Don’t Forget Your Customers When it Comes to Fraud — They’ll Remember You

FINDINGS FROM SIGNIFYD’S 2019 CUSTOMER EXPERIENCE INDEX

Findings from Signifyd's 2019 Customer Experience Index

When the hotel chain that owns Westin, Sheraton and W Hotels announced in November that it had been hacked and that the personal information of half a billion consumers had been released into the wild, it was clear the Marriott organization had a problem.

Members of Marriott's Starwood loyalty program — who had lost control of personal information including names, phone numbers, email addresses, passport numbers, dates of birth, and credit card numbers — had a problem, too.

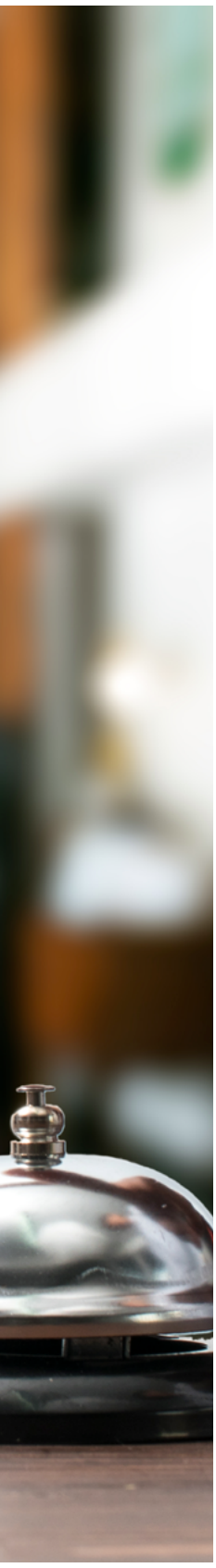
But the damage didn't stop there. You know who else had a problem?

Online retailers.

We live in the era of the data breach. The Breach Level Index now says that more than 13.4 billion data records have been lost since 2013. Last summer, the world was setting a pace of 7 million records compromised every day, according to Varonis. What do you want to bet that number is higher today?

Among the things we've learned, living in our new and disconcerting data-deluged world, is that gigantic data breaches come with collateral damage.

For retailers, that damage is both real and perceived — and sometimes perception can be as important as reality.



Signifyd recently conducted a consumer survey to gauge shoppers' attitudes toward ecommerce fraud and data security.

At the risk of giving away the story's ending, what we found is that a significant number of consumers — 62.2 percent — say they either aren't sure whether their personal information is is safe with retailers or that they are sure it is not safe.

Consumers are familiar with the problem of online fraud — unfortunately two-fifths of consumers are intimately familiar with the problem, having been personally victimized, according to Signifyd's survey. And, of particular note to retailers, a majority of consumers blame the retailer for the false credit charges, no matter who is actually at fault.

