internetRETAILER®
DECEMBER 2019 | DIGITALCOMMERCE360.COM/IR

A LOOK AT THE YEAR AHEAD

a publication of
DIGITAL COMMERCE 360

RETAILERS ADAPT TO RISING FRAUD RATES

Merchants need to ensure they have safeguards in place to filter fraud.

BY APRIL BERTHENE

Bonsai plant retailer Stilyo in November 2016 received its largest order to date: 100 levitating air-floating bonsai pots that cost $17,499.

Because the 2-year-old retailer had never experienced any significant issues with fraud, it shipped the order without conducting any background checks, says CEO Eric Haim. That was a mistake: Stilyo received a chargeback from the purchaser's credit card a few days after the package was delivered.

"The money was gone," Haim says. "As a new business owner, we didn't have any spare money and the business took a huge hit." The situation drove Haim to buy fraud-prevention software and put processes in place to avoid falling prey to criminals.

This is a lesson online retailers often learn the hard way. And the problem is getting worse. Fraud is up 40% this year among retailers with at least $10 million in annual online sales, according to the annual "LexisNexis Risk Solutions 2019 True Cost of Fraud Study." The report is based on a survey of 700 U.S. risk and fraud executives in retail and commerce.

There are multiple reasons behind the rise in fraudulent transactions, including a slew of data breaches that have made stolen customer information relatively easy for criminals to procure, as well as criminals who are frequently changing their tactics. The situation is driving many retailers to take a multipronged approach to keep fraud at bay that includes using software and fraud prevention vendors' technology and updating their business policies and procedures.

40%

The percentage that fraud increased in 2019 year over year for online retailers that sell physical goods and generate at least $10 million in online revenue.

Source: LexisNexis Risk Solutions 2019 True Cost of Fraud Study

STILYO BEGAN WORKING WITH FRAUD PREVENTION SERVICE NOFRAUD in the first quarter of 2017. The vendor uses a set of rules to flag potential fraud. For example, NoFraud's system will investigate a shopper who required multiple attempts to enter her credit card information or tried multiple card numbers.

NoFraud takes a 0.4% cut of Stilyo's orders that it evaluates, and it provides insurance on orders that are less than $1,000. Stilyo evaluates the small number of orders that exceed $1,000 on its own. It requires those shoppers to authenticate their purchases by uploading a picture of themselves with a government-issued ID, credit card and some indicator of the date, such as a newspaper. Stilyo's staff then evaluates the images to ensure the customers are who they say they are.

Roughly 25 orders per year require that additional layer, Haim says. Most shoppers with larger orders will authenticate with a photo or will call into customer service for help or to ask questions, such as why it is necessary. While some have abandoned the order after this pop-up window, that's OK with Haim because that suggests they may have attempting to place a fraudulent order.

A MAJORITY OF SHOPPERS understand they may have to verify their identity when they shop online, according to a 2019 Digital Commerce 360 and Bizrate Insights survey of 1,110 online shoppers. 69% of shoppers have never had a problem typing in an identity code a retailer has sent them, although 5%

'The money was gone. As a new business owner, I can tell you that we didn't have any spare money and the business took a huge hit. After that, we learned that we had to have software.'

—Eric Haim, CEO of online retailer Stilyo.com

of shoppers find the process frustrating and 2% abandon their purchase rather than enter the code. (The remaining shoppers selected another response.)

Similarly, 79% of shoppers understand that retailers are trying to prevent fraud when they ask them a security question, according to that same survey. 16% of consumers find security questions annoying and 5% often leave the site when presented with a security question. (The remaining shoppers selected another response.)

NoFraud's fraud-prevention software has helped Stilyo keep fraudulent transactions in line with its sales, Haim says. Stilyo's online order volume increased 54% year over year in 2018, and the number of its fraudulent orders grew about 57%, he says.

Haim doesn't expect to see any surges in fraud in the near future, as long as the software keeps pace with criminals and adapts its tactics as the criminals do. But that isn't easy. Criminals are on a relentless quest to deploy new methods to steal identities and con retailers. For example, Signifyd recently identified and squashed a bout of romance fraud that occurred for a few of its clients in the second quarter, says J. Bennett, the fraud protection vendor's vice president of operations and corporate development.

After significant research, Signifyd identified dozens of elderly women who were duped into purchasing expensive products, such as precious metals, electronics and camera equipment, from online retailers. Once the products arrived, the women sent these items to their romantic interests, who were criminals living in Malaysia and Nigeria.

One of those women called her credit card company to issue a chargeback to recover her lost money after she realized the relationship was a scam. Within a month of that call, Signifyd identified and shut down the crime ring. The vendor is now working with the FBI to find the criminals. Bennett says less than 100 of its retailer clients were affected, without revealing specifics, and about $1 million in goods were stolen from just Signifyd's merchant network. (Read more about romance fraud on page 28.)

This type of fraud, in which an actual customer paid for a product and requests a refund from the credit card issuer, is called friendly or first-party fraud. While this could be everyday people scamming retailers for free products, the complex romance fraud would also fall into this bucket. Friendly fraud accounts for 39% of medium and large ecommerce retailers' fraud losses, according to the LexisNexis survey.

ANOTHER REASON FRAUD CONTINUES TO GROW despite improving prevention technology is the vast number of data breaches.

Data breaches are "100% cyclical" because of their residual impact, Bennett says. For example, financial services institution Capital One announced in July that a hacker

'Digital card skimming is easier, lower risk and more lucrative for the hackers than other types of card theft.'

—Jason Glassberg, co-founder, Casaba Security

accessed data on 100 million U.S. customers and 6 million Canadian customers, and accessed more than 140,000 Social Security numbers, 1 million Social Insurance numbers for Canadian customers, and 80,000 linked bank account numbers.

Criminals can use this stolen information to establish false identities or sell the information to other criminals to do the same. This type of fraud, which is referred to as synthetic identity fraud, accounts for 36% of fraud losses for medium and large ecommerce retailers, according to the LexisNexis study.

The Capital One breach is far from rare. For example, online marketplace Poshmark in August announced that unauthorized users may have accessed customer data that includes their user names, cities and emails. Two months later, Bed Bath & Beyond Inc. announced a hacker acquired email addresses and passwords for less than 1% of its online account holders between Sept. 4-27.

Even though shoppers may have changed their password to their Poshmark or Bed Bath & Beyond accounts, hackers could test if they used the same credentials for other accounts or use some of their personal data to authenticate other fraudulent purchases. Consumers reusing passwords is a common way criminals commit fraud, says Mike Lloyd, cyber security firm RedSeal Inc.'s chief technology officer.

"It's important to realize that if you use the same password at your bank as you use for less important services like social media or video streaming, then a bad guy only has to break into whichever company has the weakest security, then steal your passwords and use them everywhere else you go," Lloyd says.

The hacker could also take the account information it stole, change the payment credentials or the shipping address, and then make purchases under a "trusted" account to prevent the retailer from distinguishing between the consumer and the criminal, Bennett says. This type of account take over fraud accounts for 7% of fraud loses for medium and large ecommerce retailers, according to the LexisNexis study.

Although it is not always disclosed, data breaches on ecommerce sites often occur because of digital card skimming. This is where criminals inject malware onto ecommerce websites and steal information when shoppers enter it on the site. The technique is growing because of its subtlety and effectiveness; criminals infect vendors, such as review software or a platform with digital card skimmers, and not the ecommerce sites themselves. The malware is then pushed out to all of the sites the vendor services.

"Digital card skimming is easier, lower risk and more lucrative for the hackers than other types of card theft because they can hit hundreds or thousands of websites with a single data breach—and usually these

third-party suppliers have weak security," says Jason Glassberg, co-founder of Casaba Security.

Digital card skimming is one part of a broader shift in fraud moving online thanks to the now-widespread use of EMV chip-and-pin technology in the United States at payment terminals in stores to secure payment. These chips make it far harder for cybercriminals to access payment data. Chip-to-terminal connections are far more secure than running a card stripe at a store.

Retailers' websites and apps are easier to permeate than their offline presences because they often have more entry points than a store with its one point-of-sale system, says Tan Truong, chief information officer at fraud prevention vendor Vesta.

Not all retailers' defenses rely on cutting-edge technology. For example, when a merchant's system flags a transaction as possible fraud, the retailer can call the customer to see if the transaction is legitimate. Retailers that sell expensive products, such as camera equipment, can mask the call as customer service and talk about the shopper's plan for the equipment and possible maintenance, Bennett says. This way, the call is seen as "high-touch" customer service, and not trying to determine if the person on the other end is using stolen credit card credentials.

Online retailers Auto Accessories Garage and To the Cloud Vapor Store both call shoppers with red flags to vet potentially fraudulent transactions.

At To The Cloud Vapor Store, which sells vaporizers and vape-related products, the retailer uses its own rules to assign red flags to an order and then determine in house if an order is fraudulent, says owner Tyler Browne. Browne estimates it has about 30 fraud attempts each month, out of about 500 transactions, and one to two of those will result in a chargeback, he says. In a year, maybe 6% of orders are fraud attempts, and it blocks 5.5% of those, meaning only about 0.5% of fraudulent transactions aren't thwarted, he says.

About 80% of the fraud attempts are from foreign buyers who are either trying to ship products via a freight forwarder, which is a location that ships a package on to another location, he says. That's why Browne set up rules that alert him if a transaction is made where the billing and shipping address don't match, or if a shopper makes a purchase with a non-U.S. credit card. Then, of these transactions, Browne will search for further red flags and work to verify the purchase. For example, he doesn't approve the transaction if he can identify that the shipping address is a freight forwarder. The purchaser is likely using the freight forwarder to mask his location and use a U.S. address that is more likely for software to approve, he says.

Browne looks for additional red flags for consumers using credit cards issued outside the United States. For example, if a shopper is trying to make the same transaction multiple times in a row, or if a shopper's IP address is in Texas, shipping address is to Florida and credit card was issued in Chile. When a transaction ticks one of those boxes, he'll call the consumer's phone number. If he can reach the consumer and verify the person is legitimate, he will approve the transaction. But he often declines the transaction after finding the number provided is disconnected.

