time, or ever - if they were a legitimate customer who has taken their purchases elsewhere.

Signifyd is in a position to accept more orders than individual merchants since we leverage data across our global network of merchants, and Signifyd is only paid for approved orders. Therefore, Signifyd is inclined to approve every order, if possible, since we've already invested in its data and analysis. We would actually lose money by rejecting orders. For these reasons, some of Signifyd's merchants enjoy a 100% approval rate.

As a global real-time machine learning platform, rejecting legitimate orders would deteriorate the performance of Signifyd's model, as we would introduce a bias since these rejections are without certainty. Since we carry 100% financial liability for our merchant's ecommerce fraud losses, we're able to bear these losses to accept orders that should be legitimate but turn out, in fact, to be fraudulent. While this may seem costly, it improves our model's accuracy tremendously, so we can continue to accept every possible order by bearing this ongoing cost.

Key Partners



Authorize.Net



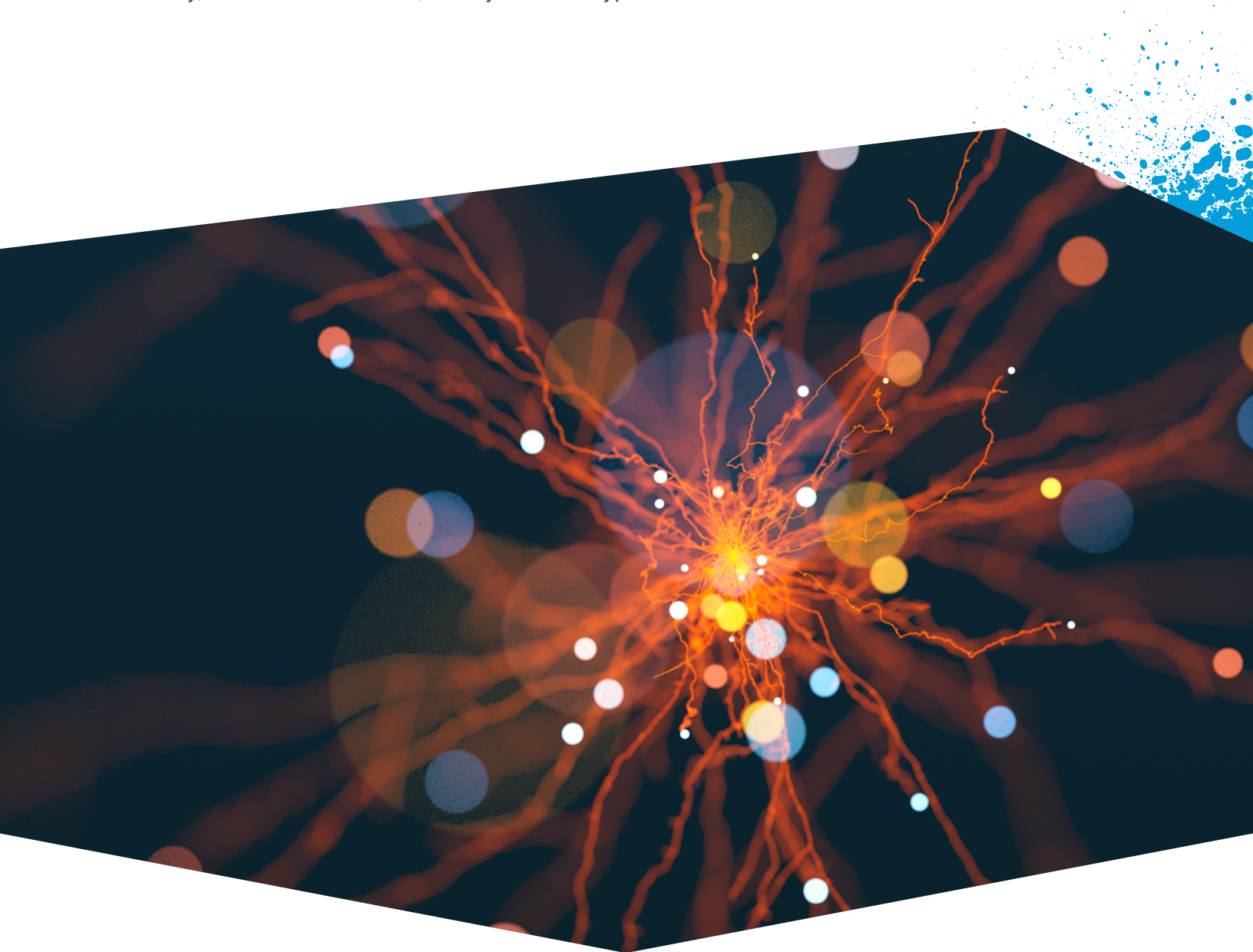
Key Awards



Methodology

The Ecommerce Fraud Index measures the growth (or decline) of attempted fraud on ecommerce merchant websites. Attempted fraud is defined as all sales transactions identified as potential fraud, including both successful and unsuccessful fraud attempts.

We base our analysis on data we have collected on fraudulent chargebacks, and the total amount of ecommerce sales in the market since Q1 2016. The data is segmented based on the merchant's industry, the value of the order, and by the fraud type.



Disclaimer



The Ecommerce Fraud Index may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to date, SIGNIFYD 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. SIGNIFYD 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. SIGNIFYD 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.

SIGNIFYD 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 SIGNIFYD AND ITS 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 Signifyd is the property of Signifyd and cannot be reproduced without its prior written permission.



Footnotes:

Alcohol, Tobacco & Cannabis

1. <https://data.drizly.com/ecommerce-consumer/>
2. <http://www.tobaccoreporter.com/2018/02/bat-volumes-increased/>

Apparel

3. https://cdn.businessoffashion.com/reports/The_State_of_Fashion_2018_v2.pdf

Consumer Electronics

4. https://www.mckinsey.com/~media/mckinsey/dotcom/client_service/Consumer%20Packaged%20Goods/PDFs/Trends%20that%20will%20Shape%20the%20Consumer%20Goods%20Industry.ashx
5. <https://www.prnewswire.com/news-releases/global-consumer-electronics-market-to-expand-at-40-cagr-by-2022-owing-to-growth-of-online-retail-industry-transparency-market-research-567217721.html>
6. <https://technology.ihs.com/549694>

Department Stores

7. <https://www.verdict.co.uk/john-lewis-department-stores-online-retailers/>
8. <https://www.economist.com/news/special-report/21730544-alibaba-demonstrates-benefits-breadth-online-retail-booming-china>

Jewelry & watches

9. <https://www.mckinsey.com/industries/retail/our-insights/a-multifaceted-future-the-jewelry-industry-in-2020>