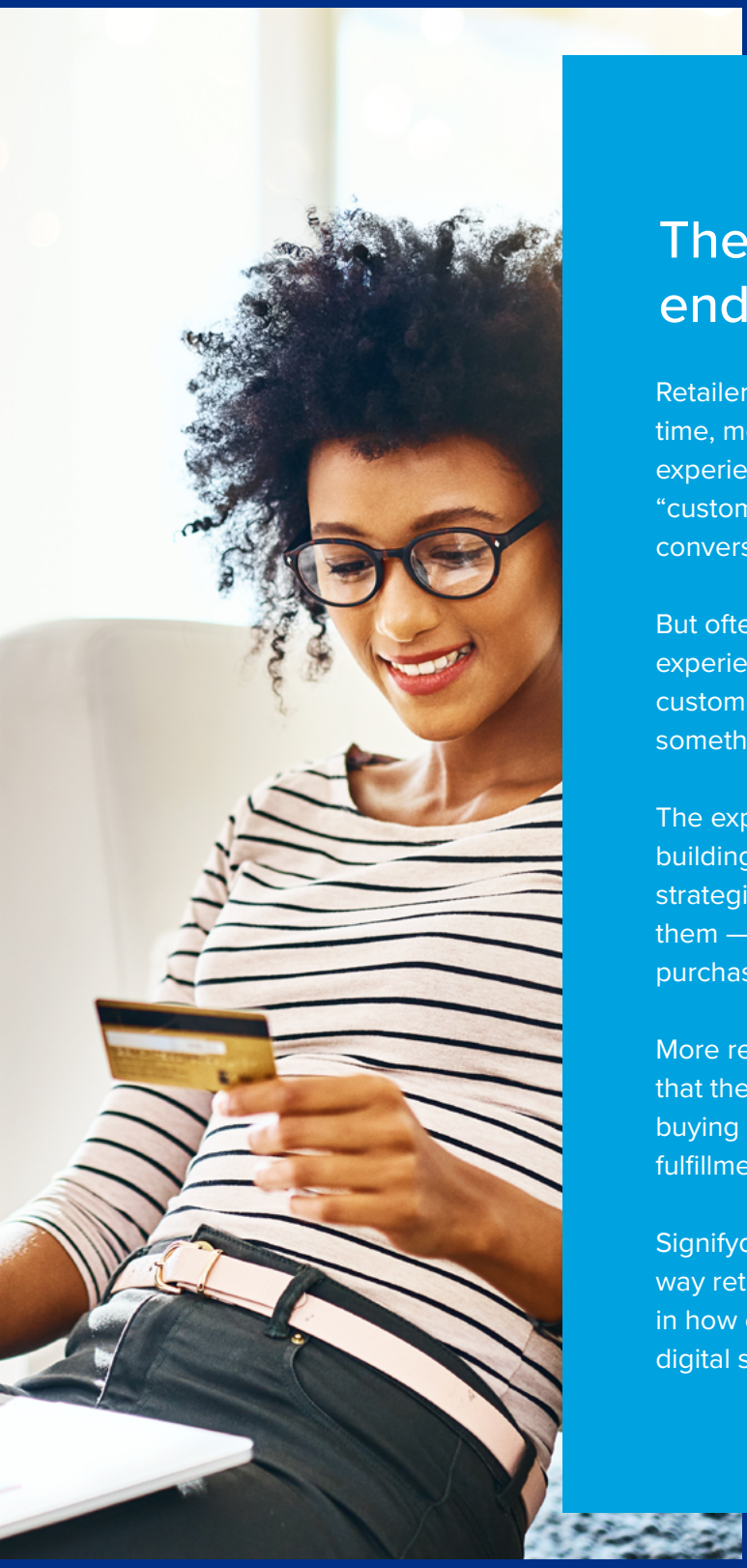
This ebook will break down the findings of Signifyd's 2019 Customer Experience Index, a survey conducted by polling firm Survata over the busiest shopping weekend of the year — Black Friday through Cyber Monday. We'll examine the responses of 2,0000 consumers and explore the implications for retailers of their high expectations when it comes to fraud and security.

Consumers exuded confidence during the 2018 holiday shopping period, particularly in the United States, where overall retail sales were up year-over-year by 5.1 percent, according to Mastercard SpendingPulse. The numbers were not as good in the United Kingdom, but the UK still held steady with last year's season.

Ecommerce spending in the United States rose by a more impressive 18.3 percent and buy-online-pick-up-in-store increased by 47 percent, according to Adobe Analytics, as shoppers appeared to revel in their power to buy anytime, buy anywhere.

But beneath the surface, shoppers' mood might not have been so rosy. The Signifyd/Survata survey paints a picture of consumers who have grown weary of constant data breaches and who remain anxious about the security of their own personal data.

Furthermore, they are implicitly saying that they are looking to retailers to find ways to reassure them when it comes to the information they share online in order to make purchases.



The customer experience hardly ends at the buy button

Retailers since the dawn of the digital age have poured time, money and angst into creating a powerful customer experience for online shoppers. You can't avoid the phrase "customer experience" at industry trade shows or in industry conversation.