Auto Accessories Garage also takes a closer look at foreign transactions for fraud because it only ships orders within the United States.

356

The number of fraudulent transactions per month, for online retailers of physical goods with sales greater than $10 million annually

Source: LexisNexis Risk Solutions 2019 True Cost of Fraud Study

The heartbreaking rise of romance fraud

Romance fraud is on the rise.

Romance fraud occurs when criminals prowl dating sites to impersonate suitors and forge romantic relationships, often with older women, says J. Bennett, vice president of operations and corporate development at fraud protection retailer Signifyd Inc. The criminals then build the women's trust over the course of months or, sometimes, years.

Once the criminals establish trust, they convince the women to send them expensive gifts. The criminals' explanations for why they need physical goods include such things as they are stationed in Iraq or they moved to Kenya to become a businessman.

At some point the criminals typically ask the women to buy gifts using the criminal's credit card credentials, which are stolen cards. Sometimes the criminals have the victims ship the goods to themselves, and then provide a shipping label they can use to forward the goods onto the criminal. Some of the criminals set up their own online stores to sell the goods they have stolen.

Reports of romance fraud have doubled from 2015 to 2018, according to reports from the Federal Trade Commission. More than 21,000 incidents of romance scams were reported in 2018, with consumers reporting a loss of $143 million. This is up from 2015, with 8,500 reports totaling $33 million in losses.

Signifyd recently uncovered a surge in romance fraud that occurred among a few of its online retailer clients, Bennett says. The vendor uncovered the fraud after one of the victims realized her relationship was a scam and she called her credit card company to issue a chargeback to recover the lost money. The retailer then turned to its fraud prevention provider, Signifyd, to investigate. This was about 14 days after the transaction.

Signifyd's data analysts spent about a week examining the transaction's attributes to determine what happened. During this period, more victims filed claims, which gave Signifyd more transactions to analyze with similar patterns, Bennett says. Ultimately, it identified dozens of women who were duped into purchasing expensive products, such as precious metals, electronics and camera equipment, from online retailers, and sending those items to criminals living overseas, often in Malaysia and Nigeria in this case.

The victims shared a number of common traits before they went on a spending spree. They had "clean data," which meant most fraud prevention wouldn't flag their transactions because they lacked any suspicious signs. For example, not only were the typical payment details accurate, but so were their email and IP addresses.

Signifyd worked with its merchant clients that had chargebacks from purchases that it had marked as legitimate to "reverse engineer" the problem. In some cases, Signifyd or the merchant called the victims to learn more about the transaction, what they bought and why they had filed the chargeback.

Once it uncovered the romance fraud scheme, it developed new rules in which it blocked purchases from older women living in certain areas in Texas on retailer sites that sold precious metals, cameras and consumer electronics. During a two-week test, Signifyd saw that blocking one transaction, a shopper tried to buy a similar product on another retailer's site that's also within Signifyd's network. This gave Signifyd the confidence that it knew it was right.

A month after the first chargeback occurred, Signifyd had indented and shut down the fraud. It is now working with the FBI to find the criminals. Bennett says fewer than 100 of its retailer clients were affected and about $1 million in goods was stolen from just Signifyd's networks.

"Occasionally, we have a customer shopping while abroad but, in general, overseas activity is a big red flag for fraud," says Rick Bentson, the retailer's director of operations.

For traffic that visits the retailer's website, AutoAccessoriesGarage.com, from a foreign country, it will show that purchaser a "challenge page," such as a captcha page, in which a consumer is presented with an easy task like identifying street light images to determine if she is a human. The retailer uses fraud security vendors coupled with its own policies to thwart fraud.

Another way To the Cloud Vapor Store verifies if the consumer is a legitimate customer or a criminal is by looking at the purchaser's internet history, such as having an active Facebook page or LinkedIn account.

"You can tell if it's real or not," Browne says. "You just decide how good you feel about it. If you've been doing this for years, there are definitely patterns."

Of the 0.5% of transactions that result in a chargeback for To the Cloud Vapor Store, many are purchasers claiming that they didn't receive the item even though To the Cloud Vapor Store requires a signature upon delivery, Browne says.

For those transactions, it is unlikely the retailer will be able to filter them out on its own without fraud-protection software. However, Cloud Vapor doesn't plan to invest in fraud-protection software.

"It's too expensive for the small amount [of fraudulent orders] that we receive," Browne says.

WHILE STARTUP RETAILERS MAY USE THIS SIMILAR APPROACH of doing the best they can with what they have, many retailers, like Stilyo, have gotten burned. These retailers have determined that they need to have software and now use a combination of software and internal policies.

Stilyo, for example, knows based on its previous experience, that an order is five to 10 times more likely to be fraudulent if the purchaser clicked to its website via social media compared with a search engine, Haim says. With a social media ad, the retailer is creating an audience and reaching out to consumers who may be interested in its products and who the brand is relevant for. "If I have a stolen card, I'm going to go as fast as I can to find whatever it is I want to buy and get it," Haim says. Therefore, once its software flags a transaction, the retailer will consider how the consumer arrived at its site into its approval or denial process.

At Auto Accessories Garage, the retailer attaches its in-house-developed "fraud score," or the likelihood an order is fraudulent, to each order based on common red flags and a mix of customer information and specific products. For example, the retailer knows criminals may target universal auto accessories because they are easier to resell than vehicle-specific items, and so those products increase that order's fraud score, Bentson says. If that score exceeds a certain threshold, then its one in-house fraud specialist will research the order and possibly call the purchaser, he says.

Criminals will not stop looking for opportunities to exploit shoppers and ecommerce retailers. Retailers know it's impossible to block all fraud. But, merchants need to stay on top of best practices, including evaluating their internal prevention polices and keeping their software up-to-date, to keep fraudulent transactions from growing. iR

APRIL@DIGITALCOMMERCE360.COM | @BYAPRILBERTHENE

Robust fraud prevention strategies help retailers decrease chargeback, increase sales

KC FOX
senior vice president of technology services, Radial

Incidents of ecommerce fraud have been steadily rising over the years and continue to worsen. According to the LexisNexis Risk Solutions report, retail fraud attempts have doubled over the last 12 months with small retailers and mid-sized retailers selling digital goods being hit the hardest. To discuss how retailers can defend themselves against fraudsters while still increasing conversions, Internet Retailer spoke with KC Fox, senior vice president of technology services at Radial, a global omnichannel technology and operations provider.

IR: What common mistakes do retailers make when it comes to fraud prevention?

KCF: Many retailers tend to not invest enough in their fraud prevention strategies. And that may be for a few different reasons. First, they think they won't have a fraud problem. A men's underwear merchant, for example, might think that fraudsters are only targeting expensive items, but studies have shown that they often go after lower cost items to make their money.

Second, retailers often don't recognize that they might already have a fraud problem. They think they're doing a great job preventing fraud—and they probably are. But they are doing it at the expense of sales by declining what may be perfectly good orders out of fear those orders are fraudulent. And finally, many fraudsters manage their fraud on the cheap. Instead of investing in robust fraud prevention tools, they try to handle it internally—delegating the task to lower level employees. Fraud prevention is very complex, so this strategy will never work.

IR: What are the most complex challenges retailers face when trying to manage fraud?

KCF: There is a very delicate balance between declining potentially fraudulent transactions and approving valuable sales. That's where retailers struggle. They need the tools and expertise to delve deeply into those particularly questionable sales to determine whether they should approve or decline those transactions.

Additionally, fraudsters are amazingly sophisticated. They're intelligent, they adapt, and they're good at figuring out where the holes are in your system and taking advantage of them. Therefore, retailers need equally sophisticated tools to combat fraudster attacks.

IR: What strategies can retailers implement to better manage ecommerce fraud and decrease chargebacks?

KCF: First, they need to either become fraud prevention experts or hire fraud prevention experts. Chances are fraud prevention isn't the focus of their business. And it can be detrimental to your relationship with a customer when you decline a sale that looks like fraud but is actually legitimate. You will insult the customer, and they likely never buy from you again. So retailers really need to invest properly in finding outside sources that can effectively handle fraud prevention for them.

An ideal fraud prevention partner, such as Radial, understands how fraudsters work. They can identify retailer's fraud vulnerabilities and set in place the appropriate measures to thwart attacks. But on top of that, they can implement strategies that help retailers optimize for taking more risk with the questionable transactions to increase sales.

IR: How can retailers increase good conversions?

KCF: In addition to working with fraud prevention experts and investing in the right tools, retailers need to plan for attacks. Understand the various attacks, then have a plan in place ahead of time for handling those attacks. The easiest way to do this is to understand your customers really well. The more you know about your consumer and how they behave normally, the easier it is to identify whether what may seem like a fraudulent transaction is actually how they behave. That helps you increase conversions.

Radial
a bpost company

SIMPLIFYING ECOMMERCE

Radial is focused on delivering technology and services to help you:

Deliver orders faster

Expose more inventory

Scale on demand

Mitigate fraud

Inspire customer loyalty

Visit **Radial.com** to see how our Fulfillment, Supply Chain Logistics, Customer Care, Payments & Fraud and Order Management Solutions can grow your business.

www.radial.com | +1 877 255 2857

HOW THE NEW NORTH AMERICAN FREE TRADE AGREEMENT WILL IMPACT ECOMMERCE

If passed, the U.S.-Mexico-Canada Agreement could drive more retailers to sell across borders.

BY ZAK STAMBOR

BEFORE PRESIDENT BILL CLINTON SIGNED THE NORTH AMERICAN FREE TRADE AGREEMENT on Dec. 8, 1993, he declared the deal "will tear down trade barriers between our three nations." He went on to note that NAFTA would "create the world's largest trade zone."

Relatively quickly, the agreement transformed the nature of the relationship among the United States, Canada and Mexico by removing most barriers to trade and investment. And it led to dramatic changes across many industries' supply chains.

"The deal created a North American supply chain," says Nate Herman, senior vice president of supply chain at the American Apparel and Footwear Association. For example, the deal enabled U.S. apparel manufacturers to ship U.S. fabrics, yarn and zippers to Mexico where they could be cut and sewn before being sent back to the U.S.—duty free—to be sold to consumers.

'[USMCA] will likely drive some retailers to begin selling abroad.'

JONATHAN GOLD, VICE PRESIDENT OF SUPPLY CHAIN AND CUSTOMS POLICY, NATIONAL RETAIL FEDERATION

But the three nations couldn't see into the future. The free trade agreement was signed nearly a year before Jeff Bezos incorporated Amazon.com Inc. and 18 months before the retail giant opened its doors. Another 21 months would pass before Pierre Omidyar launched AuctionWeb, a site "dedicated to bringing together buyers and sellers in an honest and open marketplace" that in September 1997 was renamed eBay Inc. As a result, the word "internet" doesn't appear a single time in NAFTA's hundreds of pages, 22 chapters and seven annexes.

In the more than 26 years since Clinton signed NAFTA, the three countries' economies have significantly changed. Retail has shifted online, the volume of data that retailers collect on consumers has proliferated and books, music, games and other goods have been digitized. While each of the three countries developed a patchwork of regulations to deal with those developments, many believed they were overdue to update the original deal. That's why Herman says, "it's time to bring [the agreement] up to date."

Modernizing NAFTA is the goal of the new North American free trade agreement, or the U.S.-Mexico-Canada Agreement (USMCA), a deal initially agreed to in 2018. And while the agreement languished for more than a year after the three nations' negotiators secured an agreement, on Tuesday, Dec. 10, Democrats in the U.S. House of Representatives announced support for the deal. The House is expected to vote on the deal before yearend (it still will need to be passed in the Senate, as well as the legislatures in Mexico and Canada before it can take effect). The deal, which would be the first U.S. free trade agreement to include a chapter on digital trade, includes a few key provisions that explicitly address ecommerce and that many believe will yield key benefits for online retailers while also serving as a model for future trade deals.

"The deal should help online retailers," says Jeffrey Weiss, a partner in law firm Venable LLP's International Trade Group who previously served as the U.S. Commerce Department's deputy director for policy and strategic planning. More importantly, it is designed to serve as a template for future trade deals that should help retailers, he says.

THE DEAL WILL LEAD BOTH MEXICO AND CANADA to increase their de minimis shipment value levels, which is the minimum value of an imported shipment that is subject to duty collection and customs documentation. Both Mexico and Canada are doubling their de minimis thresholds; Mexico's threshold will rise to the equivalent of $100 from $50, and Canada's will increase to C$40 ($30.25) from C$20 ($15.13). The trade agreement also means that Canadian consumers won't have to pay a duty for cross-border online orders that are C$150 ($113.44) or less; Mexican shoppers won't have to pay a duty on cross-border online orders that are the equivalent level of $117 or less.

Those changes are expected to boost cross-border shipments from U.S. online retailers to Canada by 4.6%, which translates into roughly $332.3 million in additional sales, according to an estimate by U.S. International Trade Commission. Cross-border shipments from U.S. online retailers to Mexico are expected to increase by 3.6%, which translates into $91.3 million.

‘The deal is important to our members because it brings our relationships with Canada and Mexico up to date.’

JENNIFER SAFAVIAN, EXECUTIVE VICE PRESIDENT FOR GOVERNMENT AFFAIRS, RETAIL INDUSTRY LEADERS ASSOCIATION

While Canada and Mexico’s de minimis increases are less than the United States may have wanted, they should make it easier for online orders to ship across the borders and may encourage some retailers to begin selling across the Mexican and Canadian borders, says Jonathan Gold, the National Retail Federation’s vice president of supply chain and customs policy.

“We expect that retailers will take advantage of those increases,” he says. “It will likely drive some retailers to begin selling abroad.”

A fact sheet released by the Office of the U.S. Trade Representative argues the deal is a boon to small and midsized retailers.

“Increasing the de minimis level with key trading partners like Mexico and Canada is a significant outcome for United States small- and medium-sized enterprises (SMEs),” the sheet says. “These SMEs often lack resources to pay customs duties and taxes, and bear the increased compliance costs that low, trade-restrictive de minimis levels place on lower-value shipments, which SMEs often have due to their smaller trade volumes. New traders, just entering Mexico’s and Canada’s markets, will also benefit from lower costs to reach consumers. United States express delivery carriers, who carry many low-value shipments for these traders, also stand to benefit through lower costs and improved efficiency.”

The agreement also acknowledges ecommerce’s significance within the retail industry, says Jennifer Safavian, executive vice president for government affairs of the Retail Industry Leaders Association. “The deal is important to our members because it brings our relationships with Canada and Mexico up to date,” she says.

The deal also updates the prior agreement by reducing the amount of paperwork that’s required to ship most items across borders that are valued at less than $2,500 (or C$3,300). That should speed up the time it takes for an item to be shipped across the border and eliminate some friction, says Venable’s Weiss.

The move is “a good risk management strategy that should make customs more efficient,” he says. It also will have the benefit of making it cheaper and faster for small merchants to ship items across borders.

USMCA COULD ALSO BENEFIT RETAILERS

by prohibiting the three countries from applying customs duties or other so-called “discriminatory measures” to e-books, videos, music and other digital products that are distributed electronically.

That stands to help the broad swath of retailers—game sellers, booksellers and others—that sell digital products both in terms of their sales to North America and in shaping global norms, Weiss says. “The deal locks in the ways business is currently done,” he says. “And it can also help influence how these businesses are treated in trade deals around the world.”

A number of retail trade groups are also pleased that USMCA ensures that retailers’ data can be transferred across borders. The deal minimizes any limits on where data can be stored and processed.

That ensures retailers don’t need to build out or lease costly separate data infrastructures in each

country they operate, says NRF's Gold. In doing so, it seeks to eliminate the threat of so-called data protectionism policies that force international companies to build out data infrastructures in every country they operate. Doing so would be costly, as well as increase retailers' exposure to data breaches.

"Retailers rely on data for a variety of purposes," Gold says. "If they had to house their data all over the world, it would cost them a lot of money, as well as lead to concerns about how it is protected and used."

At least that's the perspective of Pool Supplies Canada. The online-only pool supplies retailer doesn't sell internationally and doesn't plan to start, even after USMCA is signed. Instead, it seeks to ensure it delivers a high-quality experience to Canadian shoppers.

While USMCA may open up new opportunities to online retailers, those merchants' success will ultimately depend on their ability to provide a good experience to international shoppers. And that isn't easy. **iR**

ZAK@DIGITALCOMMERCE360.COM | @BYZAKSTAMBOR

USMCA'S LARGER IMPACT MAY BE FELT outside of the United States. For example, the deal could lead Canadians to look to U.S. online retailers to buy low-cost items rather than Canadian merchants because they won't have to pay the country's harmonized sales tax.

That has the potential to pose a challenge for Canadian merchants that have long benefited from the country's previous $20 de minimis level, which was among the lowest around the world. However, Canadian online retailers may be able to counteract those issues by offering incentives such as free shipping and convenient return policies, according to the results of a recent consumer survey conducted by the Retail Council of Canada.

Merchants may also appeal to Canadians' sense of patriotism. After all, 85% of Canadians considered it important to buy from a retailer that operates within Canada this holiday season, the survey found. That outpaced holiday sales (cited by 65% of respondents), free shipping (53%), convenient return policy (39%) and guaranteed shipping date (22%). Those results suggest that offering a positive online shopping experience may end up mattering more than the lowest price.

ROBOTICS ARE CHANGING ECOMMERCE FULFILLMENT

A number of retailers are turning to robotics to more efficiently manage their ecommerce orders.

BY STEPHANIE CRETS

ECOMMERCE DISTRIBUTION CENTERS LOOK DIFFERENT than they did just a few years ago. A growing number of retailers are leveraging picking, packing and delivery robots to automate key tasks—and the shift is just getting started.

More than 50,000 warehouses worldwide are expected to use commercial robotics by 2025. That would be a dramatic jump from the 4,000 in existence in 2018, according to market research firm ABI Research. In the United States alone, the research firm forecasts roughly 23,000 robot-powered warehouses in operation by 2025, up from 2,500 today in 2018.

Ecommerce's growing market share—and the push to deliver consumers' online orders the same day or next day after a shopper places an order—is helping drive that growth, says Nick Finill, senior analyst at ABI. Retailers' growing needs also help explain

'Robotics in the supply chain has the potential to reduce costs, improve efficiencies and increase human productivity and accuracy.'

DAVID GLICK, CHIEF TECHNOLOGY OFFICER, FLEXE

why the number of fulfillment-related jobs jumped 41% between 2015 and 2018 to 1.2 million warehousing and storage jobs in 2018 from 785,000 in 2015, according to the U.S. Bureau of Labor Statistics. That growth has come amid a tightening labor market as the U.S. unemployment rate has fallen to 3.6% in October 2019 from 5.5% in January 2015.

Those conditions have driven retailers to deploy the latest generation of sophisticated robotics. Those robots can handle a range of tasks—from autonomous mobile robots that can transport inventory to articulated robotic arms that can manipulate items to automated storage and retrieval robots that retrieve items for use. And many are ideally suited to ecommerce fulfillment, Finill says.

"Robotics in the supply chain has the potential to reduce costs, improve efficiencies and increase human productivity and accuracy," says David Glick, chief technology officer at logistics and fulfillment company Flexe, who previously worked as director of global fulfillment at Amazon.com Inc.

50,000

The number of warehouses that are expected to incorporate robotics by 2025.

Source: ABI Research

DRIVEN BY THE NEED for more flexible and efficient ecommerce fulfillment, Gap Inc. recently added a robotic, artificial-intelligence-powered picking system from robotics vendor Kindred.

The apparel company added the system at the same time that it was revamping its fulfillment network to better support ecommerce orders. Gap initially tested the robotics system in 2017 by integrating Kindred's SORT system into the existing infrastructure at its Gallatin, Tennessee-based facility, says Kevin Kuntz, the retailer's senior vice president of global logistics fulfillment.

The robotics technology has helped speed up the facility's fulfillment operations and helped it weather an influx of orders during peak sales seasons, Kuntz says.

"Robots enable warehouses to scale operations up or down as required while offering major efficiency gains and mitigating inherent challenges associated with labor and staffing," ABI's Finill says.

Kindred's SORT system has transformed the retailer's processes. Gap previously dropped thousands of products into a pile from a giant oval belt—known as a Bombay

'We're very proud of that so we can match Amazon's speed of delivery without the Prime member price tag.'

ROB BASS, CHIEF SUPPLY CHAIN OFFICER, BEST BUY CO. INC.

sorter—into manual sorting stations, and an employee would pick up each piece and scan it with a bar code scanner. A corresponding light on the putwall—a vertical grid of cubbies—would then light up to signal an employee which cubby corresponds to that order. After all items were scanned, the employee took the cubby's contents and passed it off to another station to be packed and shipped.

The SORT system allowed Gap to reconfigure the chutes from the Bombay sorter to send products directly to the robotic arm sorter. The system uses a camera to look at the items in the bin, comparing each to all the images of Gap items in its system. It then uses the system's various data points to calculate and execute an optimal pick strategy for each task in real time, says Kindred CEO Jim Leifer.

For example, if there is a pile of plastic bags that contain a red T-shirt, black socks and pair of jeans, the arm can look at the unstructured items and determine the correct piece to select. The arm then grasps, pinches or suctions the item, then swings to expose the item's bar code to be scanned by one of four cameras surrounding the bin to ensure it matches the order.

Occasionally, the robotic arm encounters an issue and needs human intervention. "While the solution is autonomous, there will be moments where it doesn't have the confidence level to execute its tasks," Leifer says. "We have a pilot, so if a robot needs help, then it opens a channel to one of our remote pilots within less than a second and helps the robot understand and keep working. "

Within a few months, the SORT system was picking 98% of Gap's items autonomously and rarely required pilot assistance, Gap says. Because of SORT's success at the Tennessee facility, Gap implemented the system into its Fresno, California, distribution center last fall and plans to add it to its Fishkill, New York, distribution center by the end of this year, the retailer says.

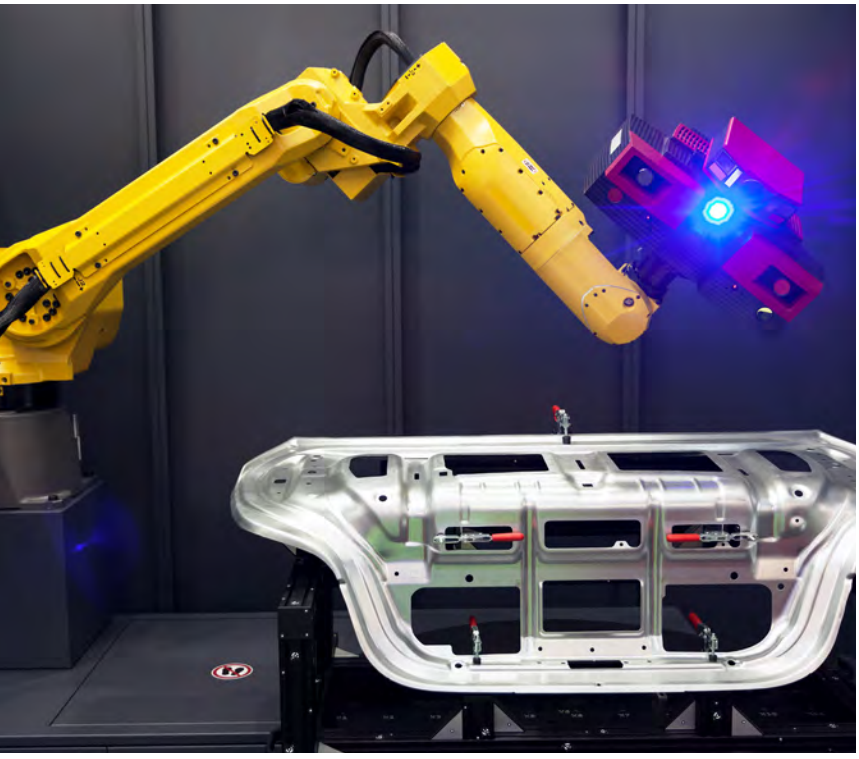
"Kindred enhanced the grippers and scanners to improve the accuracy of the machines," Kuntz says. "We have seen impressive speed improvements in the 18 months since we began implementation, and the percent of autonomous picks have increased."

While Kindred declined to reveal the cost of implementing the system, Leifer refers its approach as "robotics-as-a-service" (RaaS), which means the retailer pays per successful pick (it declined to share whether it charges any additional fees). By 2026, there are expected to be 1.3 million installations of RaaS by various robotics vendors, according to ABI Research.

Although the system is automated, a warehouse employee has to complete the supply chain flow after the robotic arm picks the order. However, the system greatly increases that worker's efficiency, he says. "A single employee can pack many more orders at a SORT station because the robotic arm

'We want to stay ahead of the curve, ahead of our competitors, and to do that, we need to stay technologically advanced.'

JASON EVEREST, DIRECTOR OF PRODUCTION AT MARLEYLILLY



20,000

The number of units Best Buy can pick per hour with the aid of robots.

Source: Best Buy

is doing most of the work," he says. "If the employee oversees multiple picking stations, he can be responsible for two to three times as much throughput."

ROBOTICS HAVE ALSO TRANSFORMED Best Buy Co. Inc.'s fulfillment processes.

About six years ago, the retailer struggled to meet consumers' delivery expectations, and it knew it needed to make significant changes if it was going to survive, says Rob Bass, the retailer's chief supply chain officer. It wanted to become more efficient, improve its supply chain and figure out how it could compete in a different way.

But the retailer had to combat several issues: roughly 60% of Best Buy's orders are repack items—which means the retailer removes them from the manufacturer's packaging and places them in Best Buy-branded packaging. But Best Buy didn't have the capital to invest in a bigger team to keep up with the ecommerce repack item demand, as well as shoppers' growing demand for more efficient ecommerce fulfillment and delivery. Plus, most of its distribution centers operated five days a week as opposed to seven days, and its systems were "old enough to smoke and drink in the U.S.," Bass says.

But it did have a few warehouses in strategically important locations: Compton, California, which is near Los Angeles; Piscataway, New Jersey, which is near New York City; and Chicago. Best Buy sought to put its "big-hitting ecommerce SKUs" inside these buildings and transform them into "metro ecommerce centers," Bass says.

Best Buy worked with logistics system integrator Bastian Solutions and with AutoStore—a bin storage system in which bins are stacked vertically in a grid and retrieved by robots that travel on the top layer of the system—to overhaul its distribution centers. The process took about 12 months to implement, but the retailer declined to share the cost of the overhaul or when it started using the new system.

The retailer now has 30,000 bins and 73 robots at each of its three metro ecommerce centers. Best Buy delivers up to 40% of a store's

inventory to a store from its metro ecommerce centers and segregates store delivery by aisle (the rest of the metro ecommerce center is focused on fulfilling online orders). Bastian and AutoStore outfitted Best Buy's regional distribution centers—located in San Francisco, Atlanta and Findlay, Ohio—with 150,000 bins and 195 robots.

Since implementing these new systems, Best Buy increased its ability to pack up to 20,000 units per hour. The system has made warehouse workers more efficient, Bass says, noting that they used to walk up to eight miles per day retrieving and packing products. They now stand in place while the bins and robots move around the facilities. This allows them to focus on individual tasks instead of running around the facility.

In turn, the retailer delivers most orders in two days, a far cry from the six days that it previously took to deliver an online order. "We're very proud of that so we can match Amazon's speed of delivery without the Prime member price tag," Bass says.

IT'S NOT JUST LARGE RETAIL CHAINS

that are adding robotics. For example, online apparel, accessories and gifts retailer Marleylilly in June 2018 began working with warehouse robot provider Locus Robotics to help it fulfill and deliver orders quickly and efficiently—especially during peak seasons.

"Our peak seasons are fast," says Tiffany Stewart, assistant manager of fulfillment at the retailer, declining to provide sales specifics.

Locus Robotics' system uses algorithms to accept clusters of orders for products in the same warehouse section or aisle and rely on warehouse mapping software to follow an optimal path among merchandise racks. Pick workers in the aisles then read order information on the robots to place the order items in bins that the robots then carry to packing stations, navigating around the facility without running into anything else, such as workers or other robots.

Locus also provides a dashboard in the warehouse so management can monitor how many picks are done per hour, how many items need to be picked for that day and the number of open orders.

It has 15 robots working within its fulfillment center and, during its peak holiday season that number grows to 25, says Jason Everest, director of production at Marleylilly. Therefore, the retailer can scale up the robotics to keep up with peak season demand without hiring additional warehouse staff.

Within nearly a year and a half of using Locus Robotics, Marleylilly tripled the number of orders it ships per month, while also significantly increasing accuracy and pick rates, although it declined to give further details. "We're not eliminating jobs, we're really just increasing the efficiency and optimizing our pick operation," Everest says. "We want to stay ahead of the curve, ahead of our competitors, and to do that, we need to stay technologically advanced."

That's increasingly important within a competitive ecommerce environment.

"Collaborative robots drive productivity increases," says Locus CEO Rick Faulk. "They ensure that brands are able to meet their fulfillment goals, despite the widespread scarcity of warehouse labor and influx in order volumes." iR

SCRETS@DIGITALCOMMERCE360.COM | @STEPHCRETSDC360