Signifyd

The State of Fraud and Abuse 2024

The industrialization of online fraud has changed the rules — and the stakes — of the game

How the industrialization of fraud has unleashed a highly sophisticated menace

While organized crime's assault on brick-and-mortar retail has been well-documented, a more menacing organized crime wave has flourished in its shadow. Granted, ecommerce fraud is not as visually dramatic as the smash-and-grab robberies at physical stores that play on a continuous cable news loop. But sophisticated rings engaged in online digital theft can steal in a matter of minutes what it takes crime rings weeks to haul off from physical stores.

Juniper Research reported that online brands lost more than $48 billion to ecommerce fraud in 2023, up from roughly $41 billion in 2022. And the picture doesn't get any brighter with Juniper predicting that cumulative online retail fraud losses between 2023 and 2027 will top $343 billion.

Online brands lost more than

$48 billion

to ecommerce fraud in 2023

No question, fraud pressure is growing along with the growing sophistication of those who commit ecommerce fraud. Signifyd's Fraud Pressure Index — a measure of the rise and fall of orders arriving with enough red flags to be presumed fraudulent — rose 19% between the first half of 2023 and the first half of this year, according to Signifyd data.

Signifyd's fraud pressure index rose

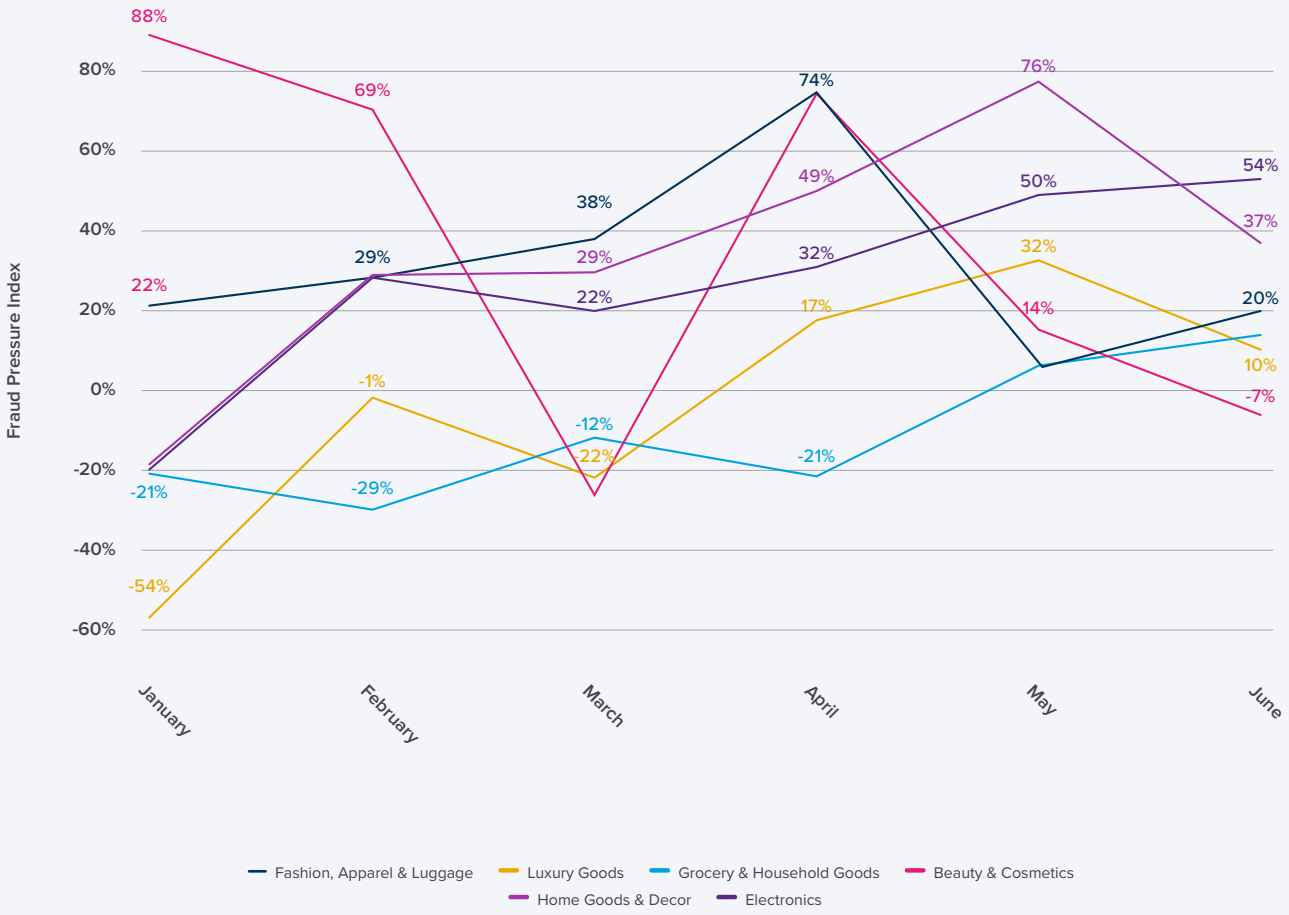
19%

between this year and last

Fraud pressure doesn't discriminate when it comes to retail categories

Traditional payment fraud continues to be a key concern for online merchants — with good reason. Signifyd data for key verticals show a consistent year-over-year rise in the fraud pressure index during the first half of 2024. Four out of six key verticals saw a significant annual increase in fraud pressure during the first six months of the year.

Fraud pressure trended higher in the first half of 2024



Not only are payment fraud losses staggering and growing, but criminal rings are more frequently branching out, attacking every segment along the buying journey and every one of the growing number of digital devices now used to order online. Not content to target checkout with stolen credentials, fraud rings now are more often infiltrating consumer accounts, engaging in promotion abuse, launching costly unauthorized reseller schemes and finding ways to take advantage of post-purchase interactions through refund and return fraud.

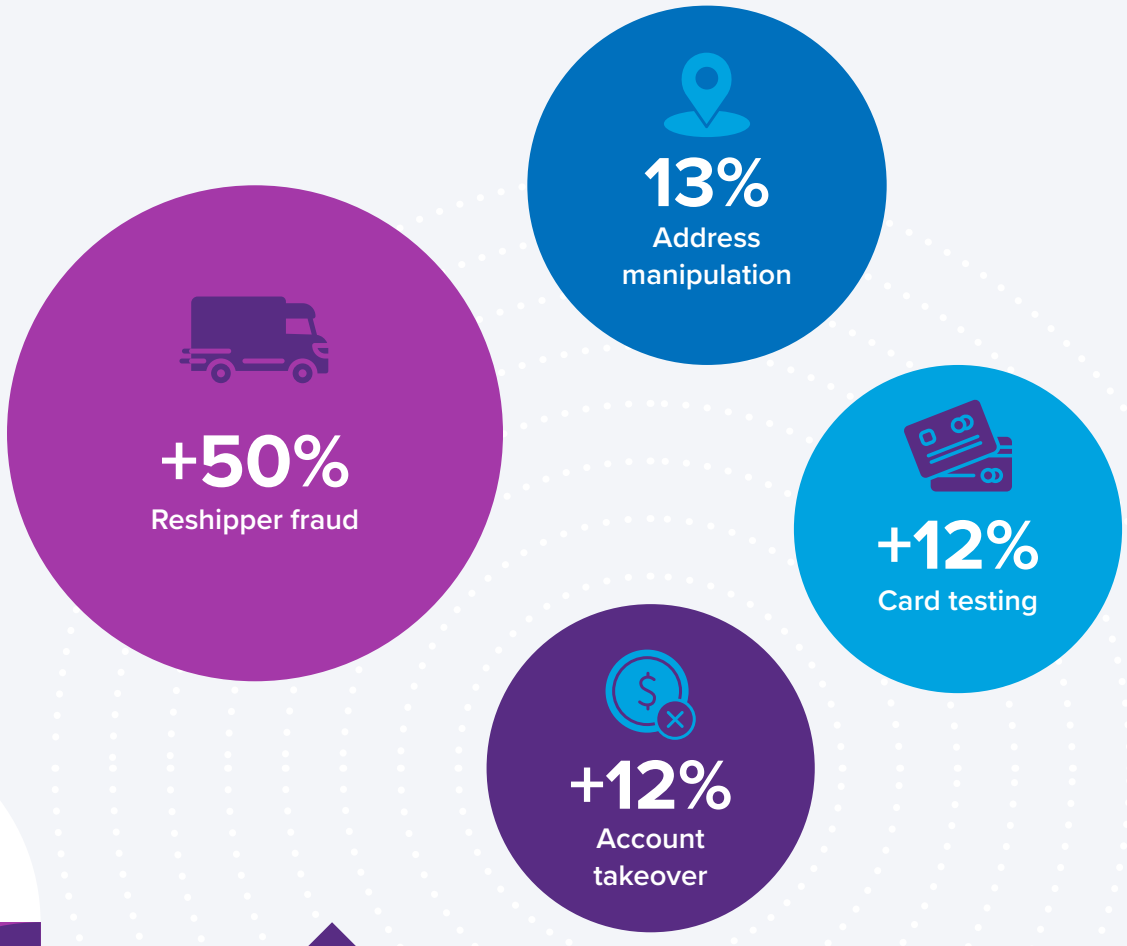
All of this is happening at a scale that experts say they have not seen before.

