DIGITAL COMMERCE 360 RETAIL

NOVEMBER 2020

TIPS TO FIGHT FRAUD DURING COVID TIMES

With more first-time customers amid surging online sales during the COVID-19 pandemic, fighting ecommerce fraud is harder than ever. This report details more than **a dozen strategies to fight fraud** during the coronavirus pandemic, including how to **prevent fraud on digital gift card sales**. Plus, what all online retailers need to know about **Magecart**.

COMPLIMENTS OF: Sift | NoFraud

CONTENTS

12 STRATEGIES FOR PREVENTING FRAUD DURING THE COVID-DRIVEN ECOMMERCE BOOM

A growing number of first-time website visitors amid the surge in online shopping and new services like curbside pickup pose challenges for fraud fighters. Here are 12 ways online retailers can respond.

By Don Davis

The spike in U.S. online shopping since the COVID-19 outbreak that forced many physical stores to close in March has created big sales opportunities for online retailers, but also challenges in deterring fraud.

Many website visitors are first-timers, which makes it harder for retailers to be sure they're legitimate shoppers and not criminals. Curbside pickup also has exploded during the pandemic, posing special obstacles to fraud fighters.

And criminals are taking advantage of the billions of pieces of consumer data that have been exposed in data breaches—4.1 billion records were exposed just in the first half of 2019, according to Forter, a specialist in ecommerce fraud prevention. In some cases, criminals combine information, such as an email address they've allowed to "age" to make it appear legitimate with a credit card number stolen from an honest consumer.

DIGITAL COMMERCE 360 RETAIL

12 STRATEGIES FOR PREVENTING FRAUD

TIPS TO FIGHT FRAUD DURING COVID TIMES

Criminals hit athletic shoe brand Brooks Running with this kind of scam in March, just as the pandemic was taking hold. However, it took Brooks a while to spot it because of the high volume of legitimate orders, says Chad Funk, fraud specialist at Brooks Running, which is owned by conglomerate Berkshire Hathaway.

"There was an insane jump in orders, which meant more orders to review and more opportunity for fraudsters to get through," Funk says. "All that combined worked against us."

Once Brooks and its fraud-prevention provider Kount identified the fraud pattern, Brooks was able to shut down the scheme. Meanwhile, the brand has fought a second type of fraud and also modified its fraud filters to keep from rejecting good orders when a surge in consumers placing phone orders tripped an alert geared to pre-pandemic shopping patterns.

Not every online retailer faced the array of fraud issues Brooks did. But many have seen an increase in fraud attacks.

NuData, a fraud-prevention company owned by MasterCard Inc., says retailer fraud losses from chargebacks—charges reversed due to cardholder complaint that a card was used without permission—increased 36% in April and May following the lockdowns compared with January through March for orders delivered to consumers.

12 TIPS TO PREVENT FRAUD

1. Encourage customers to add a second form of authentication to protect themselves from account takeover.
2. Let your fraud-prevention vendor know of expected spikes in traffic and sales.
3. If there is spike in chargebacks, look for a pattern and create rules to block similar purchases.
4. When shopping patterns change, adjust your fraud-detection rules to ensure they are in line with current customer behavior.
5. If you're selling high-value products, watch out for triangulation fraud in which criminals buy products with stolen cards to ship to consumers taken in by phony ads.
6. Adjust your fraud rules to recognize that more consumers are shipping online orders to an address that's different from their billing address.
7. Flag many rapid log-in attempts from a single device as suspicious.
8. Evaluate the history of the purchaser's email address for signs that it's being used by criminals to commit fraud.
9. Watch for transactions in which there is a great distance between the purchasing devices' IP address and the card's billing address.
10. Consider working with a fraud-prevention provider that draws on transaction data from many companies for help in determining whether transactions on your ecommerce site are legitimate.
11. Make the website the primary line of defense against fraudulent in-store or curbside pickup orders, rather than relying on store employees to deter criminals.
12. Stagger holiday sales over a longer period this year to keep fraud teams from being overwhelmed.

Those attacks are likely to accelerate during the holiday season, when online retailers struggle to review all suspicious orders because of high transaction volume. This article will discuss 12 ways online retailers can protect themselves without turning down lots of good orders.

Tip No. 1: Encourage customers to add a second form of authentication to protect themselves from account takeover.

Consumer electronics merchant Newegg Inc. was one online retailer that experienced an increase in fraud attempts on its website, but no increase in successful fraud.

"Low-sophistication fraud is trending upward, presumably due to the recent rise in unemployment and other pandemic-related economic factors," says Don Gwizdak, head of logistics and customer experience. "We see this as opportunistic fraud, which means these individuals aren't successful because ecommerce fraud isn't their livelihood or profession."

30%

The percent of traffic to ecommerce sites during the COVID-19 period from first-time visitors, compared with 5-7% of first-time visitor traffic before the pandemic.

Source: Forter

Nonetheless, he says, Newegg is considering encouraging consumers to guard against account takeover fraud by requiring a second check mechanism when they place an order, such as sending a confirmation code to the consumer's mobile phone or email address on record. General merchandise retailer Target also encourages customers to add a phone or email address to their profile so Target can prevent fraud.

Tip No. 2: Let your fraud-prevention vendor know of expected spikes in traffic and sales.

Another retailer that has seen no increase in fraud losses is Foreo, a maker of skin care devices and products that's based in Croatia and sells worldwide through Foreo.com. That's despite a 95% increase in revenue during the COVID-19 period, says Selma Busovaca, head of Foreo's business unit responsible for its Luna line of facial-cleansing devices.

Busovaca credits its fraud-prevention vendor, Signifyd, for blocking fraud. She says Foreo has used Signifyd for four years, choosing it because it promises to reimburse Foreo if any approved purchases turn out to be fraudulent. Signifyd, like competing fraud-prevention companies, reviews transaction data from all its clients to get a broader view of activity than one retailer would have, and applies artificial intelligence technology to detect fraud patterns.

Busovaca says Foreo provides information to Signifyd to help its fraud-detection system

better understand if transactions are legitimate. For example, because Foreo sells worldwide, the brand lets Signifyd know to expect a surge in transactions not only on Black Friday but also on the big Singles' Day online sales day in China, which takes place every Nov. 11. By giving Signifyd a heads up about promotions Foreo can ensure the fraud-prevention company doesn't flag good orders for review based on an unexpected spike in volume.

Tip No. 3: If there is spike in chargebacks, look for a pattern and create rules to block similar purchases.
But other retailers have not been as fortunate. In fact, Brooks Running faced two types of fraud attacks this year, Funk says.

The first began in late March, soon after many stores closed their doors and online sales began to surge at BrooksRunning.com. Online revenue increased by nearly 130% in the first eight months of 2020 over the same period in 2019, Funk says. What made the fraud hard to spot initially was that the criminals created email addresses and then let them sit for at least two years—knowing that orders from newly created email addresses raise red flags. Then, the criminals used those emails to make purchases with stolen card numbers.

When the chargebacks started coming in, Funk and his fraud-prevention provider Kount went to work figuring out the scam. Kount works with Ekata, which tracks email addresses and other elements of personal identity, and could see that the email addresses had been around long enough not to arouse suspicion. But Kount also spotted that the names in the email addresses, which often were in the format of john.smith@gmail.com, did not match the names associated with the billing and shipping address of the card being used.

"It was really easy to see it was fraud if you had your eyes on it," Funk says. "Kount has a really good program to see how orders are linked together."

Once Funk understood the scheme, he was able to set rules to stop it. Funk says 15 or 20 fraudulent orders got through early on, costing the company a few thousand dollars, while Brooks successfully stopped about 100 fraud attempts using this scheme.

Tip No. 4: When shopping patterns change, adjust your fraud-detection rules to ensure they are in line with current customer behavior.
Funk says Brooks looks for many tell-tale signs of fraud, including when a single device places a large number of orders in a short time.

1.18%
The percent of fraudulent log-in attacks that were made with the correct log-in credentials in the first half of 2020.
Source: NuData

'There was an insane jump in orders, which meant more orders to review and more opportunity for fraudsters to get through. All that combined worked against us.'

— Chad Funk, fraud specialist, Brooks Running

However, those rules sometimes must be adjusted. For example, during the pandemic, many shoppers who had not previously purchased from Brooks called customer service to get advice and then placed an order over the phone. The Brooks system assigned all orders taken by a single service representative to a single phone number, which set off a warning flag about a device placing many orders. That led to an increase in manual reviews.

Funk then adjusted the order-velocity rule to keep down his manual review rates, which he says is at 0.7% while his chargeback rate is typically a low .02%.

Tip No. 5: If you're selling high-value products, watch out for triangulation fraud in which criminals buy products with stolen cards to ship to consumers taken in by phony ads.

Brooks also faced another type of fraud in which criminals advertise popular products, like Brooks running shoes, on social media sites at deep discounts. The ads direct shoppers to bogus websites the criminals set up that take the shopper's legitimate credit or debit card payment for the advertised product. The criminals pocket the cash, then buy the product from Brooks using a stolen credit card they had obtained in some way, to keep buyers from complaining.

The shopper gets his shoes, and the consumer whose card number is used sees a fraudulent charge on her statement. She complains to her bank and a retailer like Brooks winds up with a chargeback that not only costs it the value of the sale but also can lead to additional card-processing fees.

Funk says Brooks saw more of this type of attack in the first nine months of 2020 than in all of 2019. When it spots phony sites involved in these scams, it contacts the company hosting the website, such as GoDaddy or HostGator, and files

a Uniform Domain-Name Dispute-Resolution, or UDRP, complaint to have the site shut down. Funk says Brooks has filed about 70 UDRP complaints in the past year against such criminal websites.

The marketplace version of triangulation fraud

In a variation on this scheme, criminals set up shop on online marketplaces like eBay and Amazon instead of on their own websites, then advertise deep discounts to lure shoppers to their storefronts. This is what occurred shortly after the coronavirus stay-at-home orders took effect in March to Gordon Cos., parent of ChristmasCentral.com, which sells holiday decorations.

Chief information officer Nathan Gordon says his chargebacks surged more than 500%. “Each chargeback comes in its own envelope and, all of a sudden, we had a big stack of envelopes,” Gordon says. “It took us three to five weeks to realize the problem.” By then, he says,

Nathan Gordon, chief information officer, Gordon Cos., parent of ChristmasCentral.com

ChristmasCentral.com had lost $20,000-$25,000 worth of merchandise to phony orders.

The online retailer, whose sales are up 130% since mid-March over last year, solved the problem by reviewing all orders in which the bill-to and ship-to address is not the same. In this scam, the criminal buys the item, such as a garden statue from ChristmasCentral.com, using one consumer’s credit card, then sends it to the second shopper’s address to fulfill the order. In this case, the criminals fulfill the order to maintain a good seller rating on a marketplace like eBay, Gordon says.

ChristmasCentral.com, which uses Authorize.net for fraud prevention, normally does not flag orders with different bill-to and ship-to addresses because it gets many large orders from designers purchasing decorations for a store window or a client’s home. In those scenarios, the designer typically uses his own credit card, but ships products to an address not his own.

$25,000

The estimated worth of merchandise ChristmasCentral.com lost to phony orders in a triangulation scam.

Source: ChristmasCentral.com

To counter this triangulation fraud, Gordon first notified eBay, which blocked the criminals from selling on the marketplace. In addition, Gordon now has two employees manually reviewing every order when the billing and shipping address do not match. "It's an added cost to us, and not a fee you want to pay," he says.

Tip No. 6: Adjust your fraud rules to recognize that more consumers are shipping online orders to an address that's different from their billing address.
At the same time, retailers should be aware that a mismatch between billing and shipping address is likely to be more common during the pandemic as consumers go online to buy more gifts, either to avoid stores or because they can't travel and find it more convenient to have an online retailer ship a gift. In some cases, consumers have left their primary residence to live with relatives, for example to avoid a coronavirus hot spot, and ship online orders to the address where they're currently living.

Anti-fraud specialist Signifyd found in April 2020 that the number of shipping addresses per billing address of consumers in its system had gone up by 12%, and by September it had increased by 20%. Thus, behavior typical of someone committing fraud—ordering a product for delivery to an address other than the billing address—is also increasingly common for honest consumers, says Indranil Guha, senior vice president of marketing and alliances at Signifyd, which says it provides fraud-prevention services to some 10,000 online retailers worldwide.

Tip No. 7: Flag many rapid log-in attempts from a single device as suspicious.
Criminals create automated bots that repeatedly attack ecommerce sites, often using stolen email addresses, phone numbers, passwords and other consumer data exposed in data breaches. The automated software uses many combinations of those credentials in rapid succession in an attempt to sign into customer accounts on retail websites, a form of attack called credential stuffing.

One criminal gang cited in a LexisNexis Risk Solutions report used 850 devices, 134,000 email addresses and 61,000 telephone numbers in a recent coordinated attack against five online retailers and a marketplace in the U.S. In this kind of attack, a single device may try repeatedly to log in to an account on a retailer's website, entering data faster than a human could.

65%

The percent of consumers who use the same password on multiple sites.

Source: Google survey

'Many retailers said, 'first, let's get the functionality in place,' and they didn't lead with, 'How do we make sure these transactions are secure?"

— Jeff Sakasegawa, trust and safety architect, Sift

Fraud-prevention technology supplier Sift said in September the percentage of account log-ins that were fraudulent has gone up by more than 378% since March for its retailer clients that sell physical goods online. While Sift did not disclose the average percentage of account log-ins that were fraudulent, a November 2019 study by Signal Sciences, which specializes in protecting web applications, found that account takeover attempts accounted for 29.8% of attacks on ecommerce sites, making it the largest single kind of attack.

70

The number of Uniform Domain-Name Dispute-Resolution complaints Brooks Running has filed in the past year for criminal websites running triangulation scams.

Source: Brooks Running

High-velocity data entry is a tip-off of this kind of fraud, experts says. They recommend online retailers flag rapid log-in attempts from a single device, as that is likely a malicious bot seeking to commit fraud.

Tip No. 8: Evaluate the history of the purchaser's email address for signs that it's being used by criminals to commit fraud.

One way to minimize losses is for retailers to scrutinize email addresses for signs of fraud. When a criminal gains access to a consumer's email account, such as by tricking the consumer into revealing his password in a phishing scheme, the criminal can use that email address repeatedly when creating fraudulent online accounts, often using different credit cards with different billing addresses. One large ecommerce merchant, which was not named, experienced a 40-50% increase in fraud in April from emails associated with multiple billing addresses, according to LexisNexis Risk Solutions, another fraud-prevention provider.

A retailer can leverage a multi-merchant fraud-prevention system to examine many attributes of an email address. That includes whether it's been associated with many chargebacks or refund requests in the past across many retailers, or with shipping addresses in multiple countries, says Rich Stuppy, chief customer experience officer at Kount. All those can be indicators of fraud.

Tip No. 9: Watch for transactions in which there is a great distance between the purchasing devices' IP address and the card's billing address.
LexisNexis Risk Solutions also identified another red flag during the period between April and June 2020: The fraud risk was significantly higher when the IP address of the device being used to make a purchase was more than 1,000 miles from the recipient's billing address. When the distance between those two points was less than 10 miles, the risk was far lower.

Given that fewer people are traveling now, it's less likely than in the past that someone would be far from home when making an online purchase. Criminals using stolen credit cards may be in foreign countries when making purchases, which would account for the distance between device and billing address. The decline in travel makes that distance a more important indicator of fraud during the COVID-19 period.

Tip No. 10: Consider working with a fraud-prevention provider that draws on transaction data from many companies for help in determining whether transactions on your ecommerce site are legitimate.
One reason online retailers will have a harder time determining whether a transaction is legitimate this holiday season is that more of the visitors to their websites are newcomers, rather than customers who are known to the merchant as honest shoppers. Forter says about 30% of traffic to its retailer clients' websites during the COVID-19 period have been from first-time visitors, versus 5-7% before the pandemic.

When a retailer has no history with a shopper, it is more likely to reject a purchase as suspicious. Online retailers are five to seven times more likely to decline transactions from new customers versus shoppers who have purchased before, Forter says. That means retailers likely are turning down at least some legitimate transactions.

Companies like Signifyd, Kount, LexisNexis Risk Solutions and others can spot trends like these because they monitor transactions for many companies, then apply machine learning to identify quickly new risk factors amid the vast amount of data—something humans could not do nearly as well. Among the Top 1000 online retailers in North America, at least 249 work with one of the more than 50 fraud-prevention companies serving the Top 1000.

Two of the most popular of these firms among Top 1000 merchants are owned by big payment card networks: CyberSource, which is owned by

Visa Inc., has 43 Top 1000 clients, and Accertify, a unit of American Express Co., has 25. Like NuData, which is owned by MasterCard Inc., these companies continually scan all transactions on cards of their brand, giving them a global insight into fraud—including by card, address, email address, device and other parameters—that no individual retailer could obtain on its own. That provides a retailer with a layered defense that evaluates many transaction attributes as well as factoring in current fraud trends.

Fraud-prevention providers typically charge either a flat fee or a percentage of revenue. Given the increasing sophistication of criminals targeting ecommerce, retailers may recoup those fees not only by reducing fraud losses, but also by having the confidence to accept more legitimate transactions even though they may have one or another suspicious characteristic.

PAYMENT CARD COMPANIES BUY FRAUD-PREVENTION SPECIALISTS

(Major acquisitions by leading card brands)

YEAR	ACQUIRER	COMPANY ACQUIRED	PURCHASE PRICE
2010	Visa	CyberSource	$2 billion
2010	MasterCard	DataCash Group	$520 million
2010	American Express	Accertify	$150 million
2016	American Express	InAuth	Not disclosed
2016	Visa	Cardinal Commerce	$300 million
2017	MasterCard	NuData Security	Not disclosed

Source: Digital Commerce 360

Tip No. 11: Make the website the primary line of defense against fraudulent in-store or curbside pickup orders, rather than relying on store employees to deter criminals.

One of the biggest changes in retail during the coronavirus period has been the increase in the number of merchants allowing shoppers to pick up online orders outside their stores so that consumers do not have to go inside and risk infection.

A Digital Commerce 360 study found that, while only 6.9% of store-based retailers in its Top 500 ranking of North America's leading web merchants offered curbside pickup at the beginning of 2020, that percentage soared to 43.7% of store-based retailers just nine months later.

That represents more than 100 retail chains that introduced the service in less than a year. They were responding to a surge in customer demand for a safer pickup option—and they may not have had much time to consider the security implications of the new service.

"Many retailers said, 'First, let's get the functionality in place,' and they didn't lead with, 'How do we make sure these transactions are

secure?'" says Jeff Sakasegawa, a trust and safety architect at Sift. "Now they're seeing the consequences of these new methods and how fraudsters can find them attractive."

While there is not yet any data publicly available documenting fraud from curbside pickup, experts like Sakasegawa say the option opens the door to fraud in a number of ways.

First, this kind of order does not require a shipping address since the buyer is picking up at a store. Thus, filters that flag mismatches between billing and shipping address don't help.

Second, with both store employees and shoppers wearing masks and keeping several feet away from each other, it can be hard for the employee to get a look at the driver's license or other ID the person picking up presents to prove identity. Plus, consumers often want their order quickly, giving retailers little time to screen for fraud.

Retailers are doing their best to adapt to a new and difficult situation. Gap Inc., which introduced curbside pickup broadly in August, instructs employees to check the customer's ID through the closed, driver-side window, then put the items into the customer's trunk or back seat (using the passenger-side door to minimize contact.)

Target Corp. only allows curbside orders through its app, a spokeswoman says. That makes it slightly harder for the bad guys who must take the extra step of downloading the app and creating an account. When the customer arrives in the parking lot, Target sends a code to

the app and the customer shows that code to an employee through her car window to verify her identity.

Stop the transaction on the web, not at the store

But that does little to prevent fraud, says Kevin Lee, a trust and security architect at Sift, because it's easy to install a Target app and create an account with one stolen card number, then uninstall the app and repeat the process.

He says Target should carefully examine each transaction when the order is placed online to determine if it's legitimate. And that includes paying special attention to newly created accounts placing orders for high-value items like smartphones that are easy to resell.

"Target likely knows how long it takes a typical user to sign up for an account and then to find and purchase the items they are looking for," Lee says. "If the company notices a person taking these same actions in a significantly shorter amount of time and they are buying a high-risk item, such as a cell phone, they'll want to block that order or at least ask for additional information to ensure it's legitimate."

Told of Lee's comments, the Target spokeswoman responded, "We do take a multilayered comprehensive approach to fraud prevention and that includes when guests are shopping on Target.com or choosing any of our fulfillment options." Neither Target nor Gap would comment on the extent of fraud from curbside pickup. Other retail chains did not respond to requests for comment.

Tip No. 12: Stagger holiday sales over a longer period this year to keep fraud teams from being overwhelmed.

No matter how careful an online retailer is, big surges in online shopping during holiday sales days are likely to stress its fraud-fighting team. That's why experts advise retailers to space out promotions to avoid huge spikes.

"Maybe not every item is on sale every day," says Jeff Wixted, vice president of marketing and client solutions at Accertify. "Spreading the risk over a longer period of time can be beneficial."

That's a dozen tips that can help online retailers protect themselves from the new threats that have emerged in 2020 in the wake of the pandemic. Merchants that implement them will not only be better able to block fraud this holiday season, but also in 2021, whether or not COVID-19 has been conquered by then.

don@digitalcommerce360.com | @DonDavisDC360

SPONSORED CONTENT

Q&A

Creating better experiences for legitimate customers while preventing fraud

An executive conversation with **Kevin Lee,** trust and safety architect, Sift

Cybercriminals constantly adapt and innovate. And 2020 has offered fertile ground to fraudsters. As more retailers go online to sell goods during the pandemic, sophisticated fraudsters are seizing the opportunity. And retailers are struggling to fight it while still providing frictionless customer experiences. To discuss how retailers need to embrace and execute on a strategy that protects against fraud and abuse while reducing friction for legitimate transactions, Digital Commerce 360 spoke with Kevin Lee, trust and safety architect at Sift.

How would you describe the current state of online fraud?

Recently, there have been rapid and significant changes in online fraud. First, we've seen acceleration in the frequency and severity of online data breaches—leading to mass amounts of personal information getting sold on the dark web. New online payment and fulfillment methods have also gained significant adoption. With credit and debit cards, ACH, digital wallets, deferred payments, cryptocurrencies, digital gift cards, buy online pickup in-store (BOPIS), and buy online return in-store (BORIS), cybercriminals have seized opportunities to exploit technological and logistical advances and defraud businesses. And finally, the global pandemic has forced many businesses online, resulting in substantial spikes in fraud rates.

What are the biggest online fraud challenges retailers are facing?

Cybercriminals have become incredibly efficient in recent years, primarily through the use of automation. Rather than manually attempting to defraud businesses one account or purchase at a time, fraudsters have scaled their operations with bots and scripts to overwhelm merchants with a wave of attacks at once. The sheer volume is simply impossible for merchants to manually handle.

This leads to another challenge: protecting against fraud without turning away legitimate customers. Preventing fraud at scale always comes with the unfortunate effect of insulting real customers. This is most evident when merchants apply rules-based approaches to fraud: If they see a rash of fraud coming from a certain country, a merchant may create a rule to block all transactions from that country—including legitimate orders.

What opportunities around fraud prevention can retailers leverage?

Machine learning can be a huge benefit to detecting and preventing fraud while reducing false positives. It's one of the primary ways to fight fraud and ensure that legitimate customers are able to speed through checkout.

More specifically, machine learning allows merchants to create "dynamic friction" within a site or app's experience. By using machine learning to constantly assess risk at every step of the customer journey, businesses can step up or down friction points like needing to re-enter credit card details or engaging two-factor authentication. To build a sustainable, resilient and scalable system, machine learning needs to be the primary tool.

What can retailers do to quickly put fraud-prevention technology in place?

Fraud prevention and business growth are often seen as mutually exclusive concepts, where emphasizing one comes at the expense of the other. But with the right technology and strategy, merchants can create better experiences for legitimate customers while preventing bad actors from committing fraud.

Sift, for example, offers a suite of products that enable companies to both prevent fraud and grow their business. Our Digital Trust & Safety Suite dynamically prevents fraud and abuse through the combination of technology and expertise, a global data network of 35 billion events per month, and a commitment to long-term customer partnerships. Global brands such as Wayfair, Doordash and AirBnB have been successful in gaining a competitive advantage in their markets from using Sift's technology.

sift

Online fraud stops here.

Sift's Digital Trust & Safety Suite is the only fraud prevention solution that puts your business at the intersection of protection and growth—so you can align risk and revenue decisions, and fight fraud without losing customers, money, or momentum.

Features like Dynamic Friction and Insult Monitor reduce false positives, allowing trusted customers to face less friction and frustration whenever they interact with your site.

Drive expansion without burning resources, and continuously improve risk mitigation strategies with in-depth reporting and data transparency.

With real-time machine learning and actionable feedback, your fraud prevention strategy gets smarter by the minute—and you stop fraudsters no matter where or how they attack.

Visit sift.com today to start your Digital Trust & Safety transformation.

Over 34,000 sites and apps trust Sift to deliver outstanding customer experiences while preventing fraud and abuse.

airbnb BIRCHBOX DOORDASH EVERLANE fitbit HARRY'S HelloFRESH Humble Bundle

OpenTable POSHMARK PATREON TOUCH OF MODERN Upwork wayfair Zillow ZOLA

MAGECART: WHAT IT IS AND WHAT YOU CAN DO ABOUT IT

To become targets, retailers don't have to be Magento 1.0 users. Just about any third-party software might inadvertently open a door for hackers.

By James Melton

2020 has been a big year of Magecart attacks on ecommerce websites. And with holidays looming, online criminals are likely to become even more active.

In September, criminals using Magecart techniques attacked about 2,000 ecommerce sites using Magento 1 software—which, according to news reports, was the most massive Magecart attack ever, affecting tens of thousands of online consumers.

The September attack followed attacks on more than 570 ecommerce sites in 55 countries using Magento, WordPress and Shopify software from April 1 through July 7.

DIGITAL COMMERCE 360 RETAIL

In mid-2020, Magecart became a daily occurrence for small to medium-sized ecommerce businesses worldwide, according to a July report from Gemini Advisory, a web security firm.

The Gemini report says more than 85% of the victim sites in the April-July attacks operated using outdated ecommerce platform software from Magento Commerce, the top target for Magecart attacks. The country hosting the largest selection of victimized ecommerce sites was the United States, followed by the United Kingdom and the Netherlands, the firm reported.

Adobe, which owns Magento, ended support for Magento 1 software as of June 30. However, according to CPO Magazine, roughly 95,000 retailers continued using the outdated Magento software as of September.

What is Magecart?

Fraud security experts say Magecart is a fraud-attack methodology used by many criminals worldwide. Magecart is a methodology used in online "skimming" attacks, also known as "form jacking," says Carl Wearn, head of e-crime at cybersecurity firm Mimecast Ltd.

Online skimming is the web version of the card-skimming devices criminals sometimes place on card readers on gas pumps and ATMs. Digital skimmers use malicious code to collect data entered by online shoppers and transfer it to a website controlled by the hackers. The hackers often obscure those sites using geofencing—virtual perimeter for a real-world geographic area—to keep them invisible in specific countries.

Carl Wearn, head of e-crime at cybersecurity firm Mimecast Ltd.

Magecart attacks began at least five years ago when a group began loading online "skimmers" to collect credit card information to vendor software. Dutch online security firm Sansec says it detected the first widespread Magecart attack in 2015. That attack infected about 3,500 online stores. Since then, the Magecart threat has proliferated, affecting thousands more retailers and other companies, such as airlines, that take credit card payments online.

Mimecast's Wearn says the criminals can attack websites by using vulnerabilities in outdated third-party web software that's widely used by organizations to operate payment processes online. Another route is exploiting unsecured application

programming interface (API) calls—a term used to describe information exchanges by computer applications—by injecting malicious JavaScript. JavaScript is a programming language, and programs in the language are called scripts. They can be written into a web page's programming and run automatically as the page loads.

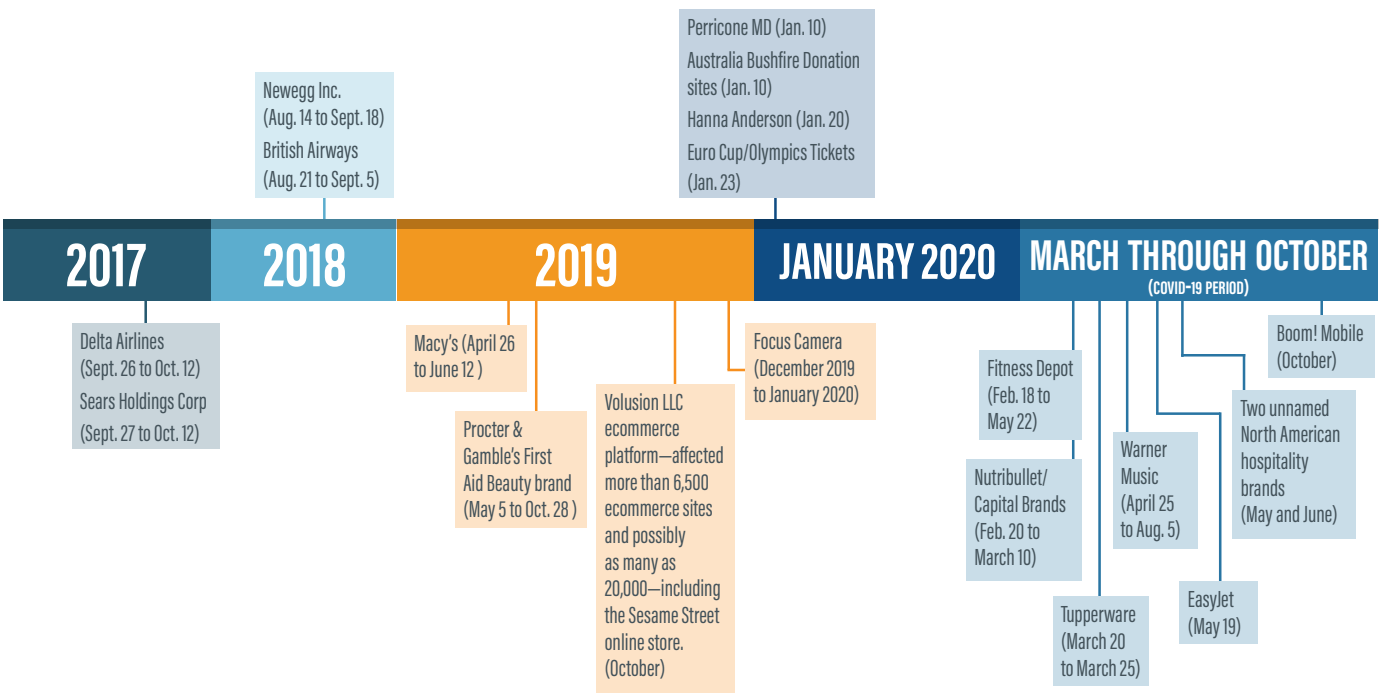
For example, in a 2018 attack on live-event ticket seller Ticketmaster in the United Kingdom, hackers placed the malware by adding it to JavaScript code from a third-party customer support product from Inbenta Technologies. With the skimmer code in place, customers' data to the website went to two servers: Ticketmaster's and one managed by the attackers.

"It interposes and diverts payment/form details, which are then harvested by the threat actor/criminal group. It's a major concern as it's an increasingly common form of attack and has been found on numerous ecommerce sites in the last year," Wearn says.

Magecart can be hard to detect because the malicious script often exists on the client-facing side of a website and waits to skim information as the customer goes through the checkout process.

A TIMELINE OF WELL-KNOWN MAGECART ATTACKS

Time period indicates how long the breach occurred



Sources: Bleeping Computer, Mimecast Ltd., PerimeterX, ZDNet, company statements, media reports

Magecart attacks are hardest to discover when criminals exploit third-party software, Wearn says. In many cases, attacks go undetected for months. “It risks the confidence and trust consumers have in any brand operating online and ecommerce generally, as it directly compromises the otherwise legitimate and genuine website operation of a retailer or vendor,” Wearn says.

And the threat keeps evolving. For example, in August, Visa issued a security alert to its security team about a previously unknown ecommerce skimmer named Baka. It is one of many online skimmer “kits” for sale on underground web forums. Baka, Visa says, uses a “unique loader and obfuscation method.”

The Baka skimmer loads in a way that avoids malware scanners and “uses unique encryption parameters for each victim to obfuscate the malicious code.” It avoids detection and analysis by removing itself from memory when it detects the possibility of detection or when data extraction is complete.

Not just one gang

The Gemini report attributed the April-July attacks to the Keeper Magecart group, which consists of an interconnected network of 64 attacker domains and 73 exfiltration domains—those that move data from one computer to another.

Ido Safruti, chief technology officer, PerimeterX

While groups like Keeper get publicity when they make dramatic attacks, Magecart isn’t the work of just one criminal gang, Wearn says. Experts believe a range of criminal gangs and other threat actors use Magecart methodology, he says.

Ido Safruti, chief technology officer at PerimeterX, a firm that provides security services for websites and mobile applications, agrees that Magecart is not the work of just one gang. It also includes more than one kind of technique, he says.

“Magecart is… an inclusive name for a set of multiple types of attacks that are basically there to skim data from users,” Safruti says. Usually, the criminals take credit card information, he says, but lately, he has seen that expanded to stealing other kinds of personally identifiable information, such as users’ passwords.

Not just a Magento problem

In these kinds of attacks, Safruti says, attackers can breach company servers or the computers of end users by modifying JavaScript code on their browsers, directing the browsers to send payment data to a third-party site. He says attackers insert malicious code into web browsers of users via vulnerabilities in software like Magento 1.0. But Magecart isn't a problem only for Magento users, he says.

"A big portion of the Magecart attacks are not related to Magento. So, you don't need to have a Magento site," Safruti says. Any third-party service could potentially have vulnerabilities that are exploitable by hackers. As an example, he cited the 2018 attack on British Airways, which doesn't use Magento. In that case, he says, attackers exploited a different kind of third-party service.

Criminals have launched Magecart-type attacks on the non-Magneto sites of Macy's Inc., Delta Airlines, Newegg Inc. and others, Safruti says.

What to do

To protect their websites, retailers must be vigilant. That means keeping their software up to date and thoroughly vetting JavaScript from outside vendors, Wearn and Safruti say.

"Organizations need to ensure they are monitoring their website logs and that their web and ecommerce software is updated to the latest version, whether operated by themselves or a third party," PerimeterX's Wearn says.

"They also need to review their scripting policies to ensure only trusted sources/API calls are permitted. There are also products emerging to monitor for this type of attack, but the methodology is constantly evolving," he adds.

Scripting policy refers to programming that defines the ways a system can execute script in specific situations.

Mimecast's Safruti says the level of monitoring needed can be daunting for retailers to do in-house. Some solutions—such as not allowing third-party JavaScript on sensitive pages—can slow down sites or otherwise damage website users' experience. And, he says, those kinds of solutions might not work because hackers can often work around them. He recommends retailers use a vendor that provides real-time monitoring.

Now is the time to act, Safruti says, because hackers looking to exploit the holiday season are currently setting up attacks. And, because of the COVID-19 crisis, many online criminals started ramping up their attacks in March.

james@digitalcommerce360.com | @JDMelton360

SPONSORED CONTENT

Q&A

Outsourcing fraud-prevention solutions reduces costs, builds customer loyalty

An executive conversation with **Isaac Gurary,** CEO, NoFraud

COVID-19 has wreaked havoc across all areas of ecommerce in the past few months—and cybersecurity is no exception. When online shopping spiked dramatically at the start of the pandemic, so did fraudulent activity online—catching many retailers off guard. According to a recent report by LexisNexis, fraud attempts per month in 2020 are up 24.2% compared to 2019, and the cost of fraud for merchants is up 7% since 2019. To discuss how outsourcing fraud-prevention solutions can not only save retailers money, but also foster long-term customer loyalty, Digital Commerce 360 spoke to Isaac Gurary, CEO of NoFraud.

How has the pandemic-related spike in online fraud impacted retailers most?

Many merchants were simply unprepared for it and have suffered as a result. Small and mid-sized retailers often handle fraud-prevention manually—employing one or two people whose task, among other responsibilities, is to identify and review suspicious orders, and then decide if they're legitimate. Manual review can be labor-intensive and time-consuming, so when order volume went up and fraudulent activity increased accordingly, many merchants using this method were overwhelmed. They just didn't have the resources in place to manage that spike.

What are the biggest fraud-prevention challenges retailers are facing?

Trying to handle fraud without professional help is a great risk for most retailers. Fraudsters today are ever-evolving and have learned to evade many popular automated fraud filters that cannot deal with their sophisticated methods. Also, an employee who isn't a fraud-prevention expert usually has a limited ability to determine whether suspicious orders are legitimate or not, and will usually err on the side of caution and decline them. That's problematic because if an order is legitimate, not only does declining the transaction lose that sale, but it also upsets the customer—who is likely to take their business elsewhere and never return.

What are some strategies retailers can implement to address these challenges?

Using an outsourced fraud-prevention partner is most helpful. Retailers should look for a fraud-prevention solutions provider that can increase the approval rate of legitimate transactions, streamline screening operations, and eliminate fraud chargebacks—which occur when the retailer has to return money to a rightful credit card holder whose payment information was stolen and used for a fraudulent transaction.

How can retailers find the right fraud-prevention partner?

The key is to look for a solutions provider that specializes in ecommerce fraud-prevention that has a good track record of accurately detecting fraudulent transactions while increasing their order acceptance rate.

NoFraud's solution, for example, is built around cutting-edge screening systems that simultaneously ensure the absolute highest order approval rate. If we see a high-risk transaction, we won't simply decline it—we understand how hard retailers work on their marketing campaigns and we're committed to never stop a good order from going through. NoFraud will put the flagged order through our highly customized review process with the goal of validating every possible legitimate transaction despite the risk factors that are presented. We also put our money where our mouth is: NoFraud guarantees that if we approve an order that wasn't legitimate, we'll cover the chargeback for the merchant.

Fraud-prevention is a tough job—and certainly one that should be left to experts. When you add up the cost of chargebacks, the loss of valid transactions, damaged customer relationships and resources spent on manual fraud review, the efficiency that a third-party fraud-prevention partner brings to the table pays for itself very quickly.

NOFRAUD

STOP losing money on chargebacks.

SHIP high-risk orders without worry.

SAY goodbye to fulfillment bottlenecks.

How much is ECOMMERCE FRAUD really costing you?

NoFraud uses AI-powered, multi-layered fraud screening technology to eliminate chargebacks and increase your order approval rate with an instant Pass-Fail decision. We guarantee our results with Chargeback Reimbursement.

NOFRAUD

WIN THE FIGHT AGAINST FRAUD FOR GOOD.

Get your free fraud audit at info@nofraud.com.
Learn more at www.nofraud.com

WHAT RETAILERS NEED TO KNOW ABOUT GIFT CARD FRAUD

The coronavirus fueled a surge in digital gift card sales. As a popular gift during the holiday season, gift card sales will only continue to increase. But gift cards are also an attractive product category for criminals. The following article helps online retailers better understand and block fraudulent gift card purchases online.

By April Berthene

Shoppers plan to buy a lot of gift cards this holiday season. And that means retailers will need to watch for more fraudulent transactions.

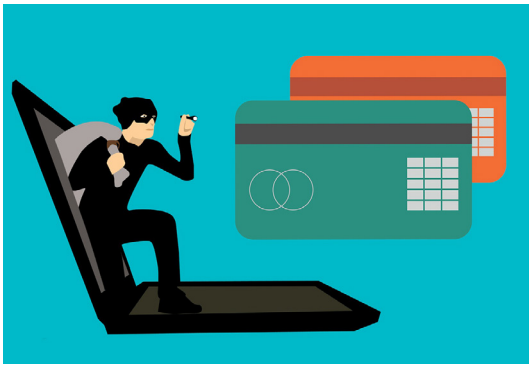
Gift card sales—both physical and digital cards—typically spike during the holiday season.

In Deloitte's annual holiday survey of 4,012 consumers released in October 2020, 48% of consumers (the No. 1 response) plan to buy a gift card—physical or digital—as a gift for the 2020 holiday shopping season. Amitai Sasson, vice present of ecommerce at online retailer

DIGITAL COMMERCE 360 RETAIL

Overstock Art can attest to this first hand. Gift cards purchased through its website generate roughly 10% of sales during the holiday season, compared with 5% during any other season of the year, Sasson says.

And the reason for the increase in gift cards during the holiday season is clear: gift cards make easy gifts for hard-to-shop-for family members. But that also makes them a target for fraud. Gift cards are attractive to criminals for the same reason they are attractive to gift-givers: they're easy. Criminals committing online fraud want to easily turn merchandise into money. This is also why electronics and not apparel is a common product category for fraud. Electronics are often high-value goods that have mass appeal, whereas apparel has to fit and is tailored to consumers with different preferences. Gift cards are the same.



30%

The increase in fraudulent attempts to purchase gift cards mid-March through mid-October compared with January-February.

Source: ClearSale

An estimated 10-25% of fraud attempts on an online retailer's website are to fraudulently purchase a gift card, says Rafael Lourenco, executive vice president, ClearSale. Nearly half of online retailers in the Digital Commerce 360 Top 1000—48.5%—accept gift cards as an online payment method. Retailers have already noticed a spike in gift card sales during the coronavirus pandemic, the holiday season is only going to make gift card sales grow even more. Merchants should be aware of the fraud associated with selling and accepting digital gift cards, and how to prevent it during these high-volumes times.

Why purchasing gift cards online is attractive to criminals

Digital gift cards have mass appeal and can be for any value. Plus, a digital card eliminates the multiple steps of having to acquire a physical good, like a smartphone, tricking a consumer into buying it and then shipping the product to the consumer. Instead, a criminal can purchase a digital gift card with stolen credit card data, resell that gift card to a consumer and pocket the cash without ever touching merchandise. This also makes the criminal harder to trace because the criminal does not need to provide a physical shipping address.

"A gift card is a perfect way for them to buy it and then they can turn it into money quickly and it

'In these times, if you know how to handle the gift card program it could be a huge growth engine for your business.'

— Yair Miron, CEO, Rise.ai

doesn't have to be delivered to another address," Lourenco says.

Plus, legitimate gift card marketplaces already exist—such as Raise.com—where consumers can buy and sell partially used or unwanted gift cards at a discount. Criminals can go to these places and pose as normal consumers to try and easily sell the gift cards they fraudulently acquired.

In addition, large retailers often let consumers transfer gift cards into cash, making it even more attractive for a criminal to purchase a gift card.

Gift cards sales and fraudulent gift card sales grow during the pandemic

U.S. retailers sold 114% more digital gift cards in the third quarter of 2020 compared with Q3 2019, according to survey data from 1,182 U.S. stores that use Rise.ai Inc.'s re-engagement software. Plus, the revenue from selling the digital gift cards increased 65% year over year in Q3, according to Rise.ai, which helps retailers manage gift cards, loyalty programs, referrals and refunds. The data does not include Amazon gift cards nor multi-store gift cards, such as a gift card that could be used at more than one store. For example, a parent brand like Gap Inc. could offer a gift card that could be used at Gap, Old Navy and Banana Republic.

Digital gift card sales are growing during the pandemic for a few reasons, such as consumers purchasing them to support local businesses, and consumers avoiding both in-store shopping and using cash as a form of payment, according to Rise.ai. Merchants also helped fuel the increase in digital gift card sales during the pandemic, as many were keen to market gift cards while their stores were closed or overall sales were hurting, as a way to keep revenue flowing in, says Yair Miron, CEO at Rise.ai.

Online retailer overstockArt.com also noticed this increase in gift card sales in 2020. During the pandemic, overstockArt.com's online sales have roughly doubled year over year, and online gift card purchases have at least doubled, Sasson says.

"We've already seeing more gift card sales than ever before," he says.

ClearSale, a fraud prevention software, also saw the increase in gift card purchases from the 3,000 clients that use its software, with gift card purchases increasing 138% from March 15 until mid-October.

But with the increase in gift card sales also comes an increase in gift card fraud. The attempts to fraudulently purchase gift cards increased 30% during that period, ClearSale says.

How to detect and prevent gift card fraud

Criminals fraudulently purchase gift cards like other physical goods, in which they use stolen credit card information to make the purchase or they take over a consumer's account and purchase. With account takeover fraud, a criminal logs into a legitimate consumer's account on a retail website using stolen username and password information.

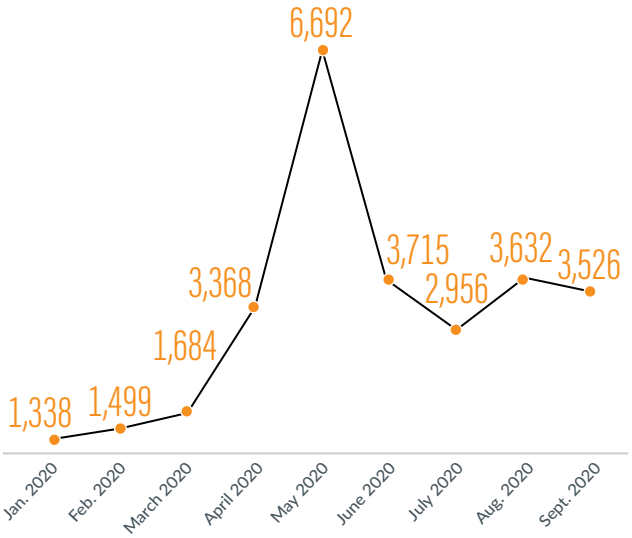
Once in the account, the criminal may see that the consumer already has a gift card saved to her account, or has enough loyalty points to purchase one. This is the best case scenario for the criminal, Lourenco says, because then the criminal can steal the gift card without having to use any additional stolen credit card information, and save that information for another nefarious transaction. He could also purchase the gift card using the account's saved payment credentials.

"Because people tend to reuse the same or similar passwords across all their online accounts, when a seemingly innocuous breach occurs at one company, it makes all the other accounts secured with those credentials vulnerable to attack," says Pattie Dillon, anti-fraud network relationship manager at fraud prevention vendor SpyCloud. "Criminals can buy breached information in underground markets then use it to attempt logins across thousands of accounts, gaining access to any that use the same login and password."

A good place to start to block fraudulent digital gift card purchases is with fraud prevention software.

PANDEMIC FUELS GIFT CARD SALES

Number of U.S. gift cards sold on e-retailer websites, on average per retailer



Source: Rise.ai, 1,182 U.S. stores

Vendors typically charge online retailers based on their online transaction or sales volume. ClearSale, for example, says its rates are determined for each merchant based on a percentage of their gross merchandise volume, which in most cases is lower than 1%, the vendor says.

Many retailers have fraud prevention software or an in-house team to help flag fraud on all of their ecommerce purchases. Many of these follow an established set of rules tailored to that merchant that will mark a transaction as potentially fraudulent. Before the purchase is approved, the retailer or the vendor will look into the flagged transaction further, such as manually reviewing more details about the purchase or making the customer confirm her identity, such as with a text message.

Common rules a retailer may have to flag fraud are if the billing and shipping address don't match, or if the transaction is a lot higher than average, such as $2,000.

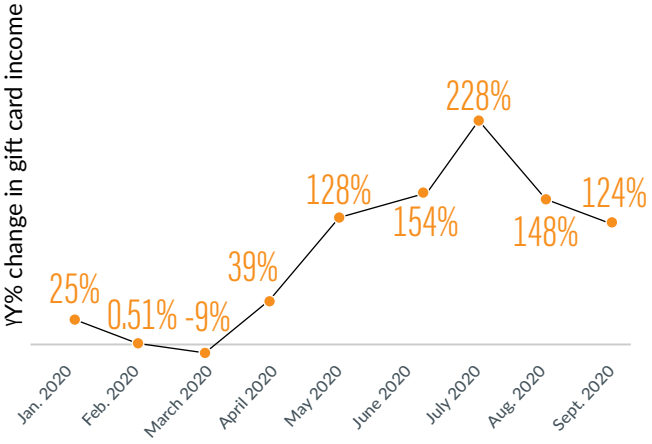
Like with other fraudulent transactions, retailers should look for signs that the purchase is not from a normal consumer, such as a transaction for a $1,000 gift card or a transaction in which the user is quickly trying many different credit card numbers before one is accepted, Miron says.

But retailers should also have a separate set of rules for gift cards because the products are much different than normal merchandise, ClearSale's Lourenco says. For example, a digital gift card will always have the same billing and shipping address. Because the retailer is not shipping a physical product, the criminal can use the stolen credit card's billing and shipping address to circumvent this rule.

"You need a clear understanding that the gift card purchase is not the same thing as your other purchases," Lourenco says. "You cannot have the same rules or polices or algorithm for fraud. You shouldn't just replicate the very same scenario, the very same rules. You've got to treat these transactions as separate."

MERCHANTS RECEIVE MORE REVENUE FROM DIGITAL GIFT CARDS AS THE PANDEMIC CONTINUES COMPARED WITH 2019

Year-over-year percent change in income U.S. retailers receive from digital gift card sales



Source: Rise.ai, 1,182 U.S. stores

'You need a clear understanding that the gift card purchase is not the same thing as your other purchases.'

— Rafael Lourenco, executive vice president, ClearSale

Instead, merchants should have additional fraud-flagging rules that account for criminal patterns more associated with gift cards than for physical goods. For example, a common fraud indicator is if the IP address of the customer is a long distance—such as 1,000 miles or in another country—from the shipping address. Because there is no shipping address for a digital gift card, instead, merchants should match the IP address with the country of origin of the credit card, Miron says.

OverstockArt.com also adjusts its fraud rules for gift card purchases. When a shopper purchases a gift card on overstockArt.com, the buyer can send it via email to the recipient. Then OverstockArt.com has an email address affiliated with that digital gift card. If the consumer then tries to redeem that gift card with a different email address, the retailer will then manually review the transaction before approving it, Sasson says. Often, it is just a family member redeeming it and so it's OK to approve, he says, but its internal review team still needs to check the transaction for fraud markers.

Another gift-card-focused fraud rule adjustment retailers can make is to the monetary value rule. Criminals may know that a high value transaction may be a fraud indicator so instead of purchasing one $1,000 gift card, they will purchase 50 $20 gift cards with 50 separate transactions. That way the purchases are not flagged for fraud, as a $20 purchase is not considered risky.

If a normal consumer, however, wanted many small gift cards, she would likely purchase them all in one transaction and not spread out her purchases. Retailers can adjust their fraud rules to look for a pattern within small gift card purchases. It will likely be impossible to catch the first couple of small gift card transactions, but after a small number, the criminal will repeat some element, and that's when a retailer can catch and block the transaction, Lourenco says.

DIGITAL COMMERCE 360 RESEARCH

RESEARCH MEMBERSHIPS

We created Digital Commerce 360 Research Memberships to give our readers exclusive access to our extensive collection of research and data. This includes everything from our published research reports, to strategic gated content, key charts and graphs, and access to the data behind the analysis.

LEARN MORE

"With those multiple transactions, maybe even with multiple credit cards, there will always be something in common. Either the time, like they are buying one after the other, or they are on the same IP address, or the email address," he says. ClearSale also has propriety technology to know the device the consumer is using, Lourenco says.

As always, experts express that just because a transaction may be flagged as possible fraud, that does not mean the retailer should automatically decline it. These orders very well may be legitimate, and if a retailer automatically declines it, it loses the revenue from that sale and creates an unhappy consumer.

10-25%

The average portion of blocked fraud transactions that are used to purchase gift cards.

Source: ClearSale

Instead, if a transaction could possibly be fraudulent, retailers should then have a manual review process so a staff member can further look into the transaction.

How gift card fraud can bite retailers twice

Retailers should be extra vigilant about blocking fraudulent digital gift card transactions because it could be more damaging than a typical fraud transaction.

The retailer incurs a loss when criminals purchase digital gift cards with stolen credit card data. The consumer will realize that the transaction on her credit card account was not made by her and will contact her bank to reverse the charges—known as a chargeback. At this point, the retailer has lost that money, and the fraudulently obtained gift card is now in the marketplace. A real consumer will likely purchase it (the criminal will keep the money) and then she will go on to try and make a purchase using it with the retailer.

The retailer will either block the transaction, as it knows the gift card is illegitimate, it may accuse that shopper of being the criminal as she is paying with the criminally obtained gift card, or the retailer will let the transaction go through and then be out the cost of the merchandise. None are ideal scenarios. This is why it's best to try and block the initial fraudulent transaction so the digital gift card is not out in the market.

Retailers should work with the secondary gift card marketplaces, as the sites are typically willing to work directly with merchants to prevent fraudulent gift card transactions on both websites, SpyCloud's Dillon says.

Another way a digital gift card can be doubly hazardous for a retailer is if it does not have the technology in place to have all of its systems sync in real time. A criminal may know this and then use the digital gift card code multiple times just on different devices, and the retailer approves all the transactions as it doesn't know yet that the card should be marked redeemed.

While Miron says these scenarios are certainly frightening, he and other fraud experts warn that the solution is not to eliminate selling gift cards. Instead, retailers should implement these strategies and work with technology partners to safely grow this channel of their business.

"Gift cards offer a very unique opportunity for retailers around the world," Miron says. "Amazon, Target and bigger brands invest so much in gift cards. There is a reason they are the most popular product. In these times, if you know how to handle the gift card program it could be a huge growth engine for your business."

april@digitalcommerce360.com | @ByAprilBerthene

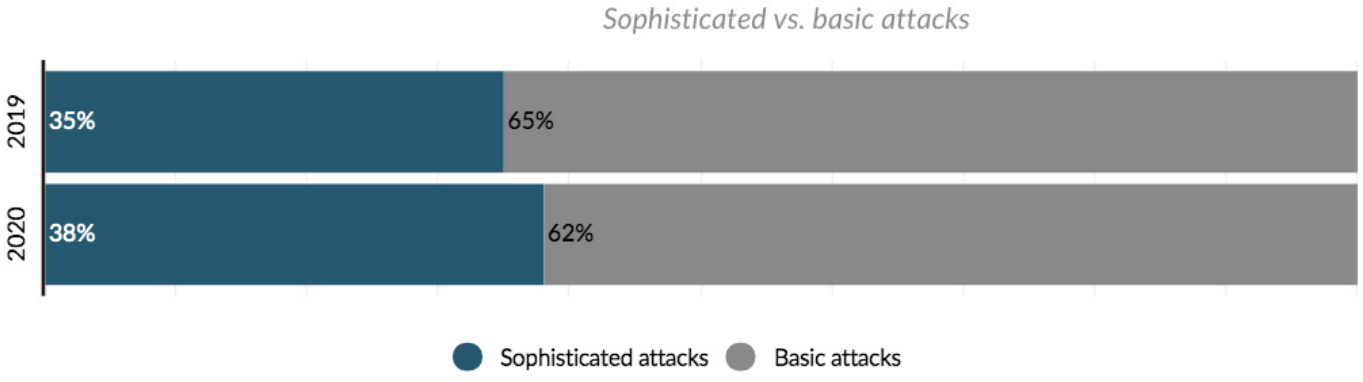
SUCCESSFUL ECOMMERCE FRAUD ATTACKS ARE ON THE RISE

Online fraud attacks have increased across business size, according to LexisNexis. Plus, fraud channels have shifted with an increase in delivery and in-store pickup fraud, according to insights by NuData.

By Tabitha Cassidy

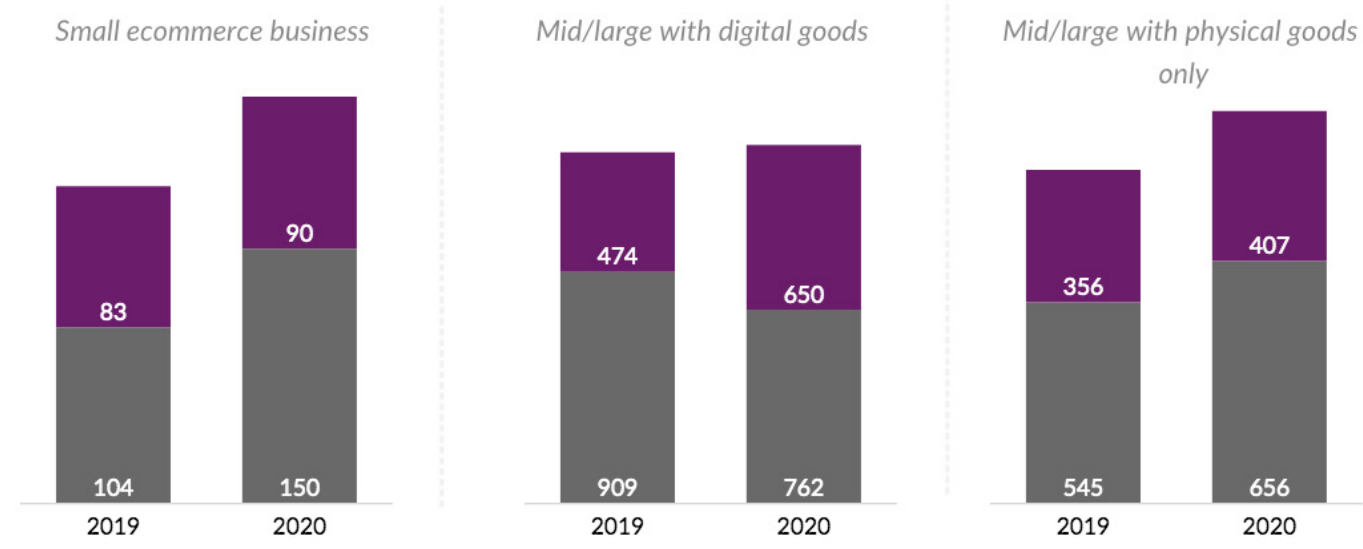
DIGITAL COMMERCE 360 RETAIL

Ecommerce retailers experience more sophisticated attacks in 2020

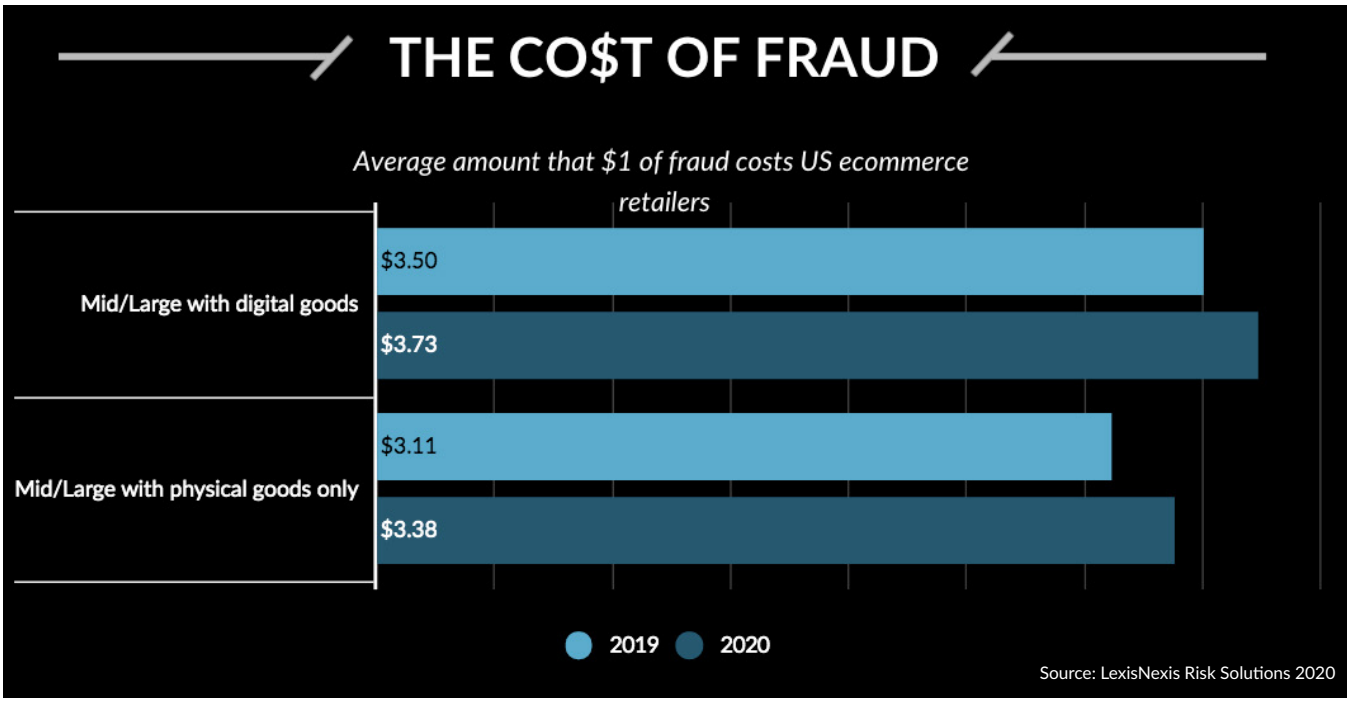


Source: NuData 2020

Successful fraud attacks increase across all ecommerce business sizes



Source: LexisNexis Risk Solutions 2020



Chargeback fraud dollar value increase pre- and post-COVID-19 lockdown

Percent increase of total chargeback fraud dollar value by channel from pre-lockdown (January-March) to post-lockdown (April-May)*

Source: NuData 2020

"A lot of fraud has really shifted channels..."

"The pandemic is really driving a lot of these changes. A lot of fraud had been occurring previously in store with card transactions. With the pandemic and within the various shutdowns around the world, you've seen in-store transactions drop off significantly. They were replaced with ecommerce transactions: either buy online pickup in store or curbside pickup, or through some mechanism delivery. A lot of fraud has really shifted channels and that's really increased the amount of goods and those dollar values of online transactions."

—Robert Capps, vice president of marketplace innovation at NuData Security

*A chargeback is a reversal in costs of an item initiated by a consumer and approved by the shopper's card-issuer. Retailers have to pay chargeback expenses. Card issues often penalize retailers with a high rate of chargebacks.

DIGITAL COMMERCE 360 RETAIL

Account takeover attacks at login are majority of fraud traffic

Source: NuData 2020

Ecommerce login attempts with correct credentials

"Attacks at login use combinations of usernames and passwords, many of which are incorrect. Attackers deploy mass-scale attacks at login, such as credential stuffing, to test those credentials and determine which combinations open an account, known as hits."

—NuData Security
2020 H1: Fraud Risk at a Glance report

1.18%

of ecommerce login attempts had the correct credentials.

Source: NuData 2020

Myth or Fact?

The holidays lead to more online fraudulent transactions. Anecdotally, fraud-fighting professionals have often said that fraud spikes around the holidays. But is that true? We asked the experts for their take.

DOES FRAUD SPIKE FOR ONLINE RETAILERS DURING THE HOLIDAYS AND WILL IT FOR THE 2020 HOLIDAY SEASON?

"The 2020 holiday season will be record breaking for online retailers. The pandemic has pushed online commerce a decade forward into the future. The record numbers will definitely scale accordingly in fraudulent transactions. If your business is susceptible to fraud, I would recommend setting up automated services to alert you of any possible fraudulent activities. Unfortunately, fraud is not the only malicious activity on the rise during the holidays, malware attacks and most notably ransomware attacks are also on the rise as attackers know that every minute your site is down costs you ten-folds during this time of the year."
— AMITAI SASSON, Vice President of Ecommerce at online retailer OverstockArt.com

"While credit card fraud has always been a challenge for online retailers year-round, the holiday season is often when retailers are most vulnerable. Retailers are typically overwhelmed with order volume and may not be paying as much attention to fraud prevention. The more sophisticated fraudsters will strike when defenses are down, hoping their attempts will not be detected. Since COVID-19, fraud rates have soared, so we expect this holiday season to be a particular tough one in terms of fraud attacks."
— SHOSHANAH POSNER, Director, Business Development, NoFraud

"My gut feeling about a fraud spike during the holiday was to say yes, there is one. After looking through my data though, there is not a significant difference in fraud during the holidays for us. Neither in fraudulent declines nor chargebacks. That said, fraud tends to come in waves as organized fraudsters target a given company. If you decline enough of their orders, they will look somewhere else. Fraudsters want a good ROI for their time, just like corporations. "
— CHAD FUNK, Specialist, Brooks Running

"In the past, Sift has seen noticeable spikes in attempted fraudulent purchases during the holiday season. In 2019, for example, we saw payment fraud attempts climb more than 40% at the beginning of November and spike 25% during the week of Cyber Monday. This year, the holiday shopping season truly started earlier, with Amazon Prime Day kicking things off in mid-October. This season we're already seeing several smaller spikes in fraud attacks rather than larger, distinct peaks like we have in years past because holiday sales are more spaced out. It's likely that we'll see elevated rates of payment fraud spread throughout the remainder of the year, in parallel with the longer shopping season. Fraudsters track sales just like deal-hungry shoppers to blend in during peak shopping times. This year they'll have more opportunities to do just that."
— JEFF SAKASEGAWA, Trust and Safety Architect, Sift

DIGITAL COMMERCE 360 RETAIL

ABOUT US

Digital Commerce 360 Retail

Digital Commerce 360 Retail provides business intelligence and editorial content on the global online retail market through our research and topic focused reports on recent retail trends, technologies, industry best practices and more. Distribution: 34,000 + opt-in subscribers, retail newsletters and on the website. Sponsorships include thought leadership articles, promotion and guaranteed leads. These exclusive reports are available only via registration download, providing qualified leads to sponsors.

Digital Commerce 360 Digital Commerce 360 is a leading media and research organization that delivers daily news and competitive data across e-retailing, B2B ecommerce, and digital healthcare. Building on the reputation of Internet Retailer® which we introduced in 1999, Digital Commerce 360 is an expert in digital strategies and publishes a wide range of products including reports and newsletters, Internet Retailer® magazine, webinars, and data on thousands of global ecommerce companies through its Digital Commerce 360 Research brand. In 2018, we also co-founded B2B Next, the premier conference for B2B executives embracing ecommerce.

COPYRIGHT