But often, what people mean when they talk about customer experience is the experience a retailer builds to attract customers to a digital site and to inspire them to buy something.

The experience is about merchandising and marketing, about building powerful site search and hatching personalization strategies that make a customer feel like a merchant knows them — all of which encourages consumers to make a purchase.

More recently, retailers have started to embrace the notion that the customer experience stretches through the entire buying process — from discovery to checkout and purchase to fulfillment to post-purchase customer support.

Signifyd's Customer Experience Index makes it clear that the way retailers manage fraud and data security plays a key role in how customers perceive their experiences on a retailer's digital sites.

Why retailers should shudder at the news of any data breach

When retailers hear about a data breach, such as the Marriott breach or Facebook or Google or Experian, they might be tempted to breathe a sigh of relief. After all, they dodged the data breach bullet.

But unfortunately, they should be nearly as concerned as if they had been the victim themselves. Data breaches, you see, no matter the immediate victim, provide the source material for digital crime waves launched by fraud rings that prey on ecommerce enterprises.

The names, credit card numbers, email addresses, social security numbers, passport numbers, dates of birth, drivers license numbers and more find their way very quickly to the Dark Web where they are sold with Amazon ease.

The stolen credentials open up all sorts of possibilities for fraudsters. They can use credit card numbers to make purchases until the legitimate consumer catches on. They can use personal information like names and email addresses to create phishing schemes that trick consumer into providing passwords and additional personal information.

They can steal whole identities and take over financial and retail accounts, charging purchases with little chance of being detected in the short-term.

Consumers are inconvenienced, frustrated and sometimes traumatized by online fraud. Retailers certainly share the frustration and they also take the hit — a hit that is exceptionally painful for an industry that generally operates on thin profit margins.

The direct cost of online fraud is nearly 1 percent. The total cost for retailers is 5.4 percent, when you factor in the costs of reviewing orders to detect fraud and the lost revenue caused by declining legitimate orders because of the fear of fraud.

But a bigger — if less talked about — cost is the damage fraud does to the relationship between a retailer and a customer. As we said earlier, consumers blame retailers when fraudulent charges show up on their credit accounts.

And while that seems unfair from a retailer's perspective, given the proliferation, sophistication and persistence of fraud rings, it's hard to blame consumers for feeling let down. They expect retailers to be vigilant, to look out for them.

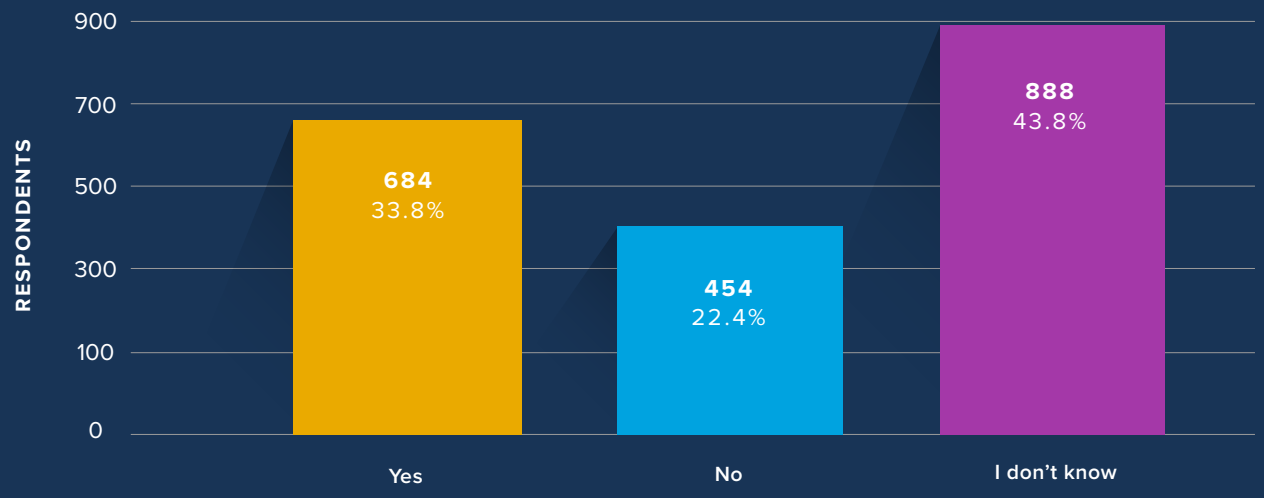
After all, they are loyal customers, don't they deserve some loyalty in return?

