MULTICHANNEL MERCHANT

ECOMMERCE SPECIAL REPORT

# Fraud Increasing in Ecommerce, But Help Is on the Way

by **Brian Kelly,** Multichannel Merchant

From account takeover to friendly fraud, phishing, spoofing, counterfeiting, chargebacks and more, there are many ways for fraudsters to disrupt and derail ecommerce. This is a major thorn in the side for retailers and honest customers alike. However, despite some depressing trends in fraud, this is not a doom-and-gloom situation. There are many robust solutions and services available to retailers. We'll take a look at some current fraud trends and explain the best ways to safeguard against those threats.

Ecommerce, bolstered by consumer avoidance of brick-and-mortar locations during the pandemic, continues to grow at record rates. U.S. ecommerce sales are projected to continue to soar by double digits, skyrocketing up 17.9% in 2021 to $933.30 billion, according to the U.S. Ecommerce Report 2021 from Insider Intelligence. Ecommerce penetration will also continue to increase, more than doubling from 2019 to 23.6% in 2025.

Fraudsters, bad actors and assorted criminals will continue to try and get their share of that legitimate commerce in an illegal fashion. While the overwhelming reason to engage in ecommerce is to grow revenue, at least 42% of retailers say they're doing so to improve customer service, according to Gartner. Unfortunately, it's a fact that a retailer's revenue, brand reputation and customer service ratings will take a hit when fraudsters get through their defenses.

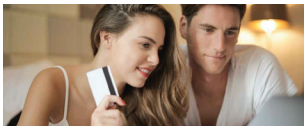
It doesn't look like it's going to get any easier for retailers, as the fraudsters are continually upping the ante. "Criminal groups are well-funded and have increasing access to substantial computing resources like cloud computing and technologies such as artificial intelligence and machine learning," said John Harmon, a senior analyst at Coresight Research, a global advisory and research firm specializing in retail and technology. "They can deploy an army of frauds to find weaknesses in networks."

The upcoming holiday shopping season is a logical time for fraud activity to increase. According to a report from Red Points on ecommerce shopping habits during the holidays:

- 81% of consumers plan to spend up to $500 more online this year compared to last year

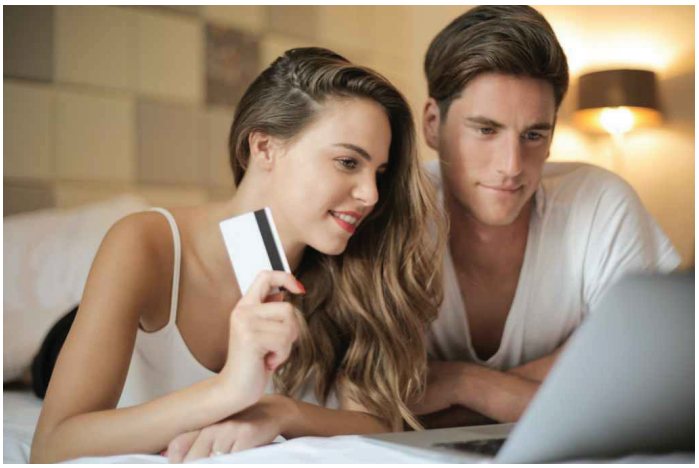
CONTINUED ON PAGE 2

## FEATURED IN THIS REPORT



Page 2
**Disconnecting The Bots**

Page 3
**There's Nothing Friendly About Fraud**



- 56% said they were victims of buying fake products online while holiday shopping

The report touches on how brands are affected when consumers believe they have purchased a fake product from a popular brand:

- 52% of consumers say they would ask for a refund
- 47% say they would leave a negative review where they bought the product
- 44% say they would complain to the original brand
- 39% say they would no longer buy the brand
- 17% say they would post on social media about it

While none of these fraud trends are necessarily new, the bad news is that there is more attempted fraud than ever before.