Calling organized crime "one of the most sophisticated industries in the world," Mastercard's head of identity solutions, Chris Reid, offered his take on the expansion of online fraud — by volume, velocity and vector — during Signifyd's FLOW Summit 2024 in April.

"It is organized crime who are attacking every single one of those vectors," Reid said. He then took audience members on a mind-bending tour of the diabolical digital choreography that makes industrialized fraud run in 2024.

Reid described a growing industry, fueled by highly skilled identity thieves and common burglars who bypass electronics during home break-ins and instead go for passports, driver's licenses, bank statements — anything that will help steal existing identities or create new, synthetic ones.

Fraud rings have grown bigger and become better at what they do by turning to new methods or by being increasingly creative with old tactics. Fraud committed through the use of reshippers and often involving unauthorized reselling is up 50% in the last year, Signifyd data shows. Address manipulation to disrupt pattern recognition is now evident in 13% of transactions, according to the data. Card-testing attempts and account takeover are both up 12%.



Artificial intelligence has taken on a new prominence in driving fraud attacks. Criminal rings are building massive, international organizations staffed, heartbreakingly, through human trafficking and indentured servitude.

And as online fraud becomes more varied and prevalent, retailers' conundrum becomes more complex. How do you redouble your protection without creating more friction for the majority of consumers who you value because they are valuable? How do you better insulate your revenue and profits from malicious raiders while warmly welcoming your best customers to buy from you easily and enjoyably?

The State of Fraud and Abuse 2024 will explore how the disturbing new trends are playing out in real life and the new, innovative ways fraud fighters are responding with creativity and technologies of their own. We will also talk to some of those on the front line of ecommerce and hear about the threats they see and why they do what they do to protect commerce and consumers from fraud and abuse.

Table of contents

Glossary

Consumer abuse — Online fraud most often committed by the rightful credit card holder. For purposes of this report, consumer abuse is measured by the number of non-fraud chargebacks Signifyd challenges as illegitimate. Schemes include falsely claiming an order never arrived or a satisfactory order arrived in unsatisfactory condition or failed to live up to its description. Consumer abuse also includes policy abuse, such as promotion abuse and unauthorized reselling.

First-party fraud and abuse — Fraud and deception committed by the rightful credit card holder. It's an umbrella term that covers a card holder falsely claiming they didn't make a purchase that they did make — sometimes that's an honest mistake, sometimes it's an attempt to game the system. For the purposes of this report, the term also includes false claims that an order never arrived or that a satisfactory order arrived in unsatisfactory condition or failed to live up to its description. First-party fraud and abuse also includes policy abuse, such as promotion abuse and unauthorized reselling.

Fraud pressure — A measure of fraudulent activity online. An online order is considered to be contributing to fraud pressure if it contains a number of anomalies and red flags so great that the order is presumed to be fraudulent by machine learning models or a combination of machine learning models and fraud analytics experts.

Fraud pressure index — A measure that represents the percentage change in fraud pressure over a given period of time, generally year-over-year in this report.

Payment fraud — Online fraud committed at checkout with a payment instrument. Payment fraud is typically committed with stolen credentials, synthetic identities or some form of identity misrepresentation.

in a survey of more than

1,100

63%

saw an increase in first-party fraud

Consumer abuse is the challenge most on retailers' minds

Payment fraud persists, but it's the growing challenge of consumer abuse that has riveted merchants' attention in recent years. In a survey of more than 1,100 merchants published this year, 63% told the Merchant Risk Council (MRC) that they'd seen an increase in first-party fraud in the past 12 months. And 48% and 45% of respondents respectively said refund and policy abuse and first-party fraud are now the two biggest threats to their businesses.

As if to underscore the severity of what could reasonably be called a first-party abuse crisis, the MRC took the unusual step of sending an email alert to all its members warning of an ongoing "unprecedented increase in fraudulent activity" targeting first-party misuse, including refund and return policy abuse.

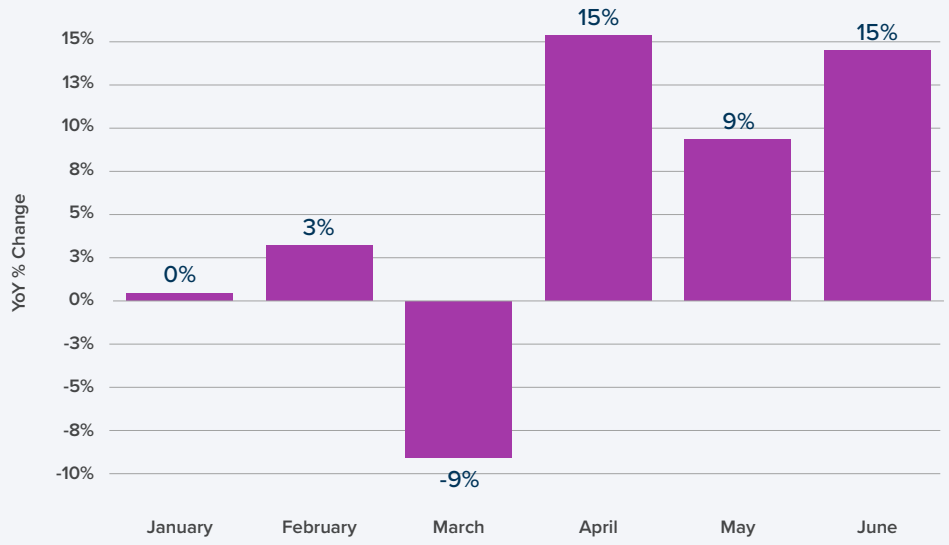
The late July email, from MRC CEO Julie Fergerson, strongly suggested that criminal rings and so-called "fraud-as-a-service" operations were involved in "a marked rise" in first-party fraud and abuse in the past month and the "significant financial loss" it had caused.

"We suspect that the fraudsters are sharing this information and that the volume we are hearing about is either systemic, organized through various online fraud as a service sites or both," Fergerson wrote to the MRC's 600 members, including retailers, fraud solution providers, law enforcement agencies and others.

Fraud fighter Catherine Tong, a partner at payments consultancy and MRC member Allyiz told Signifyd that she sees two main reasons for the increase.

"It's partly because of the refund-as-a-service type of services that exist and that have been promoted online," Tong says. "But I think it's also a reality of the current economy as well, that as people want to still live the lifestyle that they've had and got used to but maybe can't afford anymore, they're trying to find ways to still get the products and services that they want, and one way to do that is to exploit returns, loopholes or customer service goodwill gestures."

Year over year change in consumer abuse for all verticals



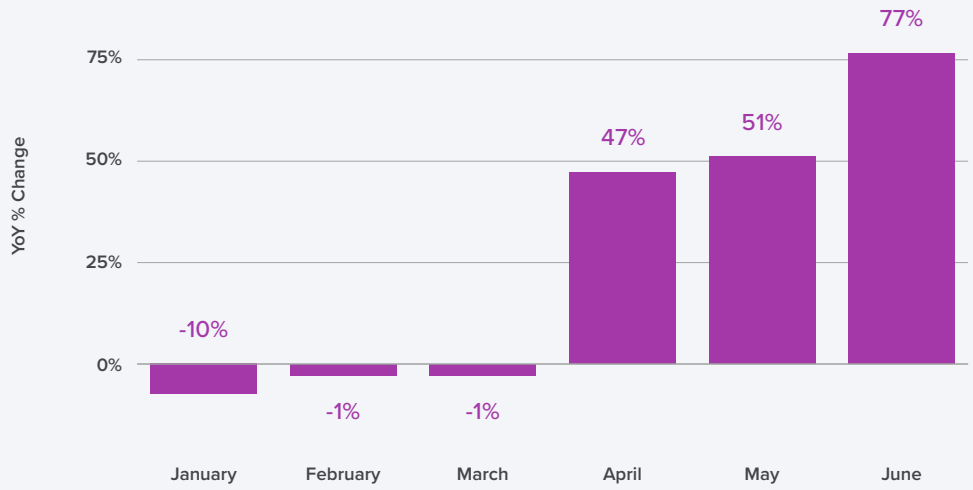
Consumer abuse 2024 by retail category — apparel

The apparel vertical had a bumpy first half of 2024, but finished the first six months of the year with online sales up 2% over a year ago, according to Signifyd data. On top of that, fraud pressure in the vertical continued to rise, up 30% in January through June compared to the same period in 2023. Consumer abuse numbers presented a bright spot for apparel — at least early in the year, when abuse was down considerably. The respite was short-lived, however, as abuse turned up dramatically starting in April. The vertical holds an unenviable distinction when it comes to its battle against abusive behavior such as falsely claiming a package never arrived and other forms of first-party fraud attempted through the chargeback process. While apparel retailers work to guard against that, they have other worries. Online apparel return rates hover around 25%, according to Coresight Research, far above the overall ecommerce average of 17.6%, cited by the National Retail Federation. Apparel brands confront wardrobing — or wearing an item once or twice and then returning it for a refund — and bracketing — buying several versions of the same garment and returning all but one. While the challenges for apparel are significant, so is the upside from stymieing those with ill-intent while removing friction for good customers.

Online apparel return rates hover around

25%

Consumer abuse in the apparel vertical



Online apparel sales were up over last year by

2%

Fraud pressure in the vertical was up by

30%

compared to the same period in 2023

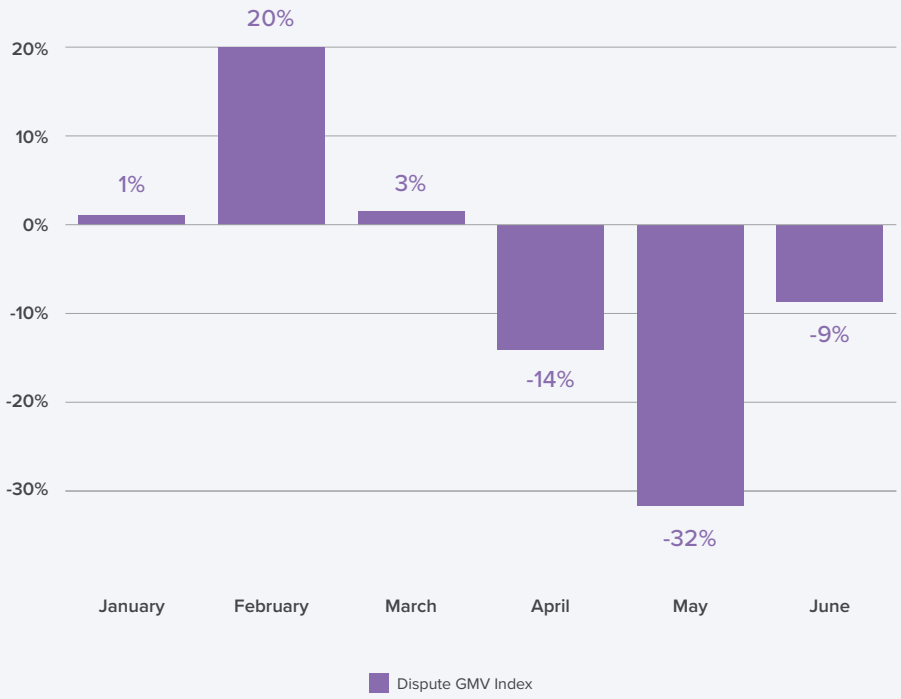
Consumer abuse 2024 by retail category — grocery

Grocery was something of an ecommerce tiger in the first half of 2024. Online sales were up 23% compared to 2023. And the vertical has been having a good run against payment fraud, too, with fraud pressure down 12.6% compared to the first half of 2023. Consumer abuse has been more of a wild ride for online grocers in 2024. Abuse grew throughout the first quarter over year-ago figures. The picture was brighter in the second quarter, when abuse was lower than the previous year, falling by as much as 32% year over year in May. The fact is, no matter the vertical, trouble can appear in a highly inconsistent way. Breaking abuse down by retail vertical reveals spikes by category and by time of year. Such peaks and valleys can reflect organized attacks by sophisticated fraud organizations or the cat-and-mouse nature of fraudster vs. fraud fighter. A particular consumer abuse scam might have a popular run, spread by word of mouth and even be repeated by certain individuals. Once it's shut down, the bad actors need to regroup and revise their schemes.

Online grocery sales up on 2023 by

23%

The ups and downs of consumer abuse in the grocery vertical



Customer abuse fell year over year in May by

32%

Consumer abuse 2024 by retail category — luxury goods

High-priced and highly desirable, luxury goods are a fat target for online fraudsters whether the status-affirming items are stolen through payment fraud or consumer abuse. The category had a strong start to 2024 with online sales up 4%, according to Signifyd data. Meanwhile fraud pressure in the first half was down 9.4% compared with 2023. Of course, payment fraud is only part of the equation. Bad actors turn to abuse schemes to pilfer designer goods for profit and personal use. While abuse in the category cooled compared to early 2024, luxury retailers still face the challenge of being prime victims for those looking to get the goods for free. Devanshu Agarwal is the DTC payment risk manager for On, which sells high-end sportswear, including designer athletic shoes by Loewe. He says luxury items are in the sweet spot for fraudsters. “Because Loewe is a luxury brand, expensive shoes,” Agarwal says, “it’s a target for payment fraud, but also reselling.”

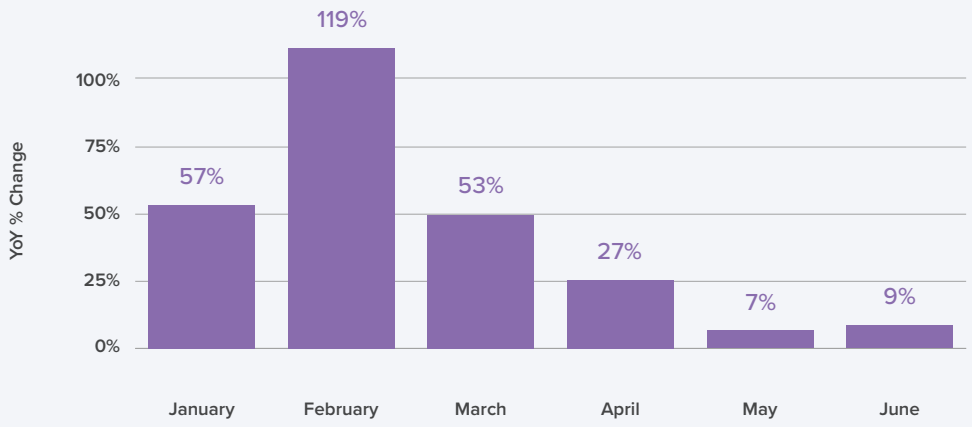
Luxury goods online sales up in 2024 by

4%

Fraud pressure down in the first half of 2024 by

9%

Luxury goods consumer abuse 2024 vs. 2023 Consumer abuse



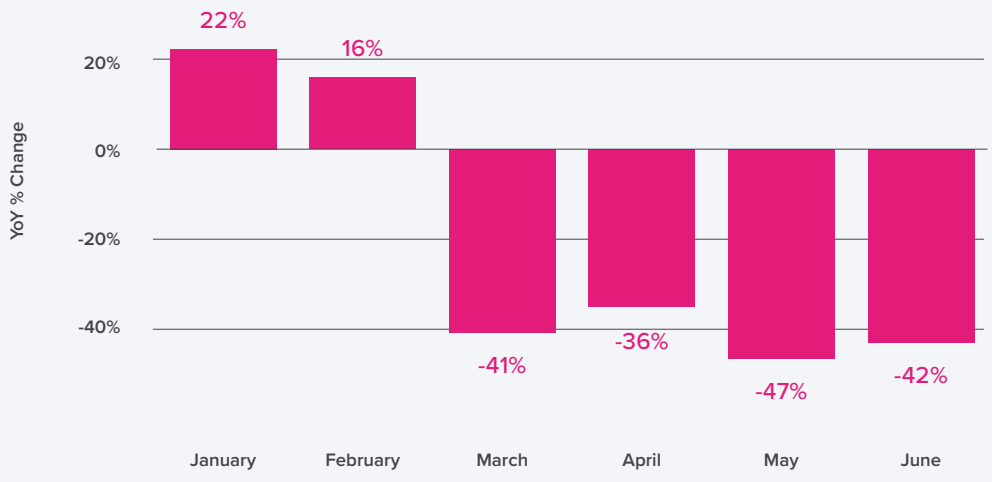
Consumer abuse 2024 by retail category — beauty and cosmetics

The beauty and cosmetics vertical had a down first half of 2024 when it comes to sales — with online revenue slipping 9% year over year, according to Signifyd data. On the upside, the category also saw a significant drop in fraud pressure, which declined 9.4% compared to 2023. And after a moderate increase in consumer abuse — peaking at a 22% year-over-year increase in January — beauty and cosmetic retailers seem to have gotten a handle on the problem. Consumer abuse during March through June was down, ranging from about 35% to nearly 50% compared to the same months in 2023.

Beauty and cosmetics fraud pressure dropped

-9%

Beauty and Cosmetics consumer abuse 2024 vs. 2023



Consumer abuse 2024 by retail category — home goods

The home goods category started out the year slowly, with sales in the vertical down 1% in the first half over the previous year. Along with lackluster sales, the vertical saw attempted payment fraud skyrocket — with fraud pressure showing a 32.3% increase over the first half of 2023. While a number of verticals saw big increases or peak increases in consumer abuse early in 2024 before experiencing relief, the trend headed in the other direction for the home goods sector. If there is reason for optimism in the category, it's that after a big jump in abuse in May, the increase in attacks slowed somewhat in June. Consumer abuse can be particularly difficult for home goods sellers to anticipate and prevent. The category is not prone to high purchase frequency given the relatively high cost and durability of items like furniture and appliances. A single retailer that depends on only its own transaction data would have limited visibility into the identity and intent of purchasers due to their relatively infrequent purchases.

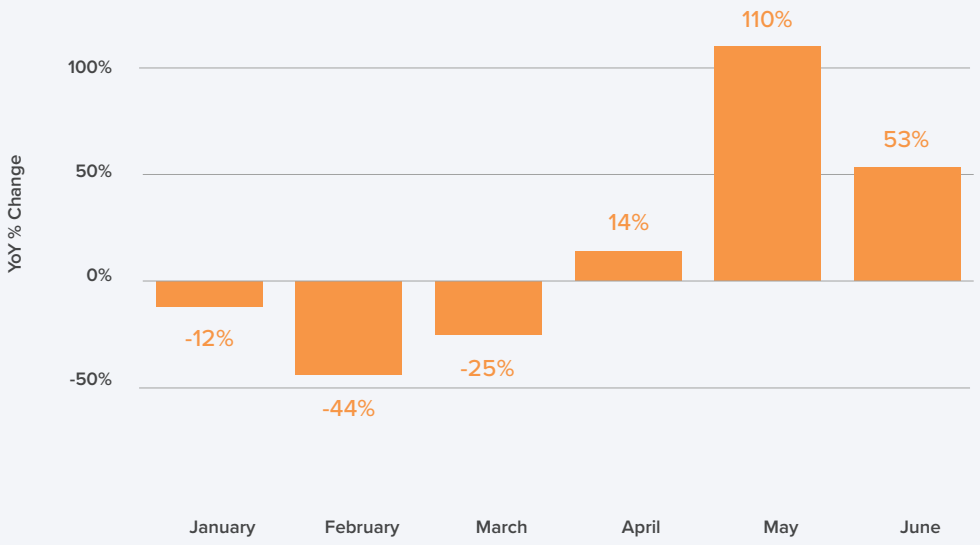
Home goods fraud pressure increased in first half of 2023 by

32%

Sales in the home goods vertical down in the first half of 2024 by

1%

Home Goods consumer abuse 2024 vs. 2023



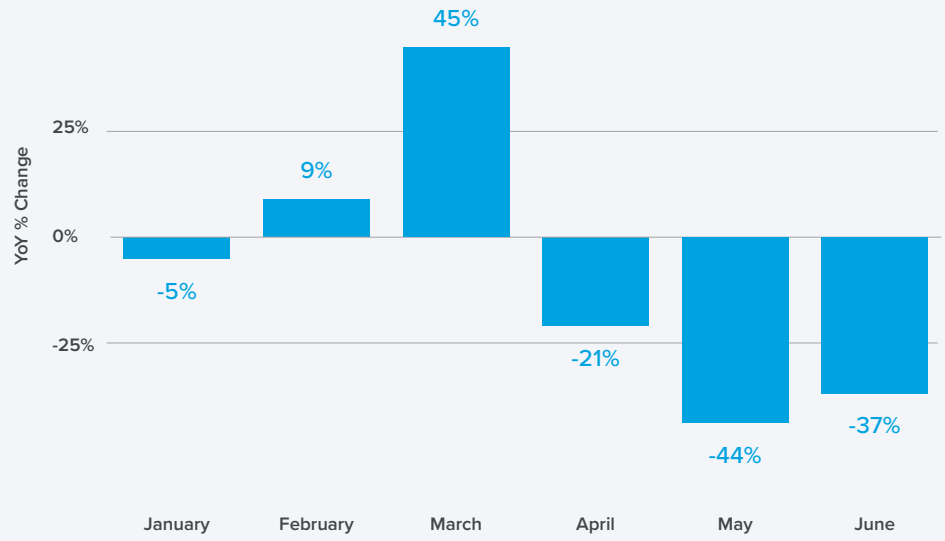
Consumer abuse 2024 by retail category — electronics

Electronics sales slowed online to begin 2024 with sales in the vertical down 1% compared to the first half a year ago. The sluggish sales were accompanied by a dramatic rise in fraud pressure, which increased 24.8% over the first half of 2023. The vertical's best news came in the area of consumer abuse. Electronics saw abuse drop in every month but two during the first half of 2024. March provided a fairly dramatic spike in consumer abuse attacks, reaching 45% higher than the same month a year ago. The good news is that as the year wore on, the numbers for electronics got much better with a strong decline in April and drops in May and June that were roughly double the declines that the category saw in April. The electronics category generally features high-priced items that are not frequently replaced. That makes it difficult for any one retailer or even a retail chain to predict whether a consumer is likely to be an abuser based on past transactions and post-transaction behavior.

Fraud pressure in the electronics vertical increased

25%

Consumer abuse 2024 by retail category — electronics



In March consumer abuse attacks reached

45%

Higher than the same month a year ago

State of Fraud and Abuse 2024 key findings

Growing industrialization of fraud

Ecommerce fraud is increasingly being committed by very large and sophisticated global fraud rings. These rings have taken on the hallmarks of Fortune 500 businesses, specializing in online commerce, fulfillment, payments, post-purchase policies and social engineering. There is increasing evidence that some are also involved in human trafficking to assemble the workforce they need for their growing enterprises.

Rise of promo abuse & first-party fraud

As fraud prevention specialists steadily improve their ability to fend off payment fraud and as fraud rings — and wayward consumers – grow in sophistication, fraudsters are increasingly attacking all segments of the buying journey. Refund and return abuse are on the rise. Bad actors are finding ways to profit from promotion abuse and unauthorized reselling. More than 60% of online brands surveyed by the Merchant Risk Council report increased first-party fraud.

+60%

of online brands report increased first party fraud

AI is transforming fraud

Fraud rings have embraced artificial intelligence — including Gen AI — to help scale their operations. AI facilitates rapid-fire card testing and large-scale purchases of high-demand items for unauthorized reselling. Phishing has entered a golden age. But fraud fighters have also increased the use of AI to understand the identity and intent behind purchases by leveraging large networks of retailers which allows them to anticipate trouble and block illegitimate transactions.

Fraud fighters are optimizing business results

Fraud fighters have taken on a new importance and a new attitude as enterprises turn to the latest generation of fraud and abuse solutions. Fraud and risk teams no longer see their roles as primarily defensive. Instead of leading with stopping fraud, modern fraud and risk teams are on a mission to optimize the business by increasing the number of good orders they approve, thereby improving the customer experience and building enduring customer lifetime value.

The growing menace of online fraud:

New methods, new targets, new technology

The rapid industrialization of ecommerce fraud

While there's been a lot of media talk about organized retail crime in the brick-and-mortar world, relatively little attention has been paid to a potentially more sinister crime wave growing in its shadow.

Online fraud carried out by sophisticated and highly organized criminal rings is growing at an alarming rate. Just as ecommerce as a channel has accelerated rapidly since the COVID era, criminal attacks against those selling online have exploded in recent years.

Like any industry, the fraud industry is organized as a whole ecosystem — criminal enterprises that specialize in supplying the raw material to provide stolen identities and create fake ones, the go-betweens, who package and sell the stolen identities on the dark web and create and polish the fake ones. Then there are the criminal organizations that use the identities to steal money, products and services.

Chris Reid of Mastercard filled a 40-minute presentation at Signifyd's FLOW Summit with examples of "the explosion of fraud markets" and the growing sophistication the dark industry trafficking in stolen documents, forged forms, synthetic identities and pilfered goods. A relatively new favorite of the criminal class: drop accounts — accounts made up from whole cloth and indistinguishable from legitimate accounts used by a merchant's best customers.

"It's going to look like people" Reid said of a drop account holder. "And they are people who are fully verified in the financial services system. They have a card. They have an account. They can move money in any way. They can pay for things in any way. They can start a merchant relationship in any way and yet they are not who they claim to be. They are criminals. They are fraudsters."

The industry relies on suppliers who steal checks, passports, drivers licenses and work with insiders to forge financial documents — all in the services of committing fraud.

"So if you think about your home being burgled 10, 15 years ago," Reid said at FLOW, "they might have taken your DVD player, your TV. Actually, that's borderline worthless. Now what they're going for during many thefts and burglaries is, they're going for identity documents."

Not only have the number, size and sophistication of attacks grown, but the scope of the attacks has spread throughout the online buying journey. Where once checkout was the focal point, now the entire buying and post-purchase process is vulnerable to sophisticated forms of attack.

You ask about the state of fraud and abuse in 2024?

"Fraud was mainly focused on when you make a purchase and you have that moment of that checkout button," says Signifyd Senior Manager, Risk Intelligence Xavi Sheikrojan. "Then fraud moved into account takeover, which is earlier in the purchase process. You also have the different types of abuse schemes that are also new, where AI is playing a part in it. People are figuring out ways to buy products and commit return abuse schemes, refund abuse schemes, etcetera. So it moves away from that checkout button toward other angles in the customer purchase process. I envision that, that will continue to become bigger. And again, the attacks are at scale in every segment of the journey. That's where I envision fraud evolving in the next two to five years."

If you ever doubted fraud was growing more sophisticated today, consider that a fraud organization specializing in identity theft nearly stole Graceland, the iconic Memphis landmark that was once home to Elvis Presley. The ring, apparently based in Nigeria, had the legal wheels in motion for a sale, before giving up on the scheme. You can look it up.

As for the scale of brick-and-mortar organized retail crime versus organized online crime, compare the large-scale ring of alleged physical retail thieves that law enforcement recently broke up in San Jose, California — home to Signifyd's headquarters. Officers arrested 13 people who were accused of stealing $150,000 worth of merchandise from Home Depot, Target, Kohl's, Lowe's, Macy's and Sunglass Hut over an extended period. Contrast that with a fraud ring that Signifyd has been monitoring for nearly two years. During the 2022 holiday season, the ring based in Southeast Asia stole an estimated $660 million in laptops, cell phones, computer chips, gaming devices and other goods from online brands across the United States during one month. At its peak that November, the ring was placing a fraudulent order a minute at one merchant on Signifyd's Commerce Network.

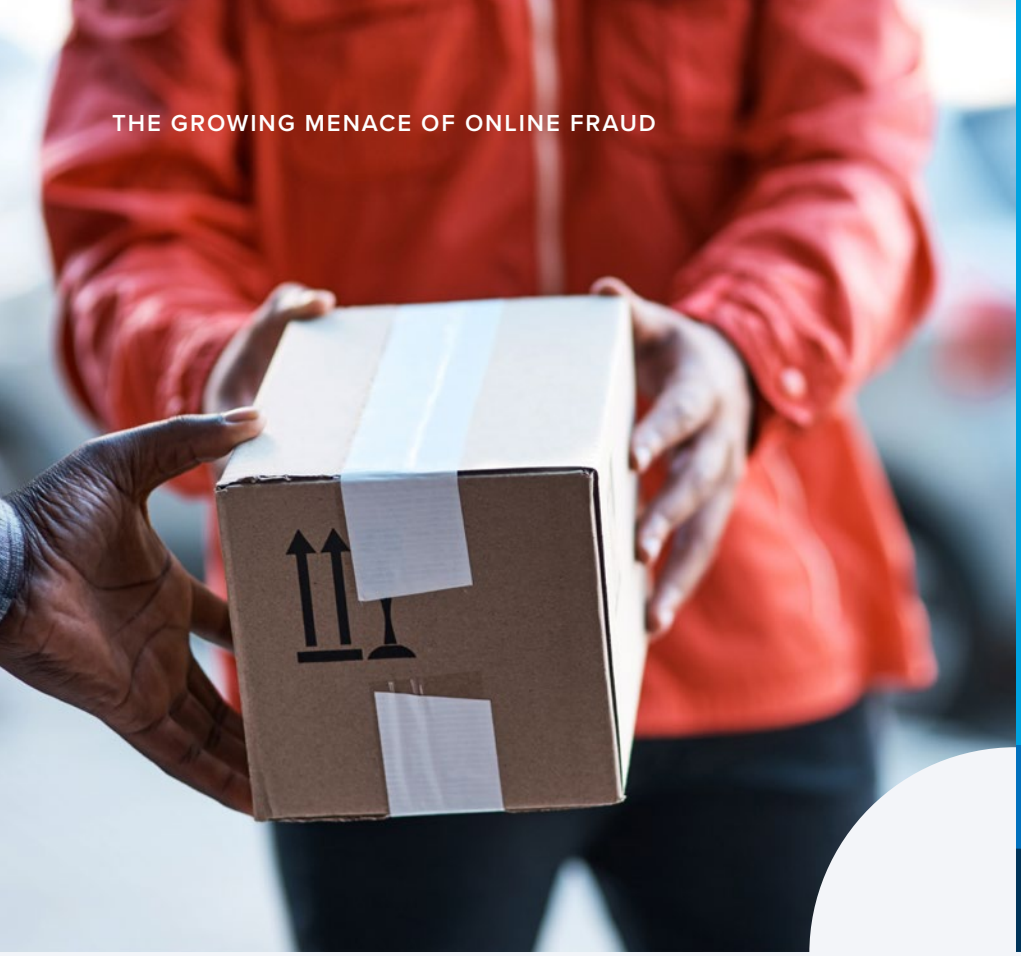
Signifyd quickly shut down the attack on its network and many of the fraudulent orders were turned away. But rather than move on, the fraud syndicate iterated and morphed and resurfaced.

A ring based in Southeast Asia stole an estimated

$660 million

Traditionally, fraudsters find vulnerability and attack repeatedly until they're shut down. Then they go away, says Signifyd Strategic Account Executive Caleb Hanson, who's made a study of the ring: "Their approach was different. Much more like cyber attacks. They would find targets and find ways to be successful. They went after a lot of companies that had manual review and order spikes. They went after electronics, gift cards and fashion."

Chief among their new tactics was address manipulation — making small changes or adding odd punctuation or symbols to an address — just enough to throw off machines, but not so much that humans delivering orders would have trouble getting the goods to the right address. The move was paired with the use of reshippers, companies that have a legitimate role in commerce but can be used to cloak fraudulent activity, too.



Signifyd detected an increase in reshipper fraud of

50%

and a boost in address manipulation of

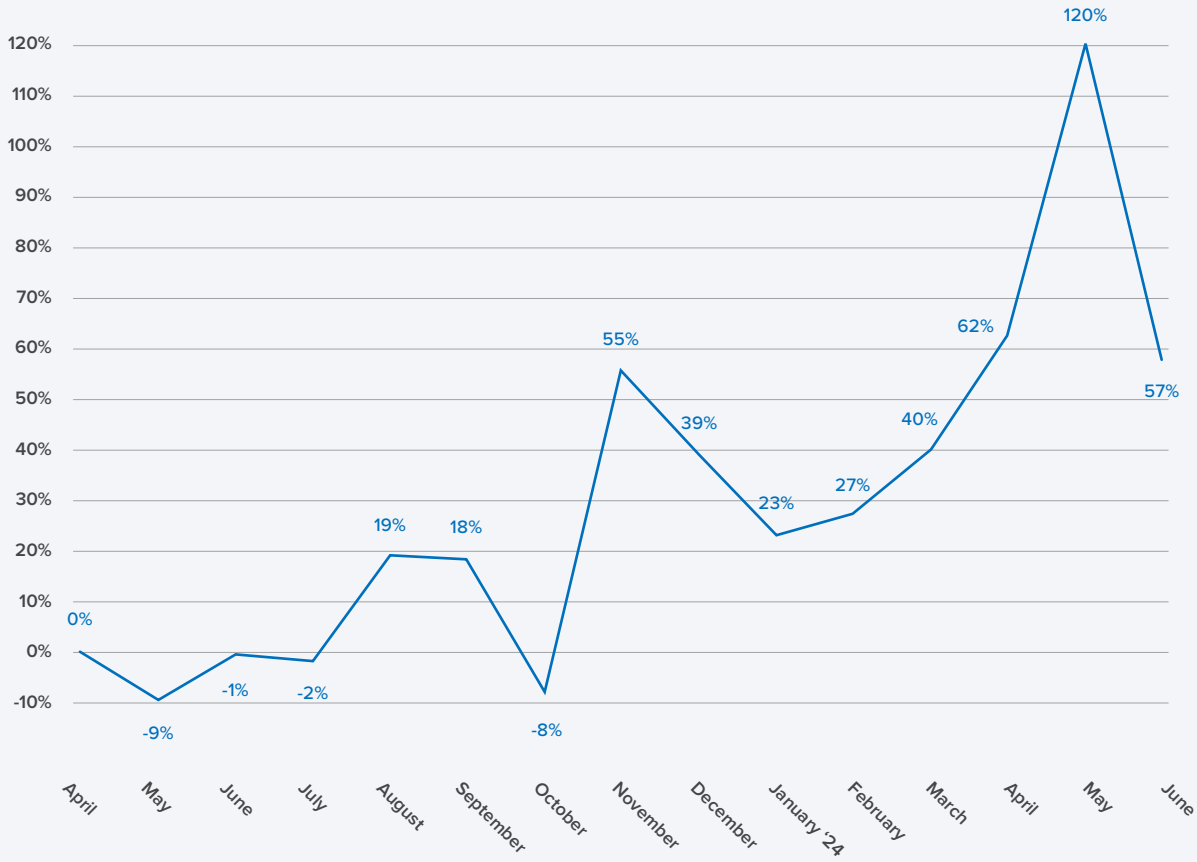
120%

Address manipulation and the misuse of reshippers are on the rise. Signifyd detected a 50% increase in reshipper fraud and a 120% boost in address manipulation between 2023 and 2024. In fact, address manipulation is now evident in 13% of all online orders on Signifyd's Commerce Network of thousands of retailers.

The Southeast Asian ring had all the markings of a major corporation — experts in ecommerce, online fraud, fulfillment, inventory and marketing. And while the Southeast Asian fraud ring was among the first detected global operations exhibiting its size and level of sophistication it was not the last — only a harbinger of an upleveling in online fraud.

"Fraudsters are nowadays managing enterprises, criminal enterprises, and they're thinking and developing roadmaps," Sheikrojan says. "They're thinking about how they can increase profit margins, how they can increase revenue, what do they need to get there, what is the right tooling, what is the right staffing from a resourcing perspective."

Use of address manipulation is trending upward



The Southeast Asian ring had one more thing: A massive workforce able to pivot quickly. That characteristic deeply worried experts in fraud, cybercrime and human exploitation. That aspect of the operation pointed to human trafficking and echoed the modus operandi of other criminal enterprises detailed in media reports and reported by the United Nations Office on Drugs and Crime.

Catherine Tong, of Allyiz, noted that organized criminal fraud rings buying with stolen credentials and reselling at a high profit have been around for years.

“What changes is where those groups are based,” she says, “For me, the sad side of that is it’s often linked to human trafficking and the people who are perpetrating that kind of fraud are the ones that they themselves are being taken advantage of to get the volumes those bad actors want to be able to resell.”

But as fraudsters and criminal rings continue to iterate and transform their organizations, so too do the best in the fraud protection business. More on that later in this report.

“What changes is where those groups are based. For me, the sad side of that is it’s often linked to human trafficking and the people who are perpetrating that kind of fraud are the ones that they themselves are being taken advantage of to get the volumes those bad actors want to be able to resell.”

CATHERINE TONG,
CO-FOUNDING PARTNER, ALLYIZ

The rise of first-party fraud and policy abuse

While the industrialization of fraud continues apace, professional fraudsters and wayward consumers are opening up another front of attack. False claims of poor service — including packages that never arrived, products that didn't live up to their promises — and policy abuse — using one-time promotions many times, engaging in unauthorized reselling of hot products — are increasing rapidly.

"First-party fraud is picking up," says Sidharth Shah, the lead fraud and payments product manager at fintech Novo. "It used to be that you would have bad actors and not bad actors. Now, you have bad actors. You have not bad actors, but still doing bad things. And then you have good actors. And so now there's multiple categories of this because it's like fraud is now not just about intent, it's also about opportunity."

He says some first-party abusers rationalize their actions because they understand the rules protect consumers and make them whole in most cases.

Meanwhile, online brands are suffering — more than ever. When the Merchant Risk Council asked online brands what the biggest fraud threat to their business was, the top two answers were refund and policy abuse and first-party misuse, all of which fall under the umbrella of first-party fraud and abuse. In fact, nearly half of the merchants surveyed pointed to refund/policy abuse (48%) and first-party misuse (45%) as their biggest fraud problems. And, 63% said first-party misuse had increased in the past year. The MRC survey concluded that 20% of all fraud incidents that merchants reported this year were first-party fraud, up from 16% in 2022. Notably, some individual merchants have reported that first-party fraud is an even more significant problem, comprising 50% or more of consumer disputes.

The most common first-party abuse schemes

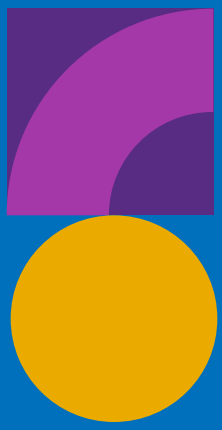
While different labels are tossed around — friendly fraud, first-party misuse, first-party fraud, policy abuse — the terms generally refer to scams that are conducted by the rightful credit card holder. The most common schemes are:

False item not received, or INR, claims

False significantly not as described, or SNAD, claims

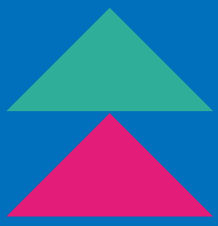
Unauthorized reselling

Promotion abuse



Customer abuse up in the first half of 2024 by

4%



The general idea is to keep a product and receive a refund or discount that the requester doesn't deserve. In the case of unauthorized reselling, the goal is to either corner the market in a popular product and sell it at a premium or to buy a product at a low price in one region and sell it or return it at the going — and higher — price in another region.

False INR and SNAD claims — forms of refund fraud — and return fraud began to flourish during the pandemic when consumers became more familiar with and dependent on ecommerce. Merchants have continued to see increases, particularly as lingering inflation and the economy's uneven performance have left some consumers feeling squeezed.

"As soon as customers realize what they can get away with, then they'll do it a little bit more and a little bit more, whether that little bit more is increasing the value of what they're doing or it's the velocity of what they're doing" Allyz's Tong says. "Then quite quickly that can start to mount up if someone becomes a serial offender."

In fact, in 2024, consumer abuse has been consistently higher than it was in 2023, according to Signifyd data. Year-over-year monthly increases last quarter in the U.S. registered 15% in April, 10% in May and 13% in June. Overall, consumer abuse was up 4% in the first half of 2024, compared to 2023.

Meanwhile, reseller abuse has become a big business. Sheikrojan's Signifyd team recently broke up a reselling scheme after an unauthorized reseller ring created a series of false accounts to appear to be many shoppers buying as many units as possible of a particularly popular household product. The fraudsters then relied on address manipulation to confound pattern recognition and began "reselling products on the Asian market for a much higher price."

Aided by bots, resellers often go after high-demand products, like Sony PlayStations during the holiday season or drops of hot fashion items, such as sneakers. On sportswear's risk manager Devanshu Agarwal sees that happen with the high-end Loewes the retailer sells sometimes as limited editions.

"Those are very limited in numbers, so they pretty much get sold out as soon as they go on," he says. "They're a target for payment fraud, but also reselling. It ends up impacting our customer experience when a legitimate customer cannot purchase a Loewe, versus some reseller or a bot placing 20 Loewe shoe orders and then reselling it on the third-party marketplace."

Indeed, customers notice when the only way they can get a coveted product is through a reseller charging a multiple of the suggested retail price. In the case that Sheikrojan and his team cracked, consumers took to social media early in the crisis posting comments such as, “Are you restocking this color? I missed it and refuse to pay over $100 from resellers.”

The damage to customer lifetime value starts with the disappointed customer who missed out in the first place and multiplies as word spreads through social posts and word of mouth.

Promotion abuse comes with its own cost. The classic scenario has an individual customer using multiple discount codes when a retailer’s policy calls for using just one. The whole idea of offering a discount or other promotion is to attract customers. Sure, it comes at a cost, but the plan is to make up that cost when a first-time or infrequent customer becomes a loyal and frequent customer. The math gets knocked for a loop when the customer acquisition cost skyrockets because a single customer uses multiple discounts which eats into the promotion’s return on investment or even turn it into a loss.

All of this first-party abuse is being accelerated by illicit businesses that offer to commit fraud on behalf of consumers for a cut of the profit. These outfits, which include fraud rings, are branching out into new product lines and revenue streams.

"We do see more and more of this type of thing popping up from the risk intelligence side, which are professional fraud organizations providing fraud as a service," Sheikrojan says. "So fraud organizations, they can leak promo codes. They can share tutorials and how to commit refund abuse. Or they can also do the whole thing for you. These fraudsters, they know their merchants, their business policies. They know where the gaps are and where their vulnerabilities are."

Industrialized fraud enterprises generate fake tracking numbers, Sheikrojan says, which allows packages to be misdirected and categorized as missing when they've been delivered to a fraud ring. Or they work with delivery company insiders who will mark packages as lost when actually they've been added to the fraud ring's wholesale inventory.

"The prediction here," he says, "is that for merchants it will become more and more challenging to deal, not only with these individual consumer abusers, but also deal with these professional fraud organizations."

How changing AI is changing fraud

The buzz around AI, heightened by the advance of Gen AI, has been deafening. And yes, of course, the dramatic advances have affected fraud and the work to protect commerce from fraud. The competition has been billed as AI vs. AI and make no mistake: It is a competition.

"More and more the strategies really have to dive a lot deeper into treating these (fraud rings) like you're against a business," says Kelley Andersen, Microsoft's director of product, payment fraud and risk. "Just as you would look at a competitor in the market for your product, so are bad actors."

AI and technical advances have powered the growth in bot attacks which, as we've seen, are vital for securing the inventory needed for profitable unauthorized reselling and for large-scale carding attacks and credential-stuffing missions. The former tests card credentials to determine whether they are viable. The latter allow fraud rings to try a limitless number of user name/password combinations on a staggering number of sites to break into accounts rich with personally identifiable information and loyalty points. AI-driven bots also allow fraud rings to spin up hundreds or thousands of fake accounts and even produce the software needed to conduct the automated raids that have become so common.

"Strategies really have to dive a lot deeper into treating these (fraud rings) like you're against a business."

KELLEY ANDERSON,
DIRECTOR OF PRODUCT, PAYMENT FRAUD AND RISK, MICROSOFT

"The interesting thing here is for that process, they don't need that strong technical background anymore to commit fraud," Sheikrojan says of fraud rings that have embraced AI. "They can have code written up for them through AI."

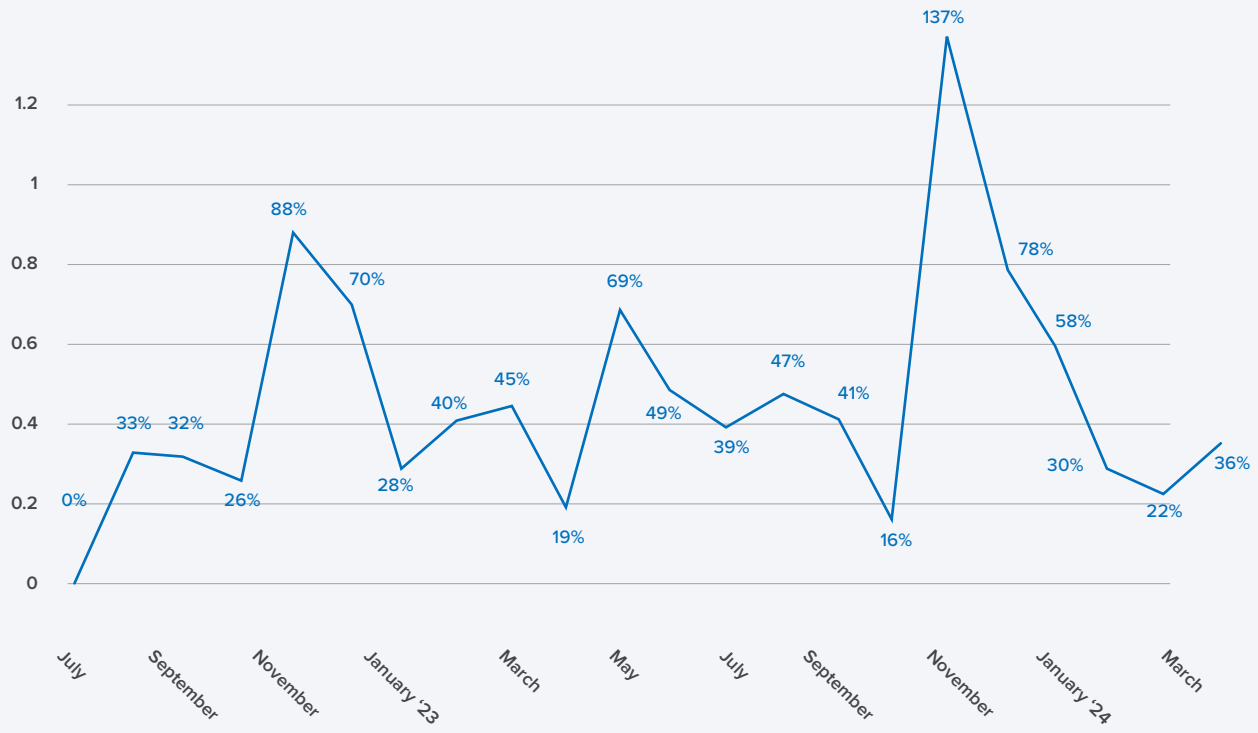
While the growth of bot attacks rises and falls monthly, as would be expected of a tactic that relies on automation to place a massive number of orders in a compressed amount of time, the trend is up, up, up. Signifyd data shows the number has been elevated for the past year, increasing by as much as nearly 140% compared to July 2022 during the 2023 holiday season.

Merchants for years now have confronted a fluctuating but increasing number of AI-powered attacks. These come in the form of bot attacks and device-, IP- and geo-spoofing orders. Such attacks have been on the rise since July 2023, increasing significantly during peak shopping periods, such as the holiday season.

Growth of bot attacks peaked year over year by nearly

140%

AI-powered attacks to continue to bedevil merchants



"The interesting thing here is for that process, they don't need that strong technical background anymore to commit fraud. They can have code written up for them through AI."

XAVI SHEIKROJAN,
SENIOR MANAGER, RISK INTELLIGENCE, SIGNIFYD

Not to be left behind in the Gen AI craze sweeping the nation, fraud rings have embraced the emerging and rapidly advancing technology to create high-quality phishing come-ons and deep fakes aimed at fooling banking and retail professionals into believing they are dealing with a legitimate customer when they are not.

"So, phishing," Sheikrojan says, "gone are those days where you receive an email in your inbox that's full of spelling mistakes and grammar mistakes. And you're like, 'Nope, that's phishing.'

"Now you'll get these beautiful, well-written emails in your inbox. That's making it much harder for you to distinguish whether it's coming from a fraudulent source or a genuine source."

One step beyond are the deep fakes that create a conversational AI fraudster who looks like the real thing in an attempt to fool a retailer.

"They take over the whole identity," Sheikrojan explains. "And not only the credit card details. Not only the email. Not only the phone number. But also the face, the voice, and also even the pauses and the tone of voice."

Sheikrojan pointed to a case in which callers were contacting customer service reps by phone to place high-value orders — $20,000 to $30,000.

"To make it sound legit, they clone the voice of their victim and the customer service representative is like, 'Oh, I have been speaking to this customer for years. Of course, it's the real person.'"

AI and machine learning in particular are also key tools for the best in the business at protecting retailers from fraud while taking liability for any fraud that eludes detection — all of which allows retailers to accept orders and better build customer lifetime value.

"Machine learning is kind of that first layer of defense against fraud. And the reason it's essential to have, nowadays we see fraud at an enormous scale. It's massive," Sheikrojan says. "We are seeing fraud attacks where they are just in a couple of minutes, they're hammering out multiple orders and that can go up into the hundreds of thousands of dollars within just a couple of minutes."

Turns out AI also has a role in protecting commerce from fraud. That's the part of the story we'll get to next.

"Machine learning is kind of that first layer of defense against fraud. And the reason it's essential to have, nowadays we see fraud at an enormous scale. It's massive."

XAVI SHEIKROJAN,
SENIOR RISK INTELLIGENCE MANAGER, SIGNIFYD

The new wave of fraud protection:

How commerce protection is keeping a step ahead of the fraud menace

Of course fraud and risk experts are not sitting idly by

Just as online fraud is being industrialized, fraud protection is undergoing its own metamorphosis. Think of it as Digital Transformation 2024. Leading retailers have traveled the initial digital transformation path, supercharging merchandising, marketing, site search and email programs while materially improving conversion and lifting revenue and profit margins.

Now, the next step is underway: Turning to AI and technology to maximize revenue and customer experience by protecting the entire buying journey from fraud and abuse. As fraud has grown in sophistication and scale, it's become evident that protecting the enterprise while maximizing the number of approved orders requires automation and a large network of merchants to provide insight into the identity and intent of shoppers.

The best fraud and risk teams today have turned themselves into business optimizers, organizations with the tools and know-how to approve virtually every legitimate order. These top teams avoid the scourge of false declines, which drive customers into the arms of a competitor. Instead, top risk teams today unlock the secret to profitable growth by building robust customer lifetime value.

"The mind-shift of the business is changing," Prerit Uppal, Adobe group product manager, payment and risk, says of modern fraud teams.
"They are no longer thinking of fraud and payments as operational centers. They are thinking of them more as revenue generators. And the reason I say that is, the question people have started asking is, 'Are we leaving money on the table?' Once you start asking that question, then you can start looking into the data to put strategies in place where you optimize first for the customer experience and also for the business impact that you are making."

2024, then, is a time when ecommerce leaders are focused on shrinking false declines so far down that they disappear. They are looking for solutions that shift liability for fraud away from themselves and onto commerce protection providers like Signifyd. They are considering building fraud protection stacks by, for instance, exploring ways 3D Secure might supplement their existing fraud solutions. They are discovering the benefits of fraud review at the pre-authorization stage and doubling down on their focus on commerce protection as a customer experience differentiator and a customer lifetime value accelerator.

"The mind-shift of the business is changing, they are no longer thinking of fraud and payments as operational centers. They are thinking of them more as revenue generators."

PRERIT UPPAL, GROUP PRODUCT MANAGER,
PAYMENT AND RISK, ADOBE

Liability Shift — How leading retailers are insulating themselves from fraud and risk

As the transformation of fraud-fighting through technological innovation continues, future-focused brands are embracing the notion of liability shift: The idea that if a commerce protection solution is effective, the providers of that solution should be willing to offer a financial guarantee against poor decisions.

Under the arrangement, liability for the cost of fraud is shifted away from the online retailer and over to the solution provider. The idea, pioneered more than a decade ago, is continuing to gain mainstream adoption, with some of the world's largest online brands adopting it as a key pillar of their fraud protection.

Signifyd is among the pioneers of the liability shift model, often referred to as "guaranteed fraud protection." It is one of the very few, if not the only, commerce protection provider that offers a guarantee against all manner of chargebacks, including those arising from consumer abuse around false claims that a package never arrived or that a product wasn't up to snuff, for instance.

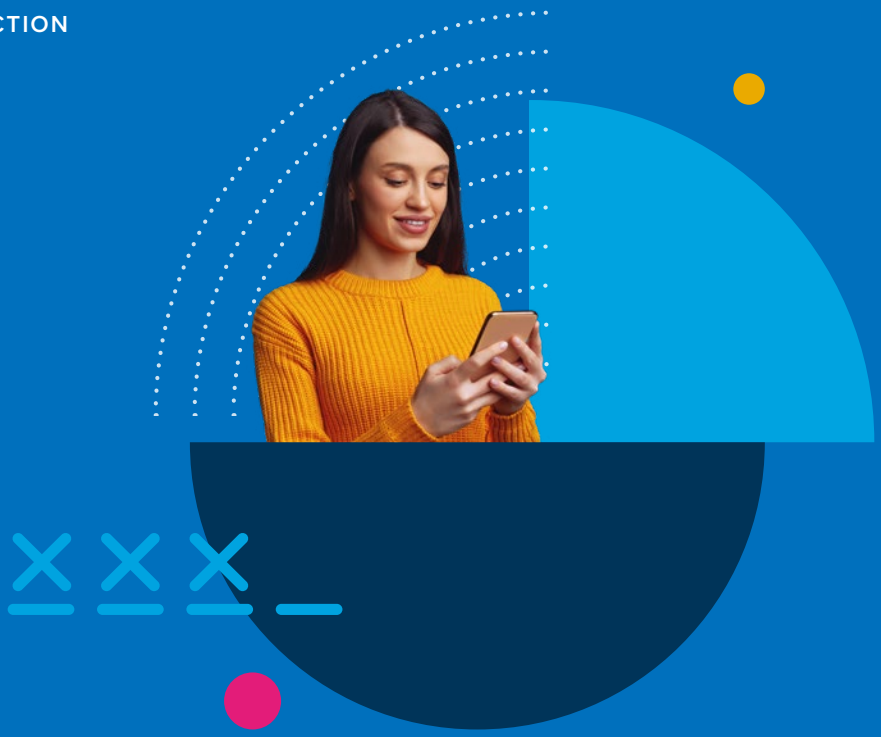
While some providers have struggled with costly claims and abandoned the guaranteed fraud protection model, different variations of the liability-shift concept, notably 3D Secure, are experiencing something of a renaissance in the North American market.

Why is 3D Secure a topic of conversation in the U.S.?

The reason for the rise of 3D Secure in North America is twofold: First, the product has been vastly improved since its launch in the early days of ecommerce. Until the recent improvements, the friction introduced by 3DS and its cumbersome consumer authentication requirements made it a conversion killer. Secondly, merchants apparently are more open to deploying more than one AI fraud solution in an attempt to achieve the maximum approval rate possible.

When the Merchant Risk Council surveyed online retailers for its 2024 Global Ecommerce Payments & Fraud Report, it found that on average merchants are using between one and two different AI-driven fraud management tools. That said, statistically speaking few in the U.S. are using 3DS, which is more prevalent in Europe, where it meets Strong Customer Authentication (SCA) regulations. But the conversation around 3DS is picking up momentum in North America.

The recent upgrades to 3DS, now often referred to as EMV 3DS, have made it a part of the conversation. It no longer comes with the baggage of its ancestor, 3D Secure, version 1.0, which was retired in 2022. The old version often required a step-up that consumers completed after being directed away from the merchant's site they were buying on. So how does 3D Secure work today?



Online merchants integrate 3D Secure into their checkout processes to add an extra layer of security to card transactions. When a customer initiates a payment reviewed by 3D Secure, the merchant's site sends a request to the card issuer or issuing bank to authenticate the transaction using 3D Secure protocols. The cardholder's issuing bank may then require additional action from the cardholder in order to complete the authentication sessions; this additional action step is referred to as the challenge flow. This can take the form of entering a one-time password or verifying a push notification to the customer's banking app.

Or, as is more often the case, the issuer might not require any action on the consumer's part at all. This is referred to as "frictionless" 3DS and is a key improvement over the old solution. Once the cardholder successfully authenticates the transaction, if necessary, the issuing bank confirms the authentication to the merchant, and the payment is processed. If the authentication fails or the cardholder does not complete the process, the transaction may be declined or flagged for further review. If the transaction is approved via 3DS, the issuing bank accepts liability for subsequent payment fraud.

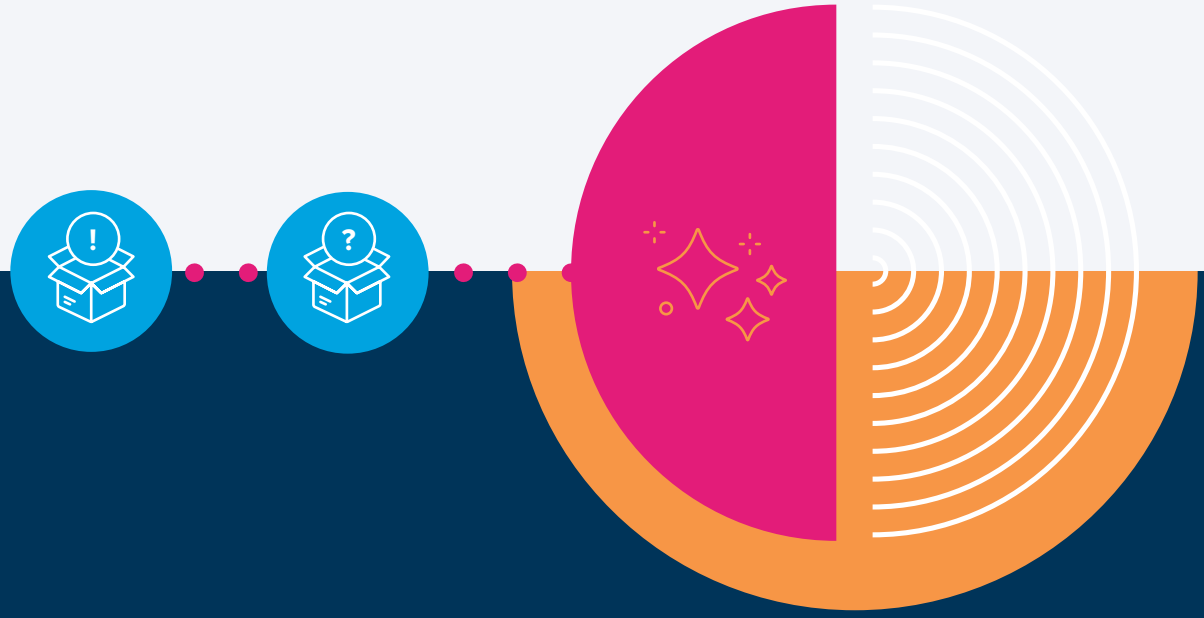
It's important to note that the 3DS liability shift does not apply to chargebacks from first-party fraud — false claims that a package never arrived or a product was unsatisfactory. In Europe, where 3DS plays a key role in relatively new regulations to protect consumers and merchants from payment fraud, fraud rings have shifted their attention to attack other segments of the buying journey.

Fraud experts often talk about 3DS as part of a larger strategy for U.S. merchants — a strategy that relies on additional options for a liability shift. The idea is to develop a thoughtful approach to payments, analyzing and understanding what path is the most economical, efficient and effective for each transaction and then developing the expertise or partnering with a fraud protection expert to manage orders to take advantage of the best option.

Signifyd provides a liability shift without the potential for step-ups

For instance, by adding 3DS to a fraud protection stack that included one of the new breed of AI-driven solutions offering a liability shift, merchants could increase their options for avoiding fraud costs when orders go bad. Signifyd, in fact, offers a liability shift on payment fraud that comes without the potential for step-ups. Its protection also extends throughout the buyer journey, so non-payment fraud like false INR (item not received) claims and dishonest SNAD claims arguing that a product was significantly not as described are also covered by a liability shift.

The concept of a liability shift is in keeping with the dawn of a new era for ecommerce. The hypergrowth of the early 2020s has passed. Merchants' focus needs to be on a period of strong, but slower growth — think 10% year-over-year rather than the 30% range inspired by the pandemic and shifting consumer habits.



Signifyd CEO Raj Ramanand laid out the significance of the change at the company's annual FLOW Summit. The most successful brands, he said, have shifted from a focus on just increasing transactions to building long-term customer loyalty — which translates into customer lifetime value. Success requires having the ability to trust that a customer arriving at an online shop is who they say they are and that the merchant has the ability to personalize the shopping experience for that person.

That doesn't mean the order at hand is any less important than it ever was. In fact, it makes approving every legitimate order more important than ever. And it makes avoiding first-party fraