

# State of Fraud Report 2021

A New Age of Fraud - A New Age of Commerce Protection

# Table of Contents

1

---

2

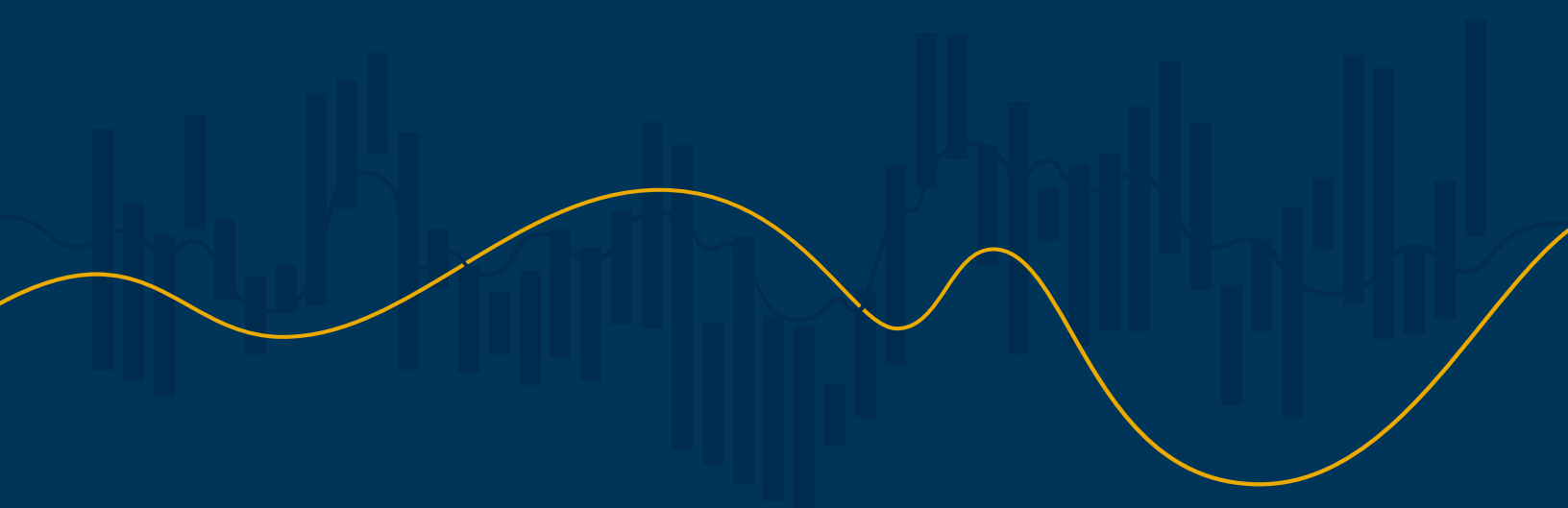
---

3

---

4

---





As the world strained against the grip of a global pandemic, the very nature of ecommerce fraud changed. In a matter of months, fraud became more abundant, more automated and more diversified in terms of techniques and targets.

As retailers became more sophisticated at protecting their enterprises from payment fraud, fraud rings innovated, iterated and persisted. In effect, they seized the disruption of COVID-19 to usher in the golden era of online fraud. What was not new in fraud was intensified.

“



Fraud has gotten more sophisticated over the years because cybersecurity has gotten better. Fraudsters have to be more sophisticated. They have to up their game, because their avenues are being shut off.

CONOR CORKRUM, FRAUD PREVENTION MANAGER

BLUE NILE.



The focus of fraud attacks moved down the payment chain to more vulnerable links, such as account creation, account login and the task of updating accounts with additional payment forms. Scams that fraud rings had historically dabbled in — synthetic identities, return fraud, fraudulent fulfillment disputes and more — flourished during a time when retailers were scrambling for their financial lives and chaos reigned. And like so many pandemic-spurred step changes, the new era of fraud will persist into the 2021 holiday season and well beyond.

This e-book will dive into the changes, the data behind the trends and the measures retailers can embrace to inoculate themselves from a more virulent strain of ecommerce fraud that is spawning new variants with stunning frequency.



### SIGNIFYD FRAUD PRESSURE



○ FRAUD PRESSURE INDEX

## Part 1: The era of fraud innovation is now

History tells us that all-encompassing, traumatic events are watersheds — they change practically everything to a degree. We move on and the changes travel with us.

Fraud realized the dawn of its golden era for many of the reasons that some legitimate businesses survived or even thrived in the time of the pandemic. Advances in technology, which of course started before the pandemic, afforded businesses and fraud rings alike the tools to remain productive while working from home.

We've all read how artificial intelligence, wisely deployed, can supercharge business and create efficiencies that were unimaginable even 10 years ago.

The same is true of online fraud. Fraud rings found new opportunities given the circumstances, too. That is the story of commerce and fraud in 2021. Innovation often thrives out of the necessity, fresh perspective and urgency that disaster brings.



What we were experiencing at Toys R Us, as well as a lot of the other retailers, was five to ten years of acceleration and modernization that you're really experiencing in a compressed five-to-ten-months time frame.

ROHAN CHERIAN, AVP ECOMMERCE & CONSUMER TECHNOLOGY



Rohan Cherian, the AVP of ecommerce & consumer technology for Toys R Us Canada, described the dizzying change many retailers endured.

“What we were experiencing at Toys R Us, as well as a lot of the other retailers, was five to ten years of acceleration and modernization that you're really experiencing in a compressed five-to-ten-months time frame. Our journey was just phenomenal and completely different from what I thought we would be doing.”

Changes were afoot in another industry as well. Advances in performance and declines in the cost of learning machines accelerated fraud rings' use of bots.

Criminal organizations could quickly test thousands of stolen credit accounts, execute fraudulent orders in rapid-fire succession and clean out whole inventories of popular products in order to resell them without authorization at sky-high prices.

Fraudsters in the past year turned to automated attacks like never before. In fact, Signifyd tracked a 146% increase in bot attacks during 2020.

## Fraudsters nimbly adapt to changing conditions

Fraud advanced in other ways during the pandemic, too, with fraudsters upping their social engineering game. With so many working from home — or wanting to — fraudsters shifted from romance mule fraud to work-at-home mule fraud schemes.

The common idea is to trick a “mule” into helping criminals move fraudulently purchased goods around the country and around the world.

The romance version takes months or years of deception to build an emotional bond.

Work-from-home mule fraud is transactional and therefore quicker. You take a job. You do the work. You expect to get paid.

Fraud rings created entire fake companies with real recruiters who would prey on people

tethered to their homes during the pandemic, either because they had school-age children at home or because they were leery about returning to offices or job sites populated with other workers.

The most recent evidence shows that after Signifyd disrupted a large number of mule schemes, fraudsters are pivoting away from mule fraud — at least on Signifyd’s Commerce Network. And at least for now.

The increasingly rapid shape-shifting of fraud means risk teams need ever-more sophisticated ways to identify different threats.

Sharon Alejandra Lopez, ecommerce jr. director for Walmart Ecommerce Mexico, for example turns to Signifyd’s Decision Center to identify threats beyond payment fraud.





“We analyze the suspicious information that we have to determine whether we are having an attack,” Lopez says. “If that’s the case, we build new policies in Decision Center. It’s a really, really quick and easy-to-use interface, and very powerful in combatting fraud and abuse.”

Fraud solutions, like Decision Center, a module of Signifyd’s Commerce Protection Platform, affect change.


For instance, after a strong run, the number of mule fraud attempts in 2021 has plummeted by 65%, according to Signifyd data.

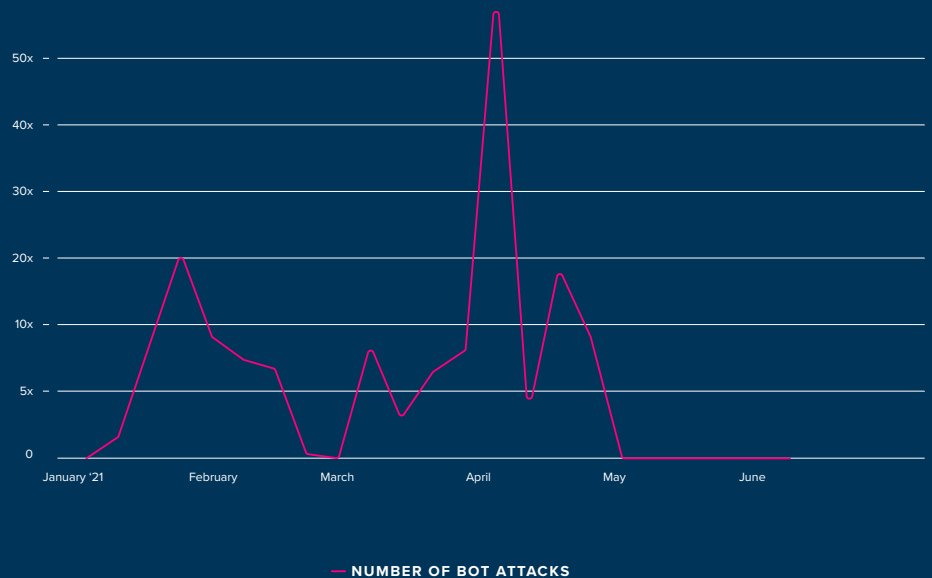
Fraud rings recently began more seriously probing the entire ecommerce payment process — not just checkout — for the most vulnerable points in the process.

In fact, one of the most mind-boggling innovations is the rise of synthetic identities, a scheme that takes identity theft one step farther and is aimed at account creation.

In cases of synthetic identity fraud, criminals create a whole new and non-existent person by patching together pilfered and made-up personally identifiable information.

Professional fraudsters know that the early stages of the payment process — when consumers create their accounts or log in or make changes, such as adding payment forms — are less protected than the later stages of checkout. Retailers don’t want to add too much friction when new customers are establishing their accounts for fear a shopper will abandon a cumbersome process and simply click over to Amazon to make their purchase.

 The fluctuation of bot attacks against a select, but substantial, segment of Signifyd’s Commerce Network in the first half of 2021. The dramatic April spike represents a fraudulent run on computer chips. The plunge in attacks in May is a result of additional fraud countermeasures that drove fraudsters away as they no doubt searched for softer targets.



## Fraudsters as entrepreneurs

The golden era of fraud has also marked a more pronounced move into forms of fraud beyond traditional payments fraud. As the volume of ecommerce has grown, in part due to the pandemic, and as the digital world has increasingly become all our worlds, fraudsters have sought out a variety of ways to take advantage of merchants and consumers.

451 Research noted the trend in a May 2021 report highlighting fraud trends.

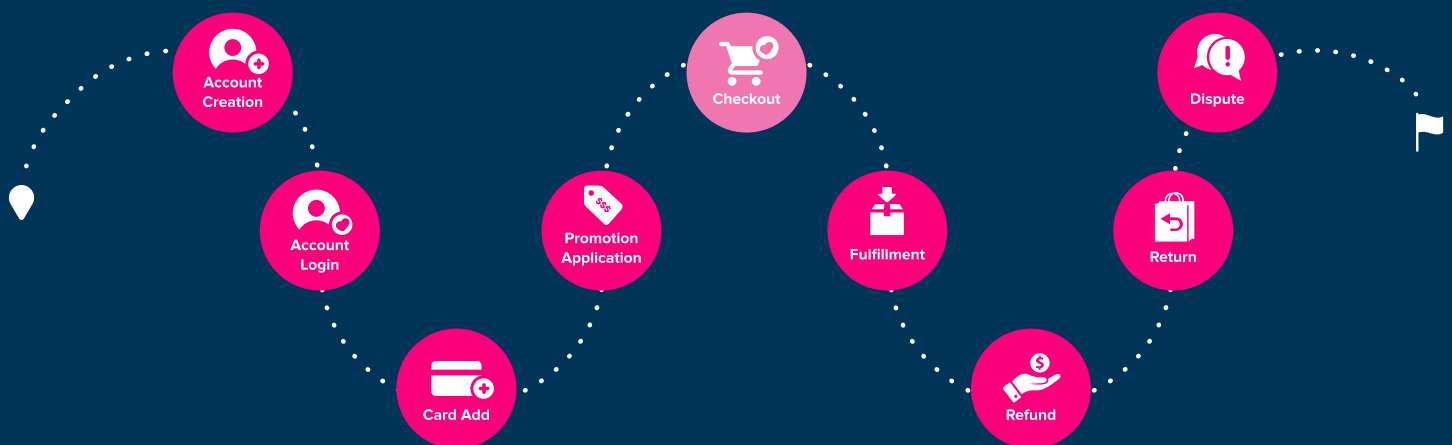
“Bad actors are broadening their focus beyond payments, targeting touch points across the customer journey,” the report said.

“Touchpoints from online account creation through to product returns have emerged as growing vectors for fraudulent activity, and consequently, both financial and reputational losses.”

It’s always helpful to remember that fraud rings are for-profit enterprises and fraudsters are entrepreneurs constantly looking to expand their total addressable market. So, as merchants have become better at protecting themselves from payment fraud with solutions like Signifyd’s Commerce Protection Platform, fraudsters have expanded into non-payment forms of fraud.

Nearly every enterprise retailer that Signifyd talks to is working to curb return fraud — generally the practice of buying a high-value item and returning some lesser-value item for a refund.

## Fraudulent Activity Spreads Across the Customer Journey





## Criminal rings are expanding into “friendly fraud”

Fraudsters have also become retailers themselves by becoming unauthorized resellers — scalpers if you will — of desirable products.

Beauty and cosmetic brand CurrentBody was familiar with the practice and was determined to protect its good name. It turned to [Signifyd's Abuse Prevention](#) to ensure that unscrupulous resellers weren't doing brand damage.

“We were very concerned about the effect resellers could have,” Lyn Carbine, head of trading at CurrentBody explained. “Controlling the distribution of our products is essential to maintaining successful brand partnerships.”

While it's become almost tiresome to blame problems and explain trends in the context of the COVID-19 pandemic, its role in the changing face of fraud can't be denied. It's true retailers have been tormented for years by a small, but significant, number of customers who make false claims about packages that never arrive. Now, however, they face claims of “item not received” from more sophisticated fraud rings.

Technical consulting agency and Signifyd partner, The Maze Group has seen the item not received, or INR, trend play out among its customers.



“



Most of our clients came out of COVID with a newfound understanding of why additional fraud mitigation was an important consideration. With more home deliveries than ever came an uptick in ‘item not received’ and other fraud types that many merchants were not fully protected against. That extra layer of protection from Signifyd, beyond what payment processors provide, has become a crucial element to any ecommerce technology stack.

MARTINA ENGLAND, HEAD OF PARTNERSHIPS



Consumer abuse, including false item-not-received (INR) claims, is up more than

**100%**

in the first half of 2021, compared to 2020.

The combination of a huge spike in ecommerce orders, a population stuck at home and a significant number of people facing financial desperation, set the ideal stage for a wave of innovation in fraud. And like many changes born of the pandemic, it appears these new or more pronounced fraud trends are here for the long-term and maybe for good.

## Shifting fraud is a case of good news, bad news

So, now we have an idea of how fraud at the dawn of the post-pandemic era is changing in type and degree. Those who work to protect retail from fraud can look at the transformation in two ways:

**A fantastic success:** Fraud and risk professionals, with the help of innovative technology providers, have made such strides in combating payment fraud that fraudsters have broadened their portfolios in search of more vulnerable ecommerce targets.

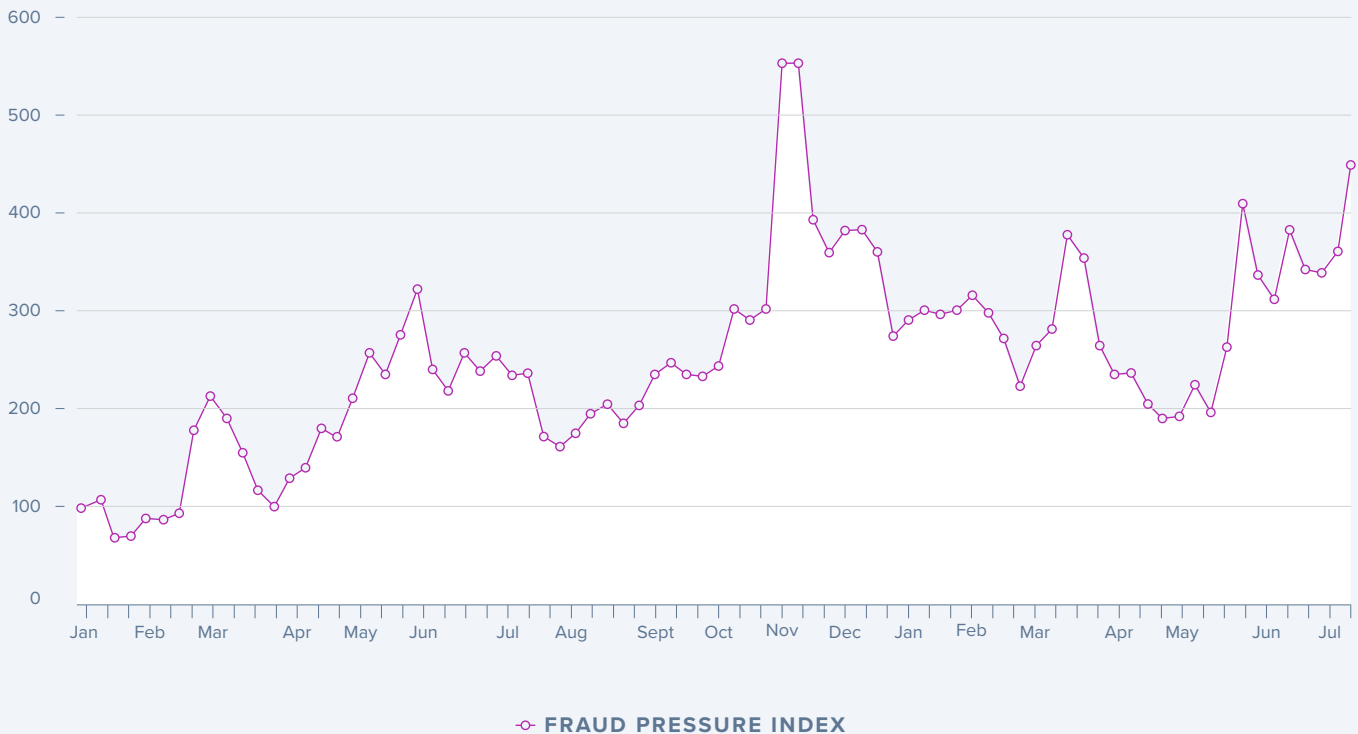
**A warning and wake-up call:** Fraud is not going away. It never has. Throughout the history of commerce, fraud has been a shape-shifter, adjusting nimbly to advances in fraud protection, whether that's CVV codes,

chip-enabled credit cards or even efforts, such as Strong Customer Authentication (SCA) in Europe. Fraud professionals need to continue to keep up in a game of cat and mouse that will keep both fraudsters and those who foil them in business for decades to come.

The Fraud Pressure Index measures the rise and fall of orders on Signifyd's Commerce Network that are determined to be a very high risk of fraud, based on thousands of signals. The index is benchmarked to fraud activity the first week of January 2020 to show the change throughout the pandemic period.



FRAUD PRESSURE



-o- FRAUD PRESSURE INDEX



## New forms of fraud IRL

Let's take a deeper dive into some of the fraud trends that gained prominence during the pandemic and those that are flourishing today.

### Mule fraud

Fraud that relies on recruiting go-betweens can't be called a new trend. It's prominence rises and falls, but every blip in mule fraud activities comes with innovations.

During the pandemic, work-from-home come-ons were the key recruiting tool and Signifyd's data indicated there were plenty of takers. The sharp increase in fraud involving big rings relying on armies of dispersed mules to receive stolen goods and forward them to reshippers and out of the country, appears to have subsided.

Signifyd recognized the trend early in the pandemic and factored the warning signs into its models. After stopping nearly 2,000 mule fraud attacks, such attacks now make up less than 1% of the fraud attempts on Signifyd's Commerce Network — which doesn't mean mule fraud won't rise again.

### Account takeover

Retailers — and consumers — have been battling account takeover for years. But during the pandemic, ATO scammers shifted to tricking consumers into giving up personal information rather than simply relying on credentials stolen in data breaches, according to a study by Javelin Strategy & Research.

Account takeover fraud allows fraudsters to find an area of attack outside the checkout process, avoiding the point in the payment process where barriers to fraud are typically the greatest. The increasing use of bots plays into this trend, as automation allows fraud rings to attempt to breach thousands of accounts in quick succession.

Taking over accounts also gives fraud rings access to loyalty points — as good as cash when it comes to buying goods and far less scrutinized by consumers. Less scrutiny gives fraudsters a better chance of getting away with the crime before anyone realizes there is a problem.





Once a fraudster makes their loyalty point purchases, they can sell the goods or return them for gift cards, which can easily be converted to cash on any number of marketplaces.

Capturing active accounts also gives fraudsters valuable inventory — in the form of accounts in good standing — that they can sell on the Dark Web.

### **Nouveau card testing**

Because retailers are loath to add friction early in the payment process — think account creation or adding a payment form to an account — fraudsters have been attacking those segments of the payment process, too.

In a growing form of card testing, fraud rings are now adding new, stolen, credit cards to breached accounts that have demonstrated a solid ordering history with a merchant.

Typically the merchant will authorize a \$0 charge on the new card to see if the banks and payment processors involved will approve the card. If the charge goes through, fraudsters know they are free to make actual purchases with the card. And they do — quickly and prolifically.

### **Synthetic identities**

The wealth of purloined personal information floating around during the pandemic fueled an increase in a pernicious fraud technique — the creation of synthetic identities.

Fraud rings create consumers from whole cloth — or more accurately from a mixture of stolen and self-generated personally identifiable information. Often starting with a stolen Social Security number — usually a child's because there will be no credit history — the fraudster makes up a name, cooks up a billing address and applies for a new credit card.

“



Voila, the fraudster is free to rack up a big bill that they will never have to pay. And they can be fairly certain the made-up person they manufactured isn't going to say a word to anyone.

In fact, financial technology leader and Signifyd strategic partner FIS reported [increases in both synthetic fraud and ATO](#).

In our recent Global Payment and Risk Mitigation Survey, the majority of merchants surveyed reported increases in synthetic and account takeover fraud over the previous year. As these and other new fraud trends emerge, the safeguarding of a merchant's revenue requires smart, dynamic protection against fraud throughout the payment lifecycle.

JOHN WINSTEL, GLOBAL HEAD OF FRAUD PRODUCT



## FIS 2021 Global Payment Risk Mitigation report

We asked: has your company detected less, more or an equal amount of the following types of payment fraud in 2020 versus 2019?

	SIGNIFICANTLY MORE	SLIGHTLY MORE	SAME	SLIGHTLY LESS	SIGNIFICANTLY LESS
CARD-NOT-PRESENT FRAUD (E-COMMERCE, ETC.)	21%	38%	25%	12%	3%
SYNTHETIC IDENTITY FRAUD	21%	34%	28%	11%	5%
CHARGEBACK FRAUD (DISPUTING VALID CHARGES)	20%	35%	30%	11%	3%
CARD TESTING	20%	33%	32%	12%	3%
IDENTITY THIEF/NEW ACCOUNT FRAUD	20%	32%	30%	13%	5%
FRIENDLY FRAUD	22%	29%	31%	13%	5%
ACCOUNT TAKEOVER FRAUD	20%	30%	31%	13%	5%

## Drive-up crimes and policy abuse

### Order online, steal from store

Pandemic lockdowns drove a tremendous increase in online purchases that were picked up in store or at the curbside. The behavior persists today.

Signifyd data shows that buy online, pick up at or in the store orders remain 210% higher than they were pre-pandemic.

And with the BOPIS spike and continued popularity came a great opportunity for those with a criminal bent. Buy online, pick up at the store orders don't come with a delivery address, a key signal in fraud protection. And by their nature, they need to be filled fast, leaving no or little time for manual review or pondering the legitimacy of an order.

In short, says 451 Research, "BOPIS shopping experiences that have been in vogue during the pandemic enable fraudsters to quickly obtain fraudulently purchased goods and circumvent traditional manual review cycles and billing/shipping address matching."

### Policy abuse

In fraud's golden era, no corner of the commerce experience is free from attack.

Fraud rings have found ample targets beyond traditional payment fraud. Take policy abuse, for instance, or the practice of breaking the rules for discounts or consideration shoppers get for referring a new customer to a merchant.

And not just fraudsters are cashing in, as 451 pointed out in [its report](#), "Fraudsters' new target: The end-to-end customer journey."

"Concerningly, many emerging types of fraud are also committed by nontraditional fraudulent actors, including otherwise 'good' customers who are attempting to game the system by abusing both merchant and issuer business policies," the report says. "This type of fraud can be difficult to detect, and tackling it creates a unique challenge for merchants, which must carefully and delicately address instances of abuse to minimize the impact on lifetime value, as well as on their overall customer base."



## When the customer is not always right

### Unauthorized reselling

Like any enterprise, fraud rings are always looking for new revenue streams. Many are already experienced retailers — reselling items they've purchased through fraudulent transactions.

Increasingly, they've added a twist by turning to another approach — one that is not always illegal, but is clearly a violation of a retailer's policies. Call it "automated scalping." Fraudsters identify a highly desirable and somewhat scarce product — sneaker release, anyone? — and turn bots loose to corner the market. Once they control the limited inventory, they cash in on the scarcity.

### Item not received — really?

As continuous innovation by Signifyd and others have put the squeeze on fraudsters focused on committing payment fraud at checkout, innovators in the golden era of fraud have turned in larger numbers to non-payment fraud, such as filing false claims that an ordered item was not received.

The INR scam is not confined to professional fraudsters, of course. During the pandemic, such claims rose dramatically in part because of more typical consumers choosing to embrace their dark sides in a dark time.

In fact, more than 30% of respondents in a [recent Signifyd consumer survey](#) said they had falsely claimed that a product they ordered never arrived, in an effort to secure a refund and keep the product. The number was a marked increase from the percentage who admitted to filing a false INR claim in a [Signifyd survey](#) conducted shortly before the start of the pandemic.

Together, professional fraudsters and wayward consumers fueled a 100% increase in false INR claims in the first half of 2021, compared to 2020, Signifyd data shows.





## Return fraud

The potential for attacks continues even after an order has been shipped and delivered. Fraudulent returns are becoming an increasing worry for merchants. [Scammers exchange tips](#) on forums like Reddit and fraud rings advertise services on the Dark Web.

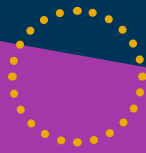
A Signifyd analysis, based on [Apriss and National Retail Federation findings](#), determined that retailers lost \$11.6 billion last year to return fraud in the cost of goods alone.

Add in associated costs — shipping, inspecting and disposing of bogus returns — and return scams cost retailers about \$43 billion last year.

Methods vary, but sending back a counterfeit copy of the product or an old or damaged version are popular approaches.

Many retailers endeavor to provide an excellent return experience by crediting an account as soon as a return is scanned in for shipment back to the merchant. That's an opening for fraudsters to ship back anything that weighs about what the original product did. In one notorious case, a [potato stood in for an iPhone](#). No doubt the retailer was fried.





## From the files of Signifyd

The numbers tell part of the story, but it's the details of fraud, turned up by Signifyd investigations, that fill the tale out. Here are a few of the stories Signifyd has tracked.

### Single-parent mule

After losing her job to pandemic cutbacks, a Pennsylvania woman was thrilled to land a job from an online ad. It would allow her to make good money from home, where she could care for her 4-year-old daughter. All she had to do was inventory and forward products shipped to her home.

But her new employer, Jerry & Sam Logistics, was a fraud-ring front. After sitting for job interviews and going through training, after shipping dozens and dozens of packages for a month, her employer went silent. She never got paid.

"It was devastating," the woman said. "Everything came crashing down. It shattered my dream."

### Basketball fever

One NBA fan — a big one — bought \$11,000 worth of souvenirs autographed by the late L.A. Lakers superstar Kobe Bryant. The buyer claimed the items were purchased fraudulently by someone else.

His online purchase history and social media activity said otherwise.

Chargeback denied. Whatever buyer's remorse the fan was suffering is something he will just have to live with.

### If the shoe fits

One single cardholder bought \$20,000 worth of Air Jordan sneakers and one-by-one filed chargebacks saying, "Wasn't me who bought them."

One problem: The big purchase was to stock the cardholder's "business" — reselling fraudulently obtained sneakers. To market the business, the cardholder posted about the big buy on Instagram and highlighted the delivery on the reseller's website.

Next photo on Insta: a mug shot?





## More stories from the Signifyd vault

### The bots who stole Christmas

The PlayStation 5 was the hot item for holiday 2020. Kids of all ages lusted after the latest Sony game console.

Everybody knew it was the “it” item — including unscrupulous, unauthorized sellers. And they went to work.

Scalpers set the bots loose, buying thousands of PS-5 units in a flash. Then they crowed and advertised by posting news of their haul on social media — and offering the consoles for sale for as much as 10 times their list price.

What was a parent to do?

### When the chips are down

It’s not hard to imagine fraudsters starting and ending their days scouring business news sites looking for the next big thing. Fraud rings dance to the rhythm of the economy and current events. As summer approached and the global shortage of computer chips tightened, fraudsters pounced. Aided by automated programs, they unleashed a fraud fusillade, ordering millions of dollars in chips and components in hours.

Most such orders on Signifyd’s Commerce Network were shut down by the company’s Revenue Protection solution. But the fraudsters undoubtedly moved on to more sites lacking Signifyd’s protection, while constantly searching for the next opportunity.

### A box of rocks

In ecommerce fraud’s golden age, return fraud is becoming more brazen and more prevalent. As anxiety over the pandemic heightened in 2020, a major electronics seller began receiving unusual returns.

The boxes were arriving not from the states where the purchases were sent, but from other locations. And inside were unpleasant surprises. Instead of the high-end devices that were shipped out, the boxes were filled with old toys and candy, weighing about the same as the original products.

Fraudsters exploited the merchant’s effort to provide a top-notch customer experience. Its return policy called for issuing a refund as soon as the return package was dropped off with the shipper — think UPS or FedEx.





## Part 2: Implications for daily ecommerce operations and holiday season

All this clever activity by online miscreants is not without its consequences, obviously.

As fraud attacks multiply and techniques morph, retailers raise their guard. Those relying on rules-based systems and manual order review find their risk teams are spending more time vetting transactions. And often a conservative self-preservation seeps into decisions, meaning good orders get declined.

Mack's Prairie Wings, a venerable Arkansas outdoors goods emporium, [faced its challenge](#) at the height of the pandemic when its online orders increased by 50% overnight.

Risk team members were reviewing a quarter of the orders coming in, often calling customers to try to verify their identities.

“Sometimes it would be one or two days’ delay,” said Debbie Pinckard, the retailer’s CFO and COO. “We live in an Amazon world and people expect their orders in one or two days. When it takes five days, people are not too happy with that.”

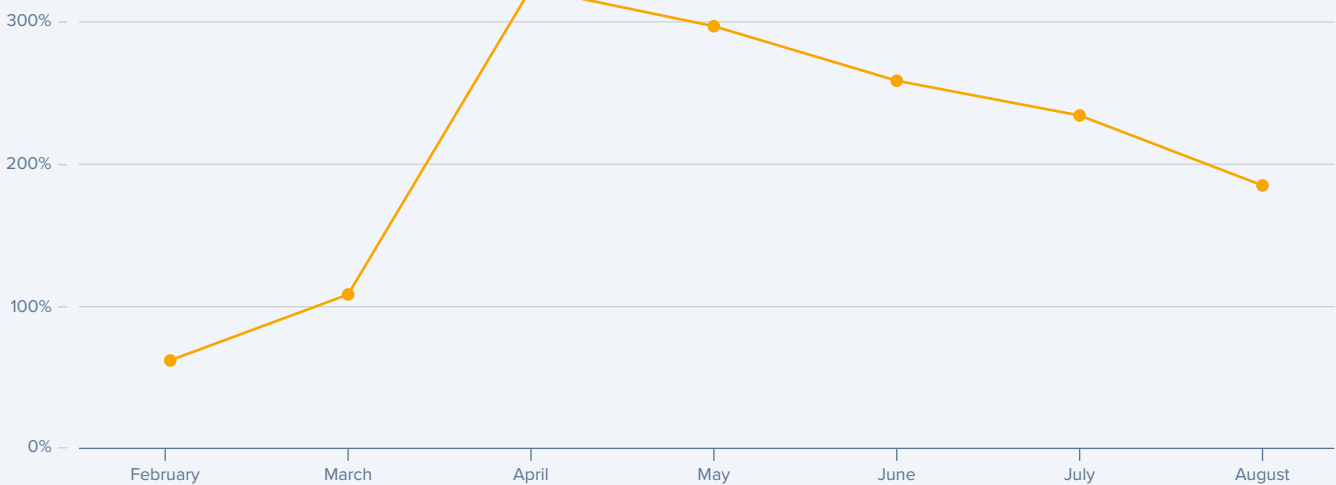
Mack’s turned to Signifyd’s [Revenue Protection](#) and [boosted its approval rate by 5.5%](#), while reducing its seasonal customer service payroll by 60%.

The outdoors retailer, which has made its name serving duck hunters, offers something of a preview of the upcoming holiday season.

Mack’s, you see, does more than 70% of its business during duck hunting season — roughly November to January.

The holiday season brings similar scaling problems to all merchants, as does the new era of ecommerce ushered in by COVID-19 lockdowns.

### Year Over Year Ecommerce Sales Growth — Leisure & Outdoor



● LEISURE & OUTDOOR - YOY%



## Avoiding the holiday holdup

As retailers around the world prepare for the holiday crush, they can dissect how Mack's moved beyond struggling to uphold its high customer service standards while manually reviewing 25% of its orders.

In Signifyd, Mack's found a Commerce Protection Platform that uses machine learning and big data to instantly sort fraudulent from legitimate orders. The platform informs decisions based on millions of transactions across thousands of merchants around the world.

Its machine models constantly learn, meaning as fraud attacks shift, their defenses shift with them.

Moreover, with its Abuse Prevention solution, Signifyd's platform extends its protection to non-fraud chargebacks, such as false item-not-received claims and claims that a perfectly good item arrived damaged or not as described.

Meanwhile, Return Abuse Prevention assures retailers that they can protect themselves in an automated fashion from return fraud, while still controlling exactly how they will handle low-risk, medium-risk and high-risk return requests.

Additionally, the platform future-proofs an enterprise's fraud and risk management with Payment Optimization, which finds the most efficient way to route transactions to ensure regulatory compliance and a frictionless customer experience.

On top of the protection and revenue optimization, Signifyd's solution enables fearless commerce by providing a full financial guarantee against all manner of chargebacks.

"Our ecommerce business saw a tremendous increase," Pinckard said. "So when you apply that increase to the incredible results that we have already seen with Signifyd, I have no doubt we made the right move."

## Holiday volumes year round

A common refrain among retailers during the height of the pandemic was that every day was a holiday.

Not as in a day off, but as in a day when ecommerce orders were arriving like many retailers had never seen. In the early COVID days, ecommerce sales as a percentage of retail sales doubled — hitting 33%.

Merchants' online revenue more than doubled, according to [Signifyd Ecommerce Pulse data](#), in the first month of lockdown as new online shoppers flocked to ecommerce to avoid stores that were either closed or loomed as a health threat.

“We obviously saw a pretty major shift from our physical retail presence to our D-to-C presence during the pandemic,” said Rob Harris, manager, fulfillment operations at Sonos, the leader in home audio. “At the same time, Sonos was a great product for when people are working from home and when people are spending so much time at home.”

By holiday 2020, all bets were off, with online sales on Signifyd's Commerce Network peaking on Black Friday at a level 500% higher than sales the week before the pandemic became official.

For Harris at Sonos, the online wave meant a record holiday.

“Even though this year we saw the largest growth in our Sonos ecommerce sales through the holidays, I found it to be the most stress-free holiday season that we've had, in part because of the automation we were able to deliver with Signifyd,” Harris said.

“It felt like the least stressful holiday season we've had in years, even though our growth was higher than it's ever been.”

Ecommerce on Signifyd's Commerce Network remained elevated at mid-year, reaching a level 73% higher than June 2019.

Obviously, holiday sales won't be up 500% during holiday 2021, but they could easily increase 3x over non-holiday sales. And of course, that increase will come off of a higher post-pandemic baseline.

Independent digital commerce specialist and Signifyd strategic partner Astound Commerce, echoed Harris' observation.

“



What were once considered benefits of purchasing digitally are now habitual practices that will prevail in holiday retail indefinitely.

JENNIFER RYAN, MARKETING DIRECTOR





“Online exploration of brands, products and experiences has become an intrinsic part of today’s customer journey, providing shoppers with endless store aisles, readily available reviews, a multitude of delivery and pick-up options – not to mention a plethora of payment methods to suit each customer’s lifestyle. What were once considered benefits of purchasing digitally are now habitual practices that will prevail in holiday retail indefinitely,” said Jennifer Ryan, marketing director at Astound Commerce. “Everyday purchases will continue to live primarily online, while holiday retail will morph into a pattern of pre-purchase online research followed by an informed physical retail experience. Brands will seek to create their own experiences to build excitement and loyalty with their customers by streamlining a hybrid shopping approach for the holidays.”

The opportunity will be there to be won for those who are prepared.

## Ecommerce verticals inhabit their own universes

It’s natural to talk about ecommerce trends. After all, ecommerce makes up a large and growing share of commerce overall. But, of course, it’s complicated. Consider fraud pressure. As ecommerce has grown as part of the retail pie, the fraud pressure it faces has grown with it. Signifyd data shows that ecommerce fraud pressure was [up nearly 350%](#) in the middle of 2021, compared to pre-pandemic levels.

But of course that wasn’t true for every retail vertical, nor was it true for any given point in time. In fact, the increase in fraud pressure in early 2021 had been as low as 89%.

A tremendous number of macro and micro factors affect the volume and virility of fraud attacks — the season, the fads, merchants’ defenses, order volume, the economy.

Remember those business-site-reading fraudsters? They communicate. If a sector or a merchant allows fraud vigilance to slip, word gets out. Attacks increase.



When the attacks are shut down, fraudsters move on to a new vertical or a new merchant.

All this to say that fraud pressure is hard to predict and anticipate. The only sure thing is that fraud rings will keep probing, keep trying, keep iterating.

Take the holiday season. Experienced risk professionals know that as a rule the overall fraud rate actually declines during the busy holiday season. The huge surge in online transactions consists primarily of legitimate orders.

If fraudsters place the same amount of orders or even increase their attacks substantially, the bigger denominator that is the overall increase in orders keeps the ratio of fraud to legitimate transactions low.

So, good, right? Well, no. Because those fraudulent orders, if shipped, mean revenue leaking away from the business. And the very threat posed by an

increase in the raw number of fraudulent attempts, also means that fraud teams frequently become overly conservative and turn away good orders. To add to the subtleties, some verticals — think jewelry, outdoor goods, home improvement — might see their big order surges in seasons other than the holiday season.

February for jewelers, May for outdoor goods, springtime for home improvement.

Among many things that the COVID-19 pandemic has left in its wake is an ecommerce industry that is changing dramatically, but in ways that are not yet entirely clear.

So for now, understanding and preparing for fraud requires even more sophistication than it has in the past.

## Fraud is not a one-size-fits-all problem

Let's break down a few of the top verticals to illustrate the point. The last quarter of 2020 was historic in terms of ecommerce.

As we said earlier, online sales were up 500% on Black Friday over pre-pandemic levels. The period saw the biggest quarterly ecommerce sales in the biggest year of ecommerce sales, according to Signifyd data.



And while fraud pressure was high across a number of verticals in Q4, it was also highly variable. Signifyd data, for instance, shows that by one measure fraud attacks were 10 times higher against general merchandisers — merchants that resemble department stores — than it was against Home Goods & Decor retailers. Electronics and Fashion, Apparel & Luggage saw similar pressure, while attacks against Luxury Goods landed between those two verticals and general merchandisers.

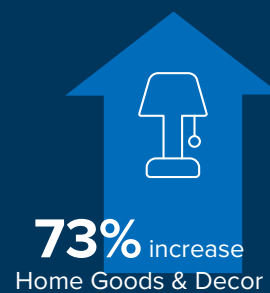
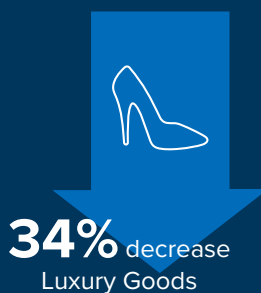
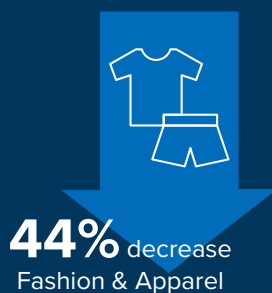
Data from the first quarter of 2021 serves to underscore the point: Fraud is not one-size-fits-all.

For the most part, with the holiday season over, fraud attacks began to subside. Fashion saw a 44% decline in fraudulent orders. Attacks against Luxury Goods merchants dropped nearly 34%. General merchandisers and Electronics merchants saw double-digit-percentage declines in fraudulent orders.

But Home Goods & Decor retailers? They would have been wise not to get too comfortable with their Q4 numbers. Attacks against home goods merchants increased 73% in Q1 2021 compared to the previous quarter.



### Q1 2021 Fraud Pressure Impact Across Select Verticals





## The ebbs and flows of fraud pressure

While the holiday season inspires intense focus by fraudsters and ecommerce leaders alike, a longer-range look at Signifyd's Fraud Pressure Index demonstrates that the ups-and-downs of fraud attacks stretch throughout the year.

The examples are many, but consider that in September 2020, fraud pressure in the Fashion, Apparel & Luggage category had dropped 28% from its January 2020 benchmark. Time to party? Well, no. Two months later, heading into Black Friday, fraud attacks were up nearly 400% from the benchmark. It settled in at about double January 2020 for most of the first half of 2021, but blips approaching 300% plagued the vertical in March.

Contrast that with Electronics. At the same time apparel was contending with its biggest fraud assault in months, fraud attacks on electronics merchants were up 25% and things got better from there with fraud pressure dropping 41% below the benchmark in the days before Christmas.

You've probably guessed it: That good fortune didn't last. By mid-January attacks were 81% higher than the benchmark. In fact, by Spring they were up 156% and they rose to 180% by mid-summer.

Pick any vertical and you can tell the same story of swings in order volume, fraud pressure and counter-measures to ease fraud.



Given the up-tick in international cyber attacks over the course of 2021, it's even more important than ever to protect both your company and customers from online fraudsters. Finding and utilizing the right software and partner to implement and manage this part of your ecommerce business is vital; both for the remainder of 2021 and for years to come.

TONY PUCETTI, COO



The lesson in all this is that retailers need to be agile when it comes to fraud protection. Constant vigilance is great, but it gets you only so far. Retailers in 2021 and beyond, need to be prepared to scale up in the face of order spikes and changes in the nature and timing of fraud attacks.

Increasingly merchants are embracing machine learning solutions that can scale immediately and infinitely to match changes in the market. And they are seeking tech-solution partners that can also provide intelligent advice and guidance when it comes to best risk practices and how to weave those practices into the enterprise's overall goals.

Leading digital agency and Signifyd strategic partner, Blue Acorn iCi, regularly speaks to ecommerce clients about the mounting risks of fraud attacks. They consistently recommend a combination of automated and manual solutions to ensure legitimate orders don't get rejected while stopping fraud. The approach minimizes the loss of sales.

"Ecommerce fraud protection is critically important for any merchant transacting online, at any time of the year," said Tony Puccetti, COO at Blue Acorn iCi. "Given the up-tick in international cyber attacks over the course of 2021, it's even more important than ever to protect both your company and customers from online fraudsters. Finding and utilizing the right software and partner to implement and manage this part of your ecommerce business is vital; both for the remainder of 2021 and for years to come."

The most successful merchants know that simply constricting the flow of orders as a way of avoiding fraud kills revenue and the customer experience that so many retailers work so hard to enhance.

## Holiday predictions from Signifyd's Risk Intelligence Team

As the gap begins to close between what daily ecommerce looks like compared to the holiday shopping season, the question of what fraud trends to anticipate trickles into the picture. For Signifyd's Risk Intelligence team, this question is particularly top of mind with the 2021 holiday season just around the corner and with spikes in daily order volume creeping close to numbers seen during holiday season.

However, as many members of the Risk Intelligence team echo, drastic increases in order volume do not necessarily correlate to increases in fraud.

As Risk Analyst Frederikke Rasmussen explained, "During the holiday season, we will have an increase in order volume, but that doesn't necessarily mean an increase in fraud cases. That increase is typically from an influx of good orders coming in."

“



Overall, what I've noticed this year is that the fraud we are seeing has become more complex; particularly with the occurrence of account takeover fraud increasing. So many more accounts can and are being compromised across the board and I don't see it stopping anytime soon, especially during the holidays.

LUZ CERVANTES, MANAGER OF RISK INTELLIGENCE, SIGNIFYD



Instead, when predicting what fraudsters will be up to this holiday season, the Risk Intelligence team is looking back to observations made during the pandemic and comparing them to pre-pandemic fraud trends. It's essential, considering how much the landscape has changed, especially with this being the first post-pandemic holiday season for many parts of the world.

## What to look out for in an uncertain landscape

For lead risk analyst, Irish Show there is one specific fraud tactic he has his eyes on this holiday season. It was particularly prevalent prior to the pandemic.

“What stands out comes from the last two years when we saw two mule fraud attacks that happened in December,” said Show.

Despite recent Commerce Network data that shows mule fraud numbers being down significantly, Show explained this absence is not uncommon when it comes to mule fraud. “Once caught, mule fraud attacks can disappear, six, seven, eight months at

times. But mule fraud has a habit of reappearing. We [Signifyd] scare them away from our merchants and after a period of time they will come back and try another attack. I will enter this December with the last two years in mind; going into this period looking for mule fraud. That's when I expect it.”

Lead risk analyst Colin McCloskey's observations over years point towards a different, yet repetitive fraud trend.

“Naturally, we see order volume increase during the holiday season. With that holiday volume, bot attacks will increase. These attacks are difficult to track because they can be misinterpreted as holiday volume, allowing them to fly under the radar,” said McCloskey. “If these attacks aren't caught early on, they can create issues beyond the holiday season; this can open up downstream fraud issues, like ATO (account takeover) or email account takeover. It becomes a chain reaction.”

Speaking of ATO, for manager of risk intelligence, Luz Cervantes, this is the exact trend she is seeing a particular spike in and anticipating to be a key fraud player in the holiday season.

“Overall, what I've noticed this year is that the fraud we are seeing has become more complex; particularly with the occurrence of ATO fraud increasing,” said Cervantes. “So many more accounts can and are being compromised across the board and I don't see it stopping anytime soon, especially during the holidays.”



## The true fraud trend for 2021

In an almost poetic way of coming full circle, it would appear that instead of asking what fraud pressures will emerge this holiday season, the question is: How have these trends changed and how likely are they to endure beyond the holiday season.

Take for instance the use of promo codes, an expected tactic used by merchants to attract customers during the holidays.

“This isn’t restricted to the holiday season, but we do see this during that time — customer abuse through promotion abuse, trade ins, or any value-add that the merchant is offering,” said McCloskey. “A merchant may look at certain value-adds as revenue drivers, but there is a fine line between adding value for the customer and leaving an open door for fraud or abusive customers.”

As merchants prepare for this holiday season, the predictions from the Risk Intelligence team all point towards remaining vigilant. Vigilance in the sense


of being prepared for the fraud trends that have made themselves known in holiday seasons of the past, but also aware of the fact that these trends have shifted, making it easier for them to potentially go unnoticed during the influx of holiday volume and potentially create more issues outside of the holiday season.



A merchant may look at certain value adds as revenue drivers, but there is a fine line between adding value for the customer and leaving an open door for fraud or abusive customers.

COLIN MCCLOSKEY, LEAD RISK ANALYST, SIGNIFYD





### Part 3: The corresponding metamorphosis of fraud and risk teams

With online fraud taking on new looks in the golden age of ecommerce fraud, fraud and risk teams are transforming themselves as well. Armed with smart machines and mounds of data, they are no longer playing defense.

Rather than focusing on loss avoidance, modern risk teams have seized the role of optimizing the business. By reframing their role, progressive risk teams are no longer seen as a cost center and instead are seen as a revenue generator.



## Fraud teams have risen in prominence with ecommerce

The truth is, fraud teams can no longer afford to be in a defensive crouch. Since the dawn of ecommerce, the online side of the retail house has been somewhat shielded from the ill effects of an economic downturn or a strategic misstep by the business.

Online sales made up only a single-digit percentage of revenue for many retailers. But with the surge in ecommerce during the pandemic, ecommerce revenue reached 33% of retail sales. Now online is a key part of the business and it needs to perform like it.

And so, fraud prevention has become risk intelligence at forward-thinking retailers. Risk teams are no longer cost centers being asked to squeeze spending while improving performance.

At the most successful retailers, risk teams work on enabling the enterprise's strategic objectives.

They turn to artificial intelligence to maximize approval rates with decisions that are made in real time.

They are architects of solutions that change the state of retail operations, allowing buy online, pickup in store and curbside pickup to run efficiently and profitably. They are a catalyst for a move into the future.

They are key partners in building a memorable customer experience.

Risk teams that have embraced this new role are looking at commerce protection in a new way. They understand that retail leaders know what to do in order to compete — particularly with dominant players like Amazon.

They understand that many ecommerce executives have been unable to act, because they are afraid of what might go wrong if they take risks.

But embracing modern fraud solutions, built on data and artificial intelligence and backed by a financial guarantee spurs a mind shift — a shift to fearless commerce.

“



Since using Signifyd, we've added thousands of dollars in revenue we would normally have declined. They're approving what we considered our riskiest orders, and we've been able to open up many new international countries as well.

KAITLIN HUTCHINSON, FORMER DIRECTOR OF ECOMMERCE





## Part 4: Assessing your fraud maturity

As we've seen, the ecommerce landscape is one that is continually shifting, and with it so do fraudsters and their tactics.

For risk and fraud teams, adaptability and agility are now more than ever important core competencies necessary to prevent the costly revenue leakage that can ensue from fraud attacks or throughout an order's lifecycle — at the payment gateway, the card processor, through anti-fraud efforts and even after delivery, through returns and chargebacks.

As with any efficient team, taking the time to assess and identify areas of improvement are key to long-term effectiveness; especially when it comes to your fraud team, one of your first lines of defense against revenue leakage.



Take the assessment [here](#) to see what your team's fraud maturity is, evaluate current processes, and receive insights on opportunities and recommendations tailored for your team.



Produced by:



Mike Cassidy,  
Head of Storytelling



Luz Cervantes,  
Manager of Risk Intelligence



Alyssa Gray,  
Product Marketing Manager



Irish Show,  
Lead Risk Analyst



Ping Li,  
Senior Director of Risk Intelligence



Colin McCloskey,  
Lead Risk Analyst



Ben Davidson,  
Manager of Risk Intelligence



Frederikke Rasmussen,  
Risk Analyst



Ashley Kiolbasa  
Director of Product Marketing

With contributions from:



## About Signifyd

Signifyd provides an end-to-end Commerce Protection Platform that leverages its Commerce Network to maximize conversion, automate customer experience and eliminate fraud and customer abuse for retailers. Signifyd counts among its customers a number of companies on the Fortune 1000 and Internet Retailer Top 500 lists. Signifyd is headquartered in San Jose, CA., with locations in Denver, New York, Mexico City, São Paulo, Belfast and London.



Contact us to learn more about operating in the new era of ecommerce.

### HEADQUARTERS

2540 North First Street, 3rd Floor  
San Jose, CA 95131  
U.S.A.

—

### WEB

[www.signifyd.com](http://www.signifyd.com)

### SUPPORT

[www.signifyd.com/contact](http://www.signifyd.com/contact)