"We're seeing an increase in chargebacks, account takeover fraud and friendly fraud," said Michael Habermann, a sales engineer, payment, tax and fraud technology at omnichannel commerce technology company Radial. "I think that the level has just risen because there's much more opportunity."

Online shopping skyrocketed during the pandemic, providing that opportunity for fraudsters. Many consumers started shopping online for the first time, and they are much less sophisticated about protecting their information on the internet.

Other factors are contributing to the increase in ecommerce fraud, as well. "The advent of social commerce and multiple shopping channels like Instagram offer an expanded number of potential entry points for hackers," said Harmon. "In addition, the greater number of people working and shopping from home makes home networking devices like webcams and routers potential entry points for hackers, and many of these are running outdated or buggy software."

## Disconnecting The Bots

Attempted fraud attacks have become more widespread as hackers have grown more sophisticated, adopting advanced technology in their quest for new sites and products to exploit. Fraudsters in the past year turned to automated attacks like never before. According to Netacea's Bot Management Review, almost 80% of ecommerce firms report being attacked by bots in the past two years. And an even more disturbing bit of information: Forrester found bad bots accounted for nearly a quarter (24%) of all internet traffic in 2019.

In addition to damaging retailers, inventory hoarding and shopping cart fraud bots disrupt customer sales. Fraudsters' bots will focus on exclusive inventory such as limited-edition sneakers, concert tickets and gaming consoles, and then resell them at huge profits. These bots essentially overwhelm a retailer's website, buy all the premium stock and leave legitimate customers out in the cold. When bots launch a successful attack, consumers don't know it happened and blame the retailer. So, they hammer away at a retailer's customer support functions with complaints, talk about their disappointing experience on social media or end up buying from competing retailers. In the worst of all possible outcomes, they buy the item from the fraudsters themselves on a marketplace platform.

"So, from the standpoint of the retailer or brand, they're still selling their inventory, but they're not selling any of the peripheral goods that go along with it," said Sandy Carielli, a principal analyst at Forrester.

"If a bot is buying sneakers, they're not buying other shoes," Carielli said. "If they're buying a game console, they're not buying a game or extra controllers. So, companies are losing out on that revenue. You're also really upsetting customers who are going to your site, finding the item sold out and going elsewhere. Maybe they don't come back to you the next time they want to buy something."

The use of bots in fraud is a growing trend, and not

one that depends on a high rate of success to bring a potentially high rate of return.

"The thing about bot fraud is that they are not taking advantage of traditional security vulnerabilities and web applications," said Carielli. "The bots take advantage of legitimate business logic. When fraudsters use bots for credential stuffing, they're taking previously stolen credentials, tens of thousands of them, and trying them against different sites in an automated fashion. And even if they only get a couple of percentage points success rate, the fraudsters are potentially taking over a good number of accounts that way."

In defending against automated ecommerce fraud, Carielli said retailers need to answer questions such as, "Is this a human or is this a bot? And if this is a bot, is it a good bot, one we've been expecting? Or is it a Google search bot that we want to be scraping our information and help us by showing up in searches?"


Help is available for beleaguered retailers. A report on bot management from Forrester shows how the most sophisticated bots can successfully fake human behavior, beat basic Captcha challenges and hijack a real customer's browser and tokens. Retailers can fight back with bot management tools that combine detection methods such as statistical analysis of user behaviors, collecting biometrics to detect anomalies and continually updating reputational scoring. Vendors of these tools also collect data on new bot trends and share that data with clients, development teams and the overall market.

## There's Nothing Friendly About Fraud

With "normal" fraud, the fraudsters use stolen identities such as someone's credit card. In friendly fraud, the fraudster is the actual cardholder, someone authorized to use the cardholder's account, or someone who is not authorized but has access to the card information. Even after requesting detailed payment information, reviewing addresses and all the normal level of verifications it's still possible to be duped by fraudulent activity from time to time. Payment protection platforms can shield retailers by putting extra layers of security between products and fraudsters.

In today's ecommerce environment, consumers are well aware of fraudsters and hackers. "We've found that well-designed, low-friction fraud screening procedures can actually be an upselling point," said Habermann. "Another thing we found that leads to better conversion rate is the amount of payment methods that retailers can offer, such as Google Pay, Apple Pay, Amazon Pay and PayPal. We've found that those payment options can convert more good orders and their clientele will have a better experience overall."

Some fraud prevention solutions providers offer single-point integration, so retailers can add any payment options they choose in a matter of seconds.

In some form or fashion, machine learning has been involved in fraud prevention since 2004. Combined with artificial intelligence (AI), machine learning develops fraud protection methodology based on all the data available from consortiums, third parties, retailers and solution providers' internal data. Retailers can more accurately pinpoint fraud risk without turning away legitimate customers by leveraging machine learning technology and consortium data to assess the risk of every transaction.

Adam Pressman, a managing director in the retail practice at AlixPartners, favors the ML/AI big data approach to fraud detection. "There are third-party solutions that provide fraud prevention, and they not only know the interaction that you're having with your customers, but they also have visibility into how your customers are interacting with other brands," Pressman said. "So, you're not just looking at the interaction directly with your brand, but also at other data points to help you understand more broadly how a consumer or a customer might be behaving."

Particularly successful fraud prevention systems use

machine learning and rules combined with a manual review process. "A lot of retailers have a pass/fail process, but we're adding the manual review process to try and save the sale and avoid false declines," Habermann said. "With all the data available, we only need to do a small percentage of manual review, but it's a valuable tool."

## Counterfeit: More Than Fake Bills

Counterfeiting is an ecommerce fraud trend that negatively impacts retailers, brands, and consumers alike. If a consumer buys a product that they believe is the genuine article, but instead receives a cheap knockoff, it blows back on the marketplace, the retailer and the brand.

Although counterfeiting is illegal around the world, the risk is generally low for fraudsters. A typical prison term for fraudsters selling counterfeit goods is three to six months, said Daniel Shapiro, vice president of brand protection solution provider Red Points.

"Not every counterfeiter gets prosecuted, unfortunately, because federal prosecutors look at someone who's had a warehouse full of counterfeit designer bags, and then they look at people who had warehouses full of drugs and guns, and who do they end up going after?" Shapiro said.

The amount of counterfeit goods sold in ecommerce has steadily risen year after year, as well as the amount of fake social media sites that promote counterfeits, and fake reviews that espouse these goods.

"It's past the scale where an internal team or an external company can use human capital to find those infringing products, or those unsafe products," Shapiro said. "Today, brands have to deploy a technological strategy, using a combination of machine learning, image recognition, locality recognition and image fingerprinting, among other kinds of techniques used to find that product. Brands need the kind of technologies that can search hundreds of thousands of listings, which have four or five photos apiece, to identify counterfeits."

## Beat The Fraudsters to The Punch with Potentially Lethal Combos

An increasing number of ecommerce sellers are experiencing fraud attacks from a variety of sources, using an almost bewildering array of tactics. This period of explosive growth in ecommerce has exposed some critical needs for retailers to protect against fraud, for brands to protect their reputation, and for all involved in ecommerce to rise to shopper expectations regarding account security.

Fear not, help is out there. "There are several tools and providers that are combining different elements of ML/AI with aggregated data and trend analysis," Pressman said. "Many brands are still leveraging manual techniques or prior algorithms to manage fraud. These new tools are coming in to more dynamically monitor and evaluate if there's still human intervention. These digital tools and support are helping retailers evolve their fraud detection techniques."

Now is the time to review your current anti-fraud policies and operations, especially as the 2021 peak holiday season is now upon us. Depending on your organization's role in ecommerce, consider bolstering existing protections, adopt and implement new policies and solutions, or – given the variety of possible fraud attacks and exposures – partner with a solution provider to build an improved fraud protection network for your business.