Consumers are jaded when it comes to data security

With millions of records being plundered every day — 56 every second, Varonis says — consumers have become slightly jaded, if no less alarmed about the data risk they face.

Signifyd's consumer survey found that 33.8 percent of consumers assume their personal data was among the data stolen in recent breaches. The number doesn't sound horrible until you consider that another 43.8 percent say they don't know if their data was pilfered — meaning they at least worry that their information could have been compromised.

Do you think any of your personal information (data) could have been included in any of the recent consumer data breaches?



Consumers' lack of confidence in businesses' data practices extends to retailers and retail accounts. More than a quarter of those surveyed said they didn't think their account information was safe with retailers.

Specifically, respondents said they thought the email addresses and passwords they'd stored with retailers might make their way to the Dark Web.

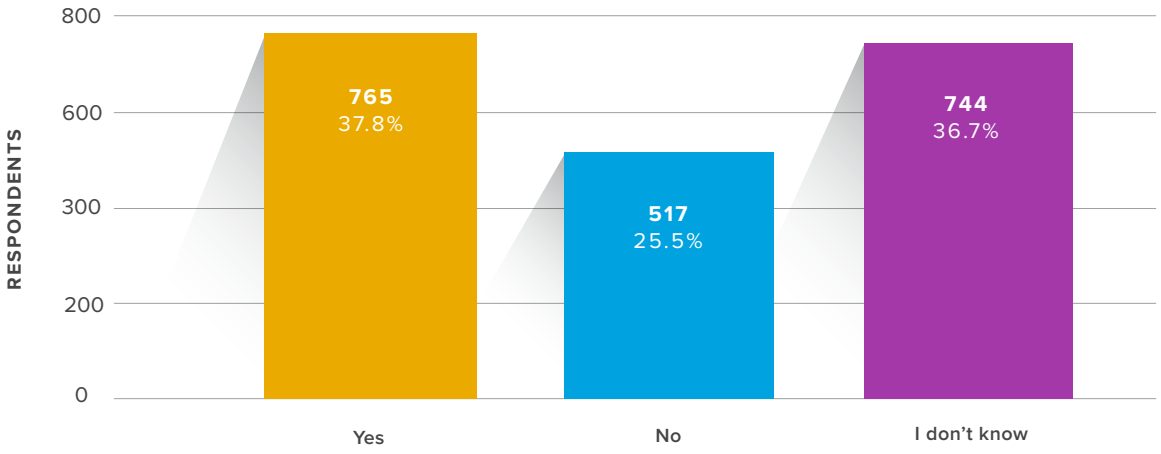
It's possible that consumers' outlook on retail security is colored by what's been a dramatic increase in a particularly insidious form of fraud attack: account takeover.

Account takeover happens when a fraudster or fraud rings obtain a consumer's account login credentials. Fraudsters come up with the credentials either through the kind of hacking that victimized Starwood or through phishing attacks or other social engineering schemes.

Once fraudsters have login credentials, they can change the password, effectively locking the rightful owner out of the account. They can also change shipping addresses, making it easier to obtain the fraudulently ordered goods. In fact, they can change any aspect of the account they choose.

Only 38 percent of surveyed consumers believed the personal information they share with retailers was safe from those who sought to use it for financial advantage. More than 25 percent said it was not safe, while the remaining 36.7 percent said they weren't sure it if was safe.

Do you think all of your login or other account information (email, password, etc.) across your retailer accounts is secure (i.e. not available on the dark web)?



Given consumer sentiment, it may come as no surprise that not even half of those surveyed felt they were safe from fraud as they went about conducting their holiday season shopping. In fact, 33.1 percent felt they were somewhat unsafe when it came to fraud, while 7.7 percent believed they were very unsafe.

Why do consumers feel the way they do about online fraud?

No question, consumers' general concern about the safety of their data and the possibility of becoming a fraud victim stems from frequent and prominent stories about data breaches.

In the past year alone, besides the Marriott breach, breaches at Facebook, British Airways, Orbitz, T-Mobile, Google and more have all been in the news.

Although a data breach is a different crime from making fraudulent charges on a consumer's account, the breaches, as we've explained, are often the source of the personally identifiable information that fuels fraud attacks.

Not to mention that the breaches add to consumers' sense that it's open season on data and identity, which feeds into a sense of gloom.

In fact, and this may be good news, not even half of those surveyed by Signifyd and Survata said they'd actually been the victim of online fraud. They survey found that 43.6 percent of consumers had been charged for a retail purchase they did not make.

There is something to be said for that number coming in at under 50 percent. On the other hand, if two out of five customers are seeing bogus charges on their credit cards or retail accounts, you could argue that retail has a problem on its hands.

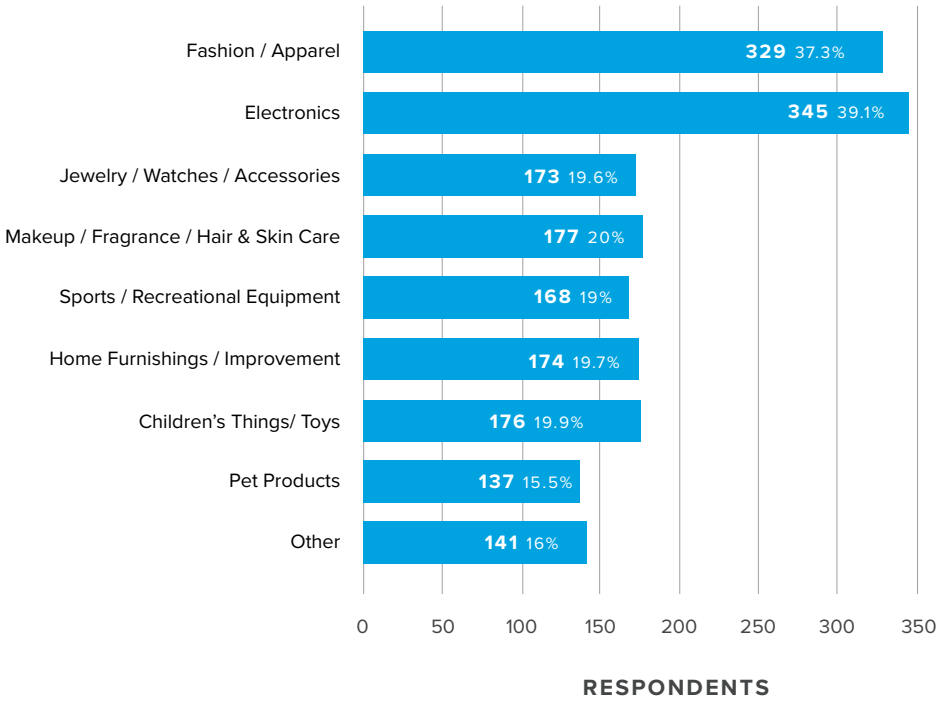
Actually, there is little need to argue. At a time when retailers are intently focused on providing a great customer experience, it can hardly be acceptable for nearly 44 percent of customers to endure fraudulent charges on their credit accounts.

Consumers don’t forgive — or forget — fraudulent charges

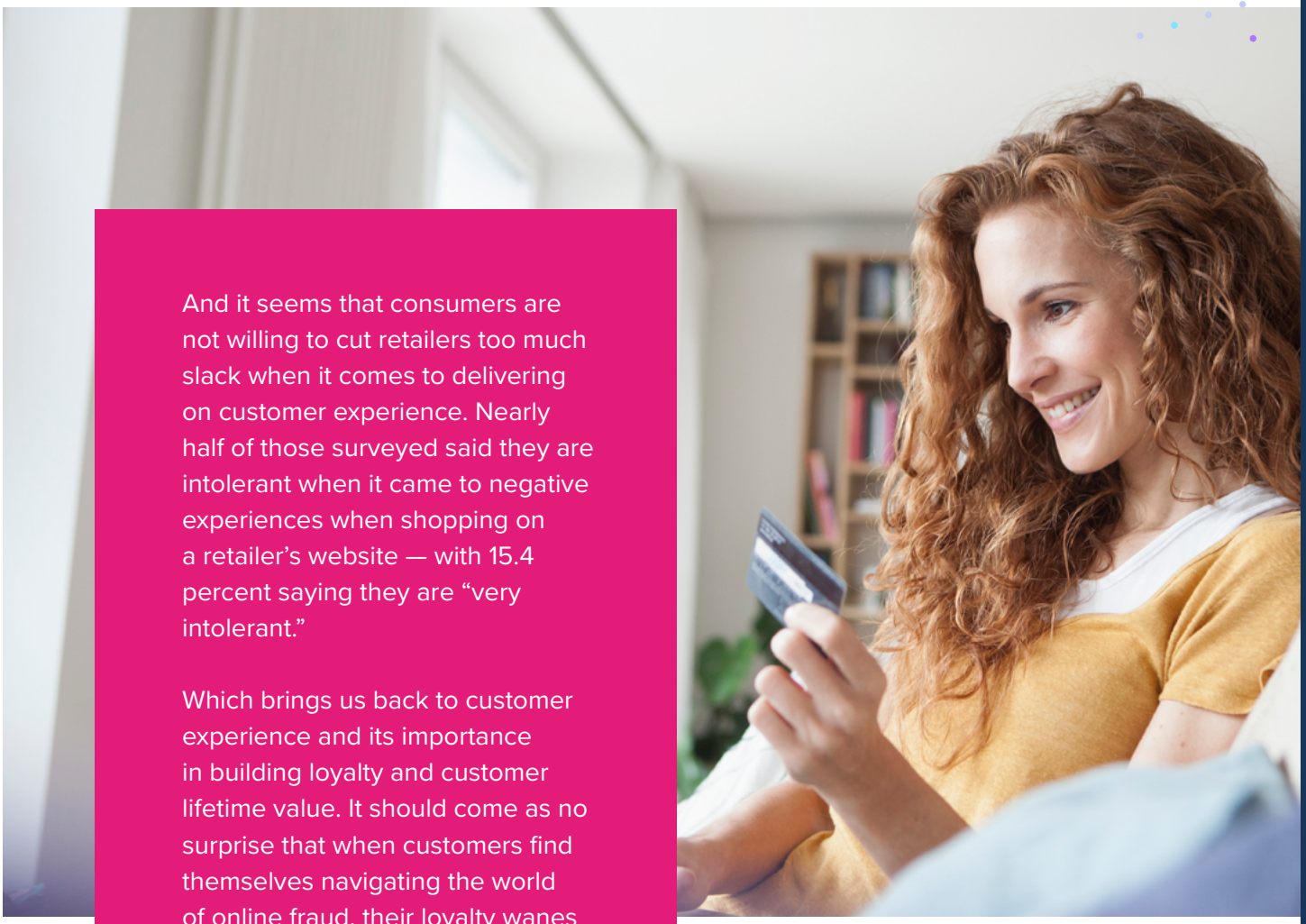
Unfortunately for retailers, being victimized is not an experience that consumers easily dismiss. The Signifyd/Survata survey found that customers remember the charges and what verticals they were shopping in when they encountered fraud.

Specifically, electronics and fashion led the way, with 39.1 percent of consumers saying they’d received a fraudulent charge from an electronics seller, while 37.3 percent said they were shopping for apparel or fashion items when fraud struck.

What type of retailer/product was it?



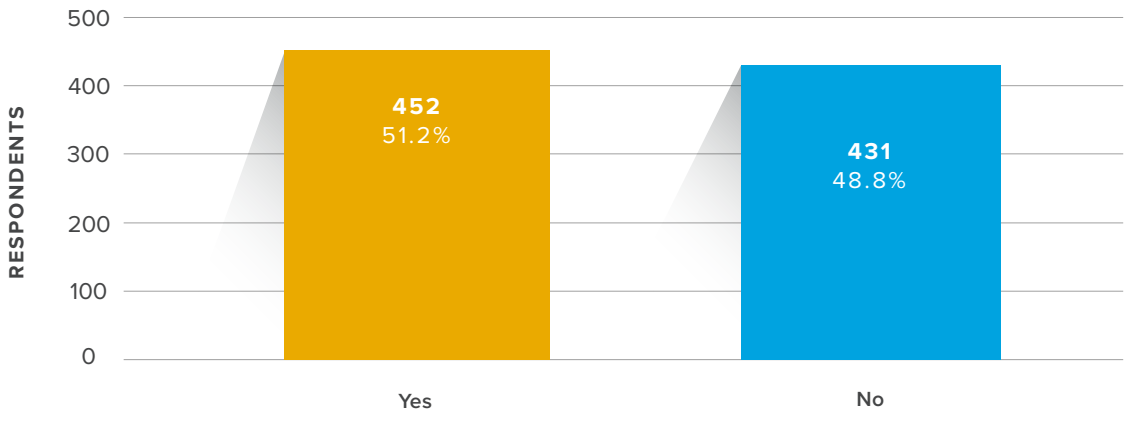
Most importantly for retailers, shoppers hold retailers responsible for fraudulent charges that show up on their accounts. More than half — 51.2 percent — of those who had encountered a charge for something they did not purchase, said the experience negatively affected the opinion of the retailer involved.



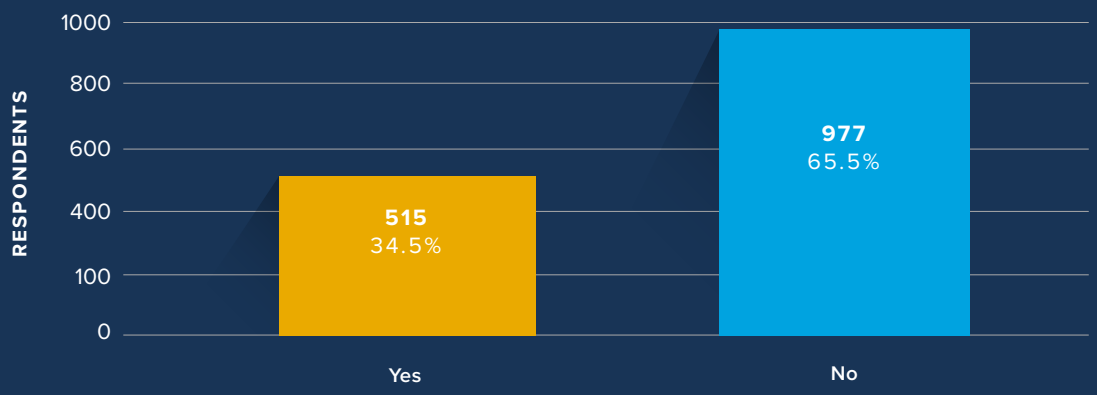
And it seems that consumers are not willing to cut retailers too much slack when it comes to delivering on customer experience. Nearly half of those surveyed said they are intolerant when it came to negative experiences when shopping on a retailer's website — with 15.4 percent saying they are "very intolerant."

Which brings us back to customer experience and its importance in building loyalty and customer lifetime value. It should come as no surprise that when customers find themselves navigating the world of online fraud, their loyalty wanes considerably.

Did that negatively affect your opinion of that retailer?



If you were declined by an online retailer for no apparent reason when trying to make a purchase, would you ever shop with that retailer again?



In Signifyd's survey, 38.2 percent of consumers said they would give a retailer one more chance after a single bad experience before turning their back on the business. Nearly 15 percent are zero-tolerance shoppers. One bad experience and they're gone.

That's a lot of pressure — 53.2 percent of a retailer's customers are hanging by a thread. One fraudulent order, one order held up by a cumbersome fraud review, one legitimate order mistakenly declined for fear of fraud, and that customer is lost — likely forever.

In fact, in Signifyd's survey, nearly two-thirds of respondents said they'd never shop with a retailer again if their order were declined for no apparent reason — the exact experience for a customer whose order was incorrectly flagged for fraud.

Innovative retailers are finding another way

It's just such heightened expectations that are leading some retailers to adopt the idea that they should orchestrate, not operate, the online customer experience. The idea, embraced by digitally native retailers such as Kylie Cosmetics, Rad Power Bikes, Allbirds, Away and others, is to build an ecommerce operations tech stack consisting of technology providers that specialize in key aspects of the online buying process.

Prominent venture capitalist Mary Meeker laid out the strategy in her 2018 Internet Trends report, breaking the ecommerce process into payment, online store, fraud prevention, purchase financing, customer support, finding customers and delivering product.

An online merchant, for instance, might build its store on Shopify, turn to Stripe for payments, rely on Signifyd for fraud protection, Affirm for financing, UPS for delivery and any number of other providers to fill in other gaps.

The idea is that the providers have deep and broad experience at what they do — working for many, many merchants at a time. For those that rely on big data and machine learning, it means they have vast data sets and lessons learned from some retailers that they can apply to all retailers.

They also may have built their enterprises on new ways of doing business. Signifyd, for instance, is among a few companies that offer guaranteed fraud protection. The model combines big data, machine learning and domain expertise to determine whether an online order is legitimate or fraudulent in milliseconds.

The guarantee model, driven by artificial intelligence, backs those decisions up with the promise that the fraud prevention provider will make the merchant whole — paying chargebacks and related fraud costs — on any approved order that later turns out to be fraudulent.

To circle back to the retailer's challenge in the era of customer experience, the guarantee model means a retailer can dramatically reduce the possibility that fraud-related problems or barriers drive customers away.

The model has demonstrated that it reduces fraudulent orders, eliminates cumbersome fraud reviews and results in a sharp decline in orders wrongly declined for the fear of fraud.

Perhaps as important as all that, the guarantee model can provide consumers with piece of mind — the survey found two-thirds of consumers put more trust in retailers that deploy AI to prevent fraud.

And providing comfort for consumers in a turbulent world goes a long way toward providing the kind of experiences they are looking for in a world where their personal data sometimes seems to be up for grabs.

About Signifyd

Signifyd, the world's largest provider of guaranteed fraud protection, enables online retailers to provide a friction-free buying experience for their customers. Signifyd leverages big data, machine learning and domain expertise to provide a 100 percent financial guarantee against fraud on approved orders that later turn out to be fraudulent. This effectively shifts the liability for fraud away from retailers, allowing them to increase sales and open new markets while reducing risk. Signifyd counts among its customers a number of companies on the Fortune 1000 and Internet Retailer Top 500 lists.

SIGNIFYD

HEADQUARTERS
2540 North First Street, 3rd Floor
San Jose, CA 95131
U.S.A.

—

WEB
www.signifyd.com

SUPPORT
www.signifyd.com/contact