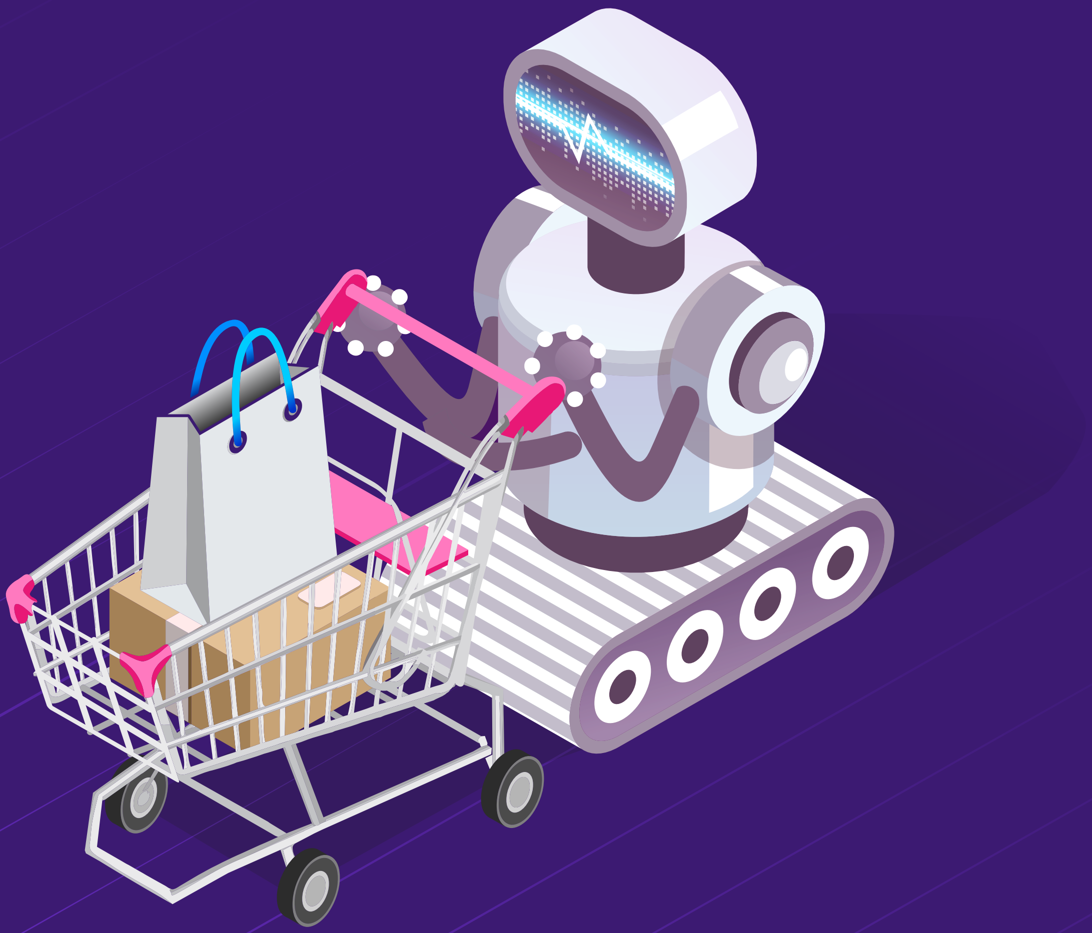
AD FRAUD BOT BEHAVIOR ON E-COMMERCE SITES



CHEQ

E-commerce sites are spending more than ever to capture new shoppers. Taking advantage of lightspeed online shopping transformations brought about by COVID-19, global brands spent $58.5 billion in e-commerce advertising by the end of 2020. The advertising boom is fueling e-commerce sales which rose by 30.4$ to $2.9 trillion worldwide by the end of 2020. Digital marketers pour money into search traffic (for instance Google Ad and Bing) and paid social channels (such as Facebook, Instagram, and Pinterest). This is used to ratchet up crucial e-commerce dials including customer lifetime value or average order value and bring down negative indicators of poor shopping experiences, such as bounce rates (the amount of visitors that "bounce off" a site before buying), and abandonment of shopping carts.

However, though digital marketing spend bring leads by targeting and attracting new shoppers, these dollars also bring invalid clicks, namely bots, onto e-commerce sites. Bots, often maintained by sophisticated ad fraudsters are software applications running automated tasks, clicking on paid search ads and keywords or social media promotions paid by e-retailers. The motivation: a quick means to make money by fraudsters, depletion of ad budgets hurting companies, and the skewing of these vital e-commerce metrics tracked throughout e-commerce businesses.

In this study we provide the first ever analysis of these bots after clicking on e-commerce ads. This report analyzes the movements and impact of bots, based on analysis of 30 leading e-commerce sites spending on paid search and paid social ads. It reveals for the first time the short and long-term implications of ad click bot movements in faking funnel numbers and hurting growth prospects.

METHODOLOGY

CHEQ analyzed 30 retailers spending at least $500,000 per month on search and paid social ad campaigns in 2020 to determine the behaviour of bots and where they land after clicking. The analysis involved real analysis of bots clicking on creative ad campaigns designed to bring new relevant shoppers into the funnel. The sample of leading e-commerce players included a top global skin care brand, grocery sites, a DIY online marketplace, a fashion and sports retailer, a travel site, an online university, a personal finance provider, and top provider of glasses and contact lenses.

This analysis tracked every click (of a real user or bot) for campaigns on paid search and paid social campaigns over a week, where users visit a site or landing page from creative ads.

Upon clicking, the CHEQ tag activated, triggering real-time user analysis of every click based on 1000 cybersecurity parameters including honeypots (bot traps), OS/Device fingerprinting and dynamic code patching. Bots are caught by a number of identifiers including clear data center traffic (48% of bots), VPN or location obfuscation (21%), activity-based filtration (9%) user agent analysis (7%) domain analysis (4%). Each of the companies mentioned in this study have had full detailed analysis of the ad fraud bot breaches revealed to them, with specific new measures to replace this bot traffic with real human customers.

10% OF E-COMMERCE AD CLICKS FROM BOTS

We found that one-in-ten ad-clicks across all e-commerce campaigns is bot driven. This is in line with a recent study by CHEQ and economists at the University of Baltimore which shows that overall click fraud reached $3.8 billion for online retailers alone by the end of 2020[1]. This cost represents the direct wasting of ad budget by non-human clickers that will never convert. The rest of this study looks at how these bots interact on e-commerce sites and the wider business damage they cause.

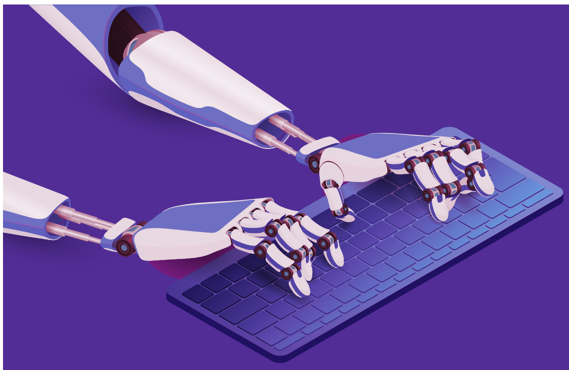
92% OF BOTS CLICK, SHOOT, AND LEAVE

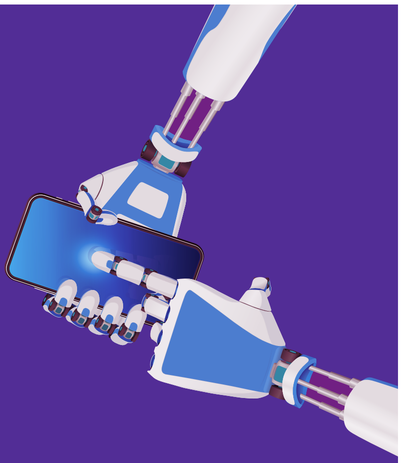
Their first tactic of bots to arrive at the landing page is clicking on ads paid for by e-commerce players to attracts customers. This achieves a primary goal of wasting vital ecommerce ad budgets relied upon to bring in new customers. Bots clicking on paid search ads were found to click on branded search terms (the name of a company, business, or brand) 70% of the time. This brings at least $1 lost to bots per click for most of the companies studied. In the case of one fashion e-commerce site for instance "men's jacket" saw a 56% invalid click rate, "shoe coupon" a 52% invalid click rate, and "Asics New", a 48% invalid click rate. Getting to the site has not only helped drain ad budgets, but also begun skewing metrics. Once on site, 92% of bots remain static for an average of 12 seconds, failing to click or move to a different section of the website. They then click off the site, leaving 12 seconds later. Most of the same bots return to the site to further mess up metrics designed to monitor real customer behavior – in one case 2117 bots returned 34031 times in a week.

[1] CHEQ and the University of Baltimore: The Economic Cost of Invalid Clicks 2020

BOTS: MOBILE VS DESKTOP

Bots behave differently whether they arrive via mobile or desktop. Bots time on site for was longer for desktop visitors at 12 seconds, compared to bots arriving via mobile (7 seconds). The bounce rate was 22% for bots arriving via desktop and 58% for mobile visits. This compares to an average bounce rate of between 20% and 45% for most e-commerce sites. Overall bounce rate, the percentage of visitors who enter the site and then leave, tended to be relatively high for bots, at a rate of 58%. Most marketers accept that a range of 55-65% for bounce rates shows significant room for improvement, but the high numbers of bots discovered shows how clearly bots affect such metrics.





Bots visited from desktop	Size of Sector	Fraud in Billons of Dollars
89%	landing page visit only	92%
12 seconds	Total time of bot visit	7 seconds
90%	Completely static	79%
22%	Average bounce rate	58%
2%	Cart or check out	0.5%

ONE IN 50 BOTS REACH CHECKOUT

In our analysis, one in every 50 bots arriving via paid search and paid social campaigns click their way to a site's online checkout page. In our study alone this equated to more than 3.5 million bots clicks. This had the effect of clogging up online baskets, causing logistical and refund challenges, and skewing vital metrics. This included filling out forms and making purchases. Bots analyzed affect conversion rates including online sales, leads, email signups, and form completions. In the case of a personal finance company this included "loan reverses". This saw the loan company approve loans based on a specified criterion, only then to cancel it as details turned out to be fake or fraudulent. his put a massive exposure on the loan business which was forced to rip up loans of those likely default on their payments. In another case, bots clicked on confirmation pages, engaging in chargeback fraud, where bots make a transaction and then seek a refund. Bots were very easily able to get past most defenses in these cases. If email verification is required, the fraudster controls the email addresses they inputs. This can be done in various ways: buying bulk addresses redirecting every email to an email address the fraudster controls and automating the clicking of verification links. They can often buy and use domains with made up names to generate emails for instance.

SOPHISTICATED ATTACKS AGAINST E-COMMERCE PLAYERS

During this analysis, sophisticated bot rings were discovered targeting online commerce sites. One ad ring used a network of infected machines, IPs, and data centers to drain the ad spend of a big spending online company resulting in millions of dollars of wasted spend. The techniques used by the fraudsters involved using a bot network and obscuring techniques to "click" on more than 20 of the most popular keywords in the sector often costing up to $30 per click.

RISING BOT SOPHISTICATION

The attacks on e-commerce players demonstrates that the sophistication of hackers attacking marketing spend, which is used as a trojan horse to enter e-commerce funnels. For the majority of fraudsters, the automation tools used to commit fraud are evolving without them having to do very much work – fraudsters just have to hide and rewrite certain elements in order to evade more and more tests. Bot-makers create millions of headless browsers, that can simulate all human-like actions such as mouse movement, page scrolling, and clicks, to load webpages and cause ad impressions which appear human. Malicious SDKs for advanced and AI-powered click injection are sold in the Dark Web to the public for a fairly low price to perpetrate ad fraud, offering the opportunity in the words of the suppliers to "emulate ad clicks and hijack clicks including Google, Facebook and organic clicks." Meanwhile data center-dwelling bots have been replaced by fraudsters using harder to-detect residential Windows systems running a Remote Desktop Protocol (RDP)[1] connection exposed to the Internet.

This typically involves brute forcing million RDP servers all over the world[2]. The activity is from a real Window with an updated, valid Google Chrome browser. Unlike normal fraud schemes which are using bot/automation tools (Selenium, Puppeteer) in this this case, the attack uses a legitimate environment (for instance an updated Chrome, Windows, and residential IP). Leading criminal lawyer Arkady Bukh, a New York-based attorney with a history of representing suspected hackers and ad fraud perpetrators from Eastern Europe, including those involved in the "Methbot" case,[3] says the growth in sophistication by bad actors is marked. "There is widespread fraud from huge amounts of traffic getting directed through botnets. Before, it was boys and girls in Russia sitting in boiler rooms clicking manual clicks in order to get apparent traffic to defraud affiliates. Now it's done by bots."

[2] RDP is a remote desktop protocol, providing a user with a graphical interface to connect to a different computer over a network connection. Although without controls it can be a significant security risk. See for example GoldBrute, the botnet searching for RDP connections https://www.pandasecurity.com/mediacenter/malware/goldbrute-botnet-rdp/

[3] The Methbot case is estimated to have cost marketers at least $3 million dollars each day the botnet operated

BOT DEFENSES

Despite the vast leaps in sophistication and overtly criminal behavior observed, we discovered that certain outdated defenses against bot activity remain. For instance, the concept of "hidden fields" were still used. This defence maintains that while real shoppers do not see hidden fields, spam bots are drawn to them, fill them out, and reveal themselves. However, these have been shown to have limited effects, and only for low IQ bots, which are no longer the standard. If a bot has a more specific purpose and money has been spent in development to target such enterprise customers, such bots will know what to click, and what to avoid.

Similarly, penetration tests carried out show that Captchas, forcing user tests to determine whether or not the clicker is human, are very easy to bypass. Vendors, including 2Captcha ($0.77 per 1,000 Captchas) have more than 2,000 workers online solving them, which fraudsters combine with automated software. The combination of software and APIs for instance allow for fast account creations to appear as human, with new accounts on Reddit easily created using dev ops software such as Puppeteer alongside such

MADE-TO-ORDER BOTS TARGETING CAMPAIGNS

We see in our analysis the appearance of bots made to order, deliberately designed to appear human-like, targeting pricy ad campaigns. To take only one example, the bot bounce rates are would not attract too much attention. Though the bots contributed higher bounce rates than industry averages, bot movements on and off sites, remain within a human range. Indeed, bot movements are deliberately created to mimic human clicking. Criminals have access to an untold number of malware-infected devices across the globe to this end. These are used to track, study, and incorporate real-world human activity, such as non-linear mouse movements.

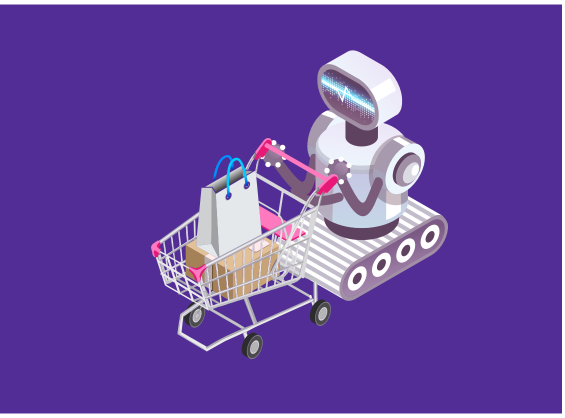
To this is added stolen credentials, which are numerous and cheap – tens of billions of credentials from successful attacks are available on the dark web, with as many 7.9 billion records exposed in the first nine months of 2019 alone.[4] In the words of independent ad fraud expert Dr Augustine Fou: "Bots love to click on ads. In fact, they would click on every ad if they could, but 100% click through rates would be too obvious, even to marketers that only occasionally pay attention. So, bots dial their clicking back so that an average of 5 - 15% click through rates are seen in reports. Compared to click through rates from humans (in the 0.1% - 1% range) these look spectacular."

[4] Risk Based Security, Q3 2019 Data Breach Report, November 2019.

8 BOTS CAUGHT ON E-COMMERCE SITES

Based on the undercover movement of bots clicking and scrolling beneath the surface of e-commerce sites, we identified 8 bot types living rent free on e-commerce sites.

1. CART BOTS



2 % of bots arrived to the online cart, hurting conversion metrics. We found multiple carts simultaneously being loaded up with items, which can cause infrastructure and software slowdowns.

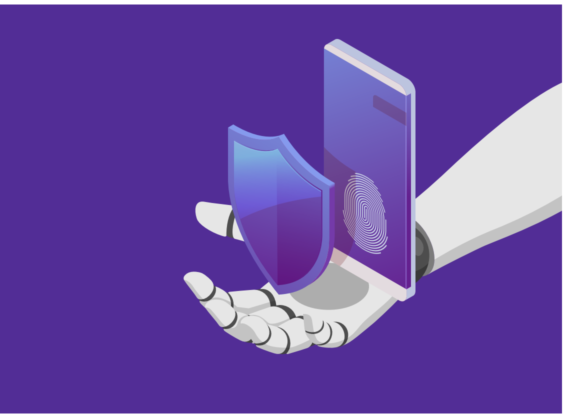
2. RETURNERS

Thousands of different bots returned several hundred times. Not content with simply hurting spend, these bots became the subject of retargeting campaigns designed to reach real shoppers. On one site for instance, 2117 bots returned 34031 times.

3. SCRAPERS

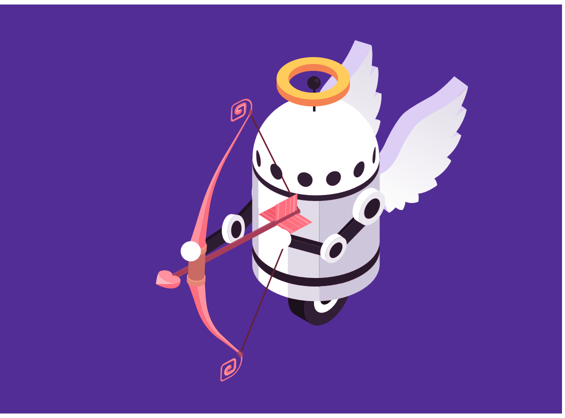
Scraping is the automated collecting by bots of large volumes of data from web pages and applications. There was an average of 5000 clicks on one site generated by scrapers. One business driving users to its recipe sites discovered that bots were stealing and monetizing this quality content through online advertising, hurting their rankings and

4. LONG DISTANCE LOVERS



One in five bots used VPNs or other location obfuscation methods to pretend to be US, UK or Japanese shoppers. In fact the attack was located located in countries that the e-commerce player did not ship to, including Pakistan, and Vietnam. In one case a top global skin care brand analyzed spent hundreds of thousands of dollars on PPC spend suffered from malicious VPN and data center traffic. One of the world's largest DIY marketplaces, spending $2.5million a month, saw more than 14,000 invalid clicks, with users deploying a VPN to mask their location, primarily from China and Malaysia (masking their location as UK buyers).

5. HEARTBREAKERS

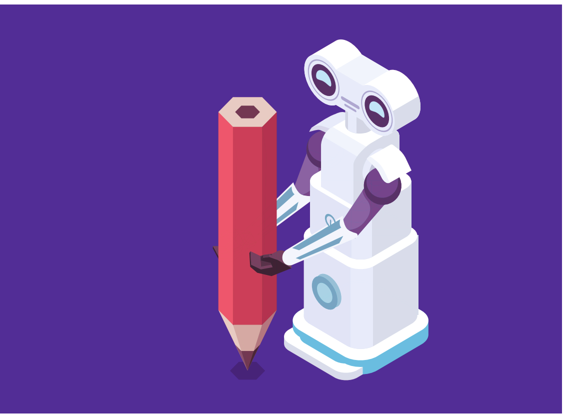


Retargeting aims to get website visitors who didn't convert back to your site by showing them relevant ads. One in five marketers have a dedicated budget for retargeting. But it can be heartbreaking when money and attention is used to reach returning bots. In one case an online e-commerce player wasted $3500 retargeting bots that visited the site.

6. CHARGEBACKERS

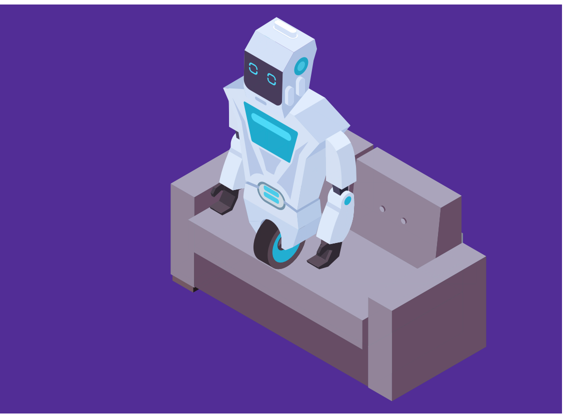
CHEQ found that bots clicked on confirmation pages, engaging in chargeback fraud. This is where bots make a transaction and then seek a refund. One large company spent $7million a month on paid search and paid social media channels. Our analysis found thousands of invalid clicks on their confirmation pages, indicating chargeback fraud.

7. CRITIC BOTS



Bots also generated fictitious reviews, damaging reputations for service-driven ecommerce players. It has been shown how easy it is for bots to write fake reviews (positively for inflating companies) or negatively against businesses. Fake reviews bot-driven services are common on the dark web, including generating fake app ratings. In the analysis of our travel site, we found 2500 invalid clicks from bots generating fictitious reviews.

8. SIT-IN BOTS



Sit-in bots for the most part just clicked on to the landing page and chill. They are content to waste the business budget of the retailers. They also serve to hurt core metrics relied upon by e-commerce businesses.

HOW BOTS SKEW VITAL E-COMMERCE METRICS

By identifying this bot behavior, it soon becomes clear how easily e-commerce business metrics are fooled due to sophisticated bad actors and armies of bots on sites. E-commerce players and marketers rely on e-commerce metrics when determining where money is spent on campaigns, and providing future assurance to investors and shareholders on the success of marketing efforts.

1. BOUNCE RATES

E-commerce bounce rates suffer when bots click on and off landing pages without engagement. Our analysis shows that the average bot actually stays on site for between 7 seconds (mobile) and 12 seconds (desktop). This is a high bounce rate but is designed deliberately by fraudsters not to arouse suspicion.

2. CART ABANDONMENT RATE

The abandonment of shopping carts – that is a user skipping after adding items - is a $4 trillion problem for e-commerce, with bots playing a significant part in this headache. With 2% of bots heading straight to the cart or checkout, billions of dollars could be shaved off the large global shopping cart abandonment rate through measures to reduce bots in carts. In addition, while humans abandoning carts can return to buy, bots will not. Retargeting can often lead to simply throwing good money after bad bots.

3. CONVERSION RATES DROP

Conversion rate refers to the percentage of your visitors who take an action on your website. This action can be anything, such as signing up for an email newsletter or making a purchase. Removing bots can be a powerful means to improve conversion rates. Say that you get 20,000 visits to your website and that 2% of visitors convert and buy a $100 product, you will make $40,000. If you increase your landing page conversion rate by just 0.5% by preventing thousands of bots clicking, you will make an additional $10,000.

4. COST OF CUSTOMER ACQUISITION

Customer acquisition cost – also referred to as CAC – is how much money it takes to "buy" a customer. This helps us plan how many customers we want to acquire in a certain time period and allocate our marketing budget appropriately. When companies understand the levels of bots that can be removed, you may be able to reduce the costs of getting real customers. This, in effect, replaces hundreds of bots with real customers. Those not tackling bots are likely to see diminishing returns for marketing dollars.

5. CUSTOMER LIFETIME VALUE

Customer

Lifetime Value (CLV) is crucial in determining your business' present and future success. It is an often-overlooked metric that can accurately predict how much your customers are really worth. Bots skew the data, particularly when in 2% of cases they end up checking out on your e-commerce sites or taking part in chargeback frauds which then have to be deducted post-purchase from

6. AVERAGE ORDER VALUE

Average order value (AOV) is a useful measure of how much shoppers are spending. AOV is a simple calculation: the amount of revenue generated divided by the number of orders received. By replacing bots with real customers, the average order value of this metric is likely to increase sharply.

RESULTS FROM PREVENTING BOT CLICKS

The impact of removing bots from the e-commerce equation can be highly impactful. Reinvesting $14000 spent on bot clicks and replacing them with real human customers is expected to bring the average e-commerce player 163 additional customers a month. This is based even on a conservative estimate that only 55% of bots will be prevented through cybersecurity-based blocking shown in this analysis. In addition, retargeting which represents 4% of media spend across our companies, will become far sharper - targeting humans rather than new or returning bots. In the case of an online education portal, we found that removing 1213 bots per week with real leads, equated to 788 real human learners, 10 new enrollments and $150,000 more revenue per month. The methods of bot removal also alerted our e-commerce players to other types of fraud – whether bot or not. This included instances of partner and affiliate fraud and long-term challenges from affiliate partners.

CONCLUSION

Improving marketing processes is taking center stage at a time when marketers are required to justify every single dollar of spend. E-commerce has seen a rising amount of opportunity during COVID-19. Indeed according to consultancy McKinsey in May 2020, e-commerce vaulted five years forward in consumer and business digital adoption in a matter of around eight weeks. But growth nevertheless remains precarious, not least with fresh e-commerce challenges such as record online competition, and rapidly changing consumer behaviors.[5] Added to this is a new wave of highly sophisticated bots surfing on waves of rising ad spend. Every invalid click delivered by such bots represents ad spend that is not generating genuine advertising engagement. Putting money into serving bots is even more counterproductive when real (human) customers desperately need to be ushered into funnels and buy things, in a period when marketers and CEOs are feeling the pressure to hit core metrics. Removing this unnecessary wastage and replacing bots with qualified prospects will give a significant advantage to players to achieve growth in a rapidly shifting e-commerce landscape.

[5] Shopify, the future of eCommerce in 2021