4
Fraud Models that Threaten Retail and E-Commerce

5 Threats to Retail Marketers and the Marketing Technology Stack

7 Threats to Inventory and Logistics

9 Threats to Web Applications, User Accounts, and E-Commerce Modules

10
The Tale of the Tape: How Big is the Challenge?

11
Where Do We Go from Here?

Unsplash

Browser Window Shopping:

Threats to E-Commerce and How to Stop Them

Adam Sell, Director of Digital Marketing
Bethann Noble, Senior Director of Product Marketing

Over the last several years, the concept of “Black Friday” has expanded into a virtual cottage industry, a shopping mall directory of when and where holiday shopping could be best directed. Black Friday begat Cyber Monday, which begat Small Business Saturday, which begat Giving Tuesday, and so on. Last year’s digital sales on Black Friday were up 14% from 2018[1], setting a new high-water mark of $7.2 billion. And Black Friday is just the beginning of the traditional holiday shopping season.

With COVID-19 still depressing in-person shopping opportunities throughout much of the United States, however, that 2019 number could well be obliterated in 2020 as shoppers take to their computers instead of to their cars in search of the best holiday shopping experience. More than 7,500 stores in the US have closed in 2020 alone[2], following a closure of more than 9,000 stores in 2019. The pandemic has forced every industry to transform in one fashion or another, and the retail and e-commerce industries will need to emerge from this unique state of being far more ready to accommodate the desk warrior than ever before.

That evolution, though, comes with an opportunity, a price, and a risk. The opportunity is that there are new audiences that will be receptive to online shopping in a way they might not have before. Shoppers may find that they’re buying more things online than they have in the past: groceries, clothing, toiletries, even alcohol. Retailers have a chance to win the loyalty of folks who’ve never considered or engaged with products or services like theirs.

On the flip side, however, is the price - when there are new audiences and new opportunities for success, there are also new audiences and new opportunities for fraud. A common axiom in the anti-fraud business is that “fraud follows money”. And if more money is coming from shoppers less familiar with basic cybersecurity measures, then the fraudsters will be hot on their heels, trying to snatch a portion of that money.

And the risk is that unemployment hasn’t fully settled following the outbreak of COVID. The Bureau of Labor Statistics reports that the unemployment rate

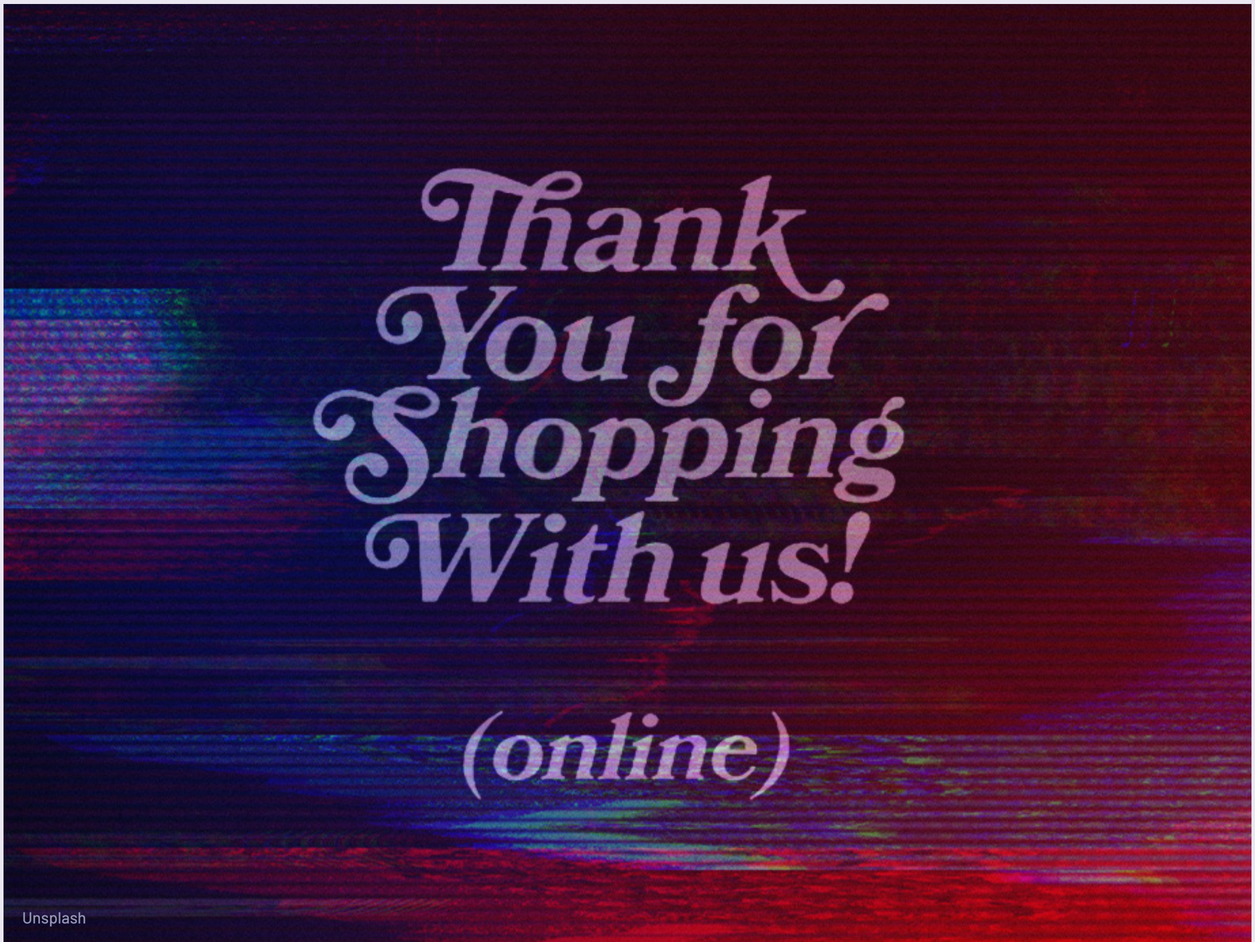
[1] Record Black Friday Sales: 14% Growth To $7.2B In Digital Revenue, Forbes, November 30, 2019
[2] More than 7,500 stores are closing in 2020 as the retail apocalypse drags on. Here’s the full list., Business Insider, August 17, 2020
[3] The Employment Situation - September 2020, Bureau of Labor Statistics, October 2, 2020

in September 2020 is roughly double[3] that of the same time a year ago. At its April peak, more than 14% of Americans were out of work. At the same time that retailers are bracing for a surge in online shopping, driven in no small part by consumers better accustomed to brick-and-mortar shopping, those same consumers may have less disposable income than in previous shopping seasons.

Every dollar a retailer spends on marketing this holiday season will need to work that much harder to accommodate these shifting challenges and opportunities.

As the 2020 COVID-influenced holiday season continues, there are a number of fraud models that retailers and e-commerce companies should be aware of, each with different threats associated. These threats siphon thousands of dollars every day from leading retailers. What's more, they have an unmeasurable impact on the way retailers are perceived by current and potential customers. When a consumer fails to complete a transaction because of a bot-based fraud scheme, it's not the fraudster they blame, it's the retailer.

These models of bot fraud aren't without remedy, though. The right bot mitigation tool can alert on—and even prevent—the deleterious impacts of fraud before they steal a retailer's money and reputation.



Unsplash

Fraud Models that Threaten Retail and E-Commerce

Sophisticated bots—and the fraudsters who deploy them—have a wide variety of attack vectors at their disposal, targeting different budgets or aspects of the e-commerce experience. Some of these models are more common than others, but each poses a distinct threat to a retailer, especially during a challenging holiday season.

These attacks fall broadly into **THREE CATEGORIES**

- THREATS TO RETAIL MARKETERS AND THE MARKETING TECHNOLOGY STACK
- THREATS TO INVENTORY AND LOGISTICS
- THREATS TO WEB APPLICATIONS, USER ACCOUNTS, AND E-COMMERCE MODULES

The damage that each style of attack is capable of varies pretty widely: some attacks focus almost entirely on an organization's budget, seeking in large part simply to make a retailer waste money chasing ghosts. Others can have a more dramatic impact, depleting inventory and wrecking customer sentiment by making it impossible to purchase highly sought-after items.

But even if the bots are hitting a retailer where the public can't see it, those bots are still making holiday shopping strategies that much harder to carry out.

Unsplash

THREATS TO RETAIL MARKETERS AND THE MARKETING TECHNOLOGY STACK

The absolute simplest way to explain these threat models is with a question: are you absolutely sure that all of the contacts in your marketing and advertising databases are real?

Short answer: the odds are pretty good that they're not. And while that might seem on its face like a minor inconvenience, the impacts of trying to market to fake contacts can be surprisingly far-reaching.

From a retail and e-commerce perspective, one of the key threats in this arena is **retargeting fraud**. Many retailers have a retargeting tool in place – it's a fundamental component in retail digital marketing. A cookied visitor is served ads throughout the web pertaining to the brand or items that they've looked at in the past. One retargeting provider[4] estimated that using retargeting tools can increase conversion rates by as much as 43%.

But if the person on the other side of those retargeting ads isn't a person at all, that conversion rate is zero. And the money spent following that bot all over the web is money lost and performance metrics spoiled.

The thing to remember here is that today's bots don't look like yesterday's bots.

[4] The Power of Retargeting: Computing and High Tech by the Numbers, Criteo, July 24, 2018

Earlier generations of bots came from data centers and were fairly easy to spot - they behaved in predictable ways and had obvious bot-like characteristics. Today's bots, though, are much more sophisticated. They come from the personal devices we all use every day, and as a result, they carry with them much more human characteristics. Browsing histories, purchase histories, realistic patterns of use - all of these make today's sophisticated bots a lot harder to identify.

That's what makes retargeting fraud so critical: even if a contact has all the hallmarks of being a real person, it may still be a sophisticated bot.

Those bots can make their way into the marketing and advertising databases in the first place through **lead-generation fraud**. Bots will spy a form on your website and automatically fill out the information requested to gain access to whatever's on the other side of the gate. The information that's submitted, though, doesn't correspond with an actual person with an actual email address who wants your actual communications. And that creates problems.

Email marketing is the lifeblood of numerous retail organizations - newsletters, sale alerts, incentive program reminders, the list goes on. It's the most effective (and cost-effective) way for a retailer to get their information in front of a current or potential customer.

Garbage in the email marketing system, however, isn't just an inconvenience, it's an actual hazard. With email providers deploying new anti-spam and bulk mail measures all the time, email deliverability is of enormous concern for email marketers. And the more bouncebacks that each email blast creates, the more damage is done to the email server's reputation—the scoring system that assesses how legitimate an organization's email outreach is—and the more likely that further emails from that retailer will be pulled into spam filters, even for real customers.

And believe it or not, that's the best case scenario for email issues following lead-generation fraud. The bots that are filling out those forms often need email

40%

Recent HUMAN research reveals that 40% of **marketing leaders could not estimate what percentage of the traffic to their website was human**, as opposed to driven by sophisticated bots.

addresses with proper syntax and structure to get through the gate, and one of the easiest sources for those email addresses is through leaked information courtesy of the most recent data breach. It's not difficult for a fraudster to harvest thousands of email addresses from a data breach and arm the bot army with those addresses.

Those addresses belong to real people who suddenly start receiving communications they didn't sign up for. In the age of GDPR and CCPA regulations, lead-generation fraud can put your marketing organization out of compliance. Each violation is a costly one, and when retailers have significant international operations, those violations have the potential to add up very quickly.

One final point on threats to the martech stack: CAPTCHA is not enough to prevent sophisticated bots from getting through. There are numerous services that offer CAPTCHA-breaking at an incredibly low price: some as low as $.60 for a thousand solves. If the reward for filling out a form is good enough, a fraudster will absolutely contract out that step of the process.

75%

Three-quarters of **marketing leaders expressed concern about compliance** with digital marketing regulations like GDPR and CCPR, but less than half scrubbed their databases regularly for fake contacts.

THREATS TO INVENTORY AND LOGISTICS

Many of us have experienced the scramble of trying to complete a purchase of a high-profile item immediately after the sale begins. Concert or sporting event tickets, limited-edition merchandise (like sneaker drops), or new gaming equipment - all of these command intense attention at the time of launch, and all of them have enormous opportunities for fraud.

Inventory fraud occurs when bots swoop in at the launch date and snatch up high-value items before humans can possibly complete the process. Machines, as a general rule, work faster than humans ever could. And those items inevitably find their way onto third-party resale sites at an enormous markup.

In 2020 alone, the releases of Sony and Microsoft's new gaming consoles resulted in high-volume presale events in the fall, many of which appeared to be plagued by bots descending on the event[5] and grabbing up as many consoles as possible before the limited inventory was depleted. Search any resale site and you'll find countless listings of these consoles, often at a steep markup from MSRP.

What's frustrating for retailers is that it's not the fraudsters that are blamed in this situation - it's the retailers themselves. Sentiment can turn rapidly from positive to extremely negative when a promised item becomes unavailable before a customer has a chance to complete the transaction. And in a season when logistics and supply chain management will already be pushed to the breaking point by the influx of new customers, retailers may find it difficult to respond to customer complaints about inventory availability.

[5] Walmart's latest PS5 preorders were gone in about a minute, The Verge, September 17, 2020

Unsplash

THREATS TO WEB APPLICATIONS, USER ACCOUNTS, AND E-COMMERCE MODULES

Perhaps one of the most insidious ways bots can influence the holiday shopping season is through the accounts that shoppers create on each site they visit. No matter how many data breaches are publicized each year, the public still fails to take cybersecurity best practices into place, creating an environment ripe for exploitation and fraud.

Account takeover is a blanket term used to describe a number of different tactics, but the end result is the same: the owner of an account is no longer the person in control of the account. Rather, a fraudster can use any saved information—including credit card and other payment information—to conduct fraudulent transactions. The fraudster could also simply harvest that information for resale on a black market later.

And as in other threat models, if a user's account is "hacked", it's the retailer who'll be blamed, not the user's own insufficient cybersecurity tactics. The retailer's reputation, in this way, relies in part on the customer's personal data hygiene.

An alternative attack, which bears some relationship to other attacks mentioned above, is **fake/automated account creation**. Imagine the advantage a fraudster can create for themselves on a limited-edition sale when they have a thousand accounts at their disposal instead of just one. Or imagine the lost margins a retailer will experience when a thousand accounts daisy-chain referral bonuses onto one another before purchasing big-ticket items.

$12

The average **value of stolen credit card information** is $12/account, according to TotalProcessing.

Each data breach has a cascading effect: the information harvested in that breach is sold on to other cybercriminals who use it to break into accounts for other web applications to collect and/or misuse what's stored in that database, which can result in a whole new set of information worth selling onto another cybercriminal, and so on.

The long and the short of it is: rolling your eyes at news of a data breach isn't an option, as your web application or e-commerce module might be the next target in the dominos.

Unsplash

The Tale of the Tape: How Big is the Challenge?

Here's where the rubber meets the road: how much does it cost for retailers to be victimized by the attacks above? Accenture estimates cybercrime cost global businesses on average $13 million in 2019[6]—up 12% from the previous year—and $27.4 million in the United States. No global business hub is immune: Japan, Germany and the United Kingdom also report annual average cybercrime costs in the double-digit millions with extremely high growth trends, with average annual costs up 31% from the previous year in the UK, for example.

Recent HUMAN research indicates that retailers may be losing more to retargeting and lead-generation fraud than they might expect. A conservative estimate revealed that top retailers with e-commerce capabilities could lose as much as $20,000 every day to marketing fraud, with an additional $20,000 per day lost to costs of using tools that manage fraudulent contacts. That translates to more than $15 million lost to marketing fraud every year for those businesses, split between the costs of fraudulent paid media and storing and retargeting fake/fraudulent names and information.

And that number may get worse before it gets better: recent research from analyst firm Gartner[7] revealed that while 53% of respondents expected a decline in their revenue in the next 12 months, 86% planned to increase their digital investment anyway, as businesses look to digital as the primary channel for commerce.

[6] The Cost of Cybercrime, Accenture, 2019
[7] 10 Things COVID-19 Will Change in Digital Commerce, Gartner, October 8, 2020

$13 Million

average lost to cybercrime in 2019.

Unsplash

Where Do We Go from Here?

All is not lost, however. The fight against sophisticated bots and their numerous attack vectors is still one that's winnable by humans. What it takes is a technology partner that looks beyond the characteristics that make earlier generations of bots easy to uncover. It takes looking at behavioral and contextual signals that these bots and the devices they live on send out. They're often very, very subtle, but they exist, and they make it possible for a bot-or-not determination to be made.

HUMAN is the global leader in making those bot-or-not decisions. HUMAN verifies more than 10 trillion interactions every week across the advertising, marketing, and cybersecurity ecosystems, and protects enterprises around the world—including some of the largest internet platforms—from the impacts of fraud.

HUMAN' technology can detect—and in many cases, prevent—these sophisticated bots from carrying out their attacks. Contact us today for more information about how HUMAN can supplement your fraud prevention toolkit to ensure sophisticated bots don't turn your holiday season campaigns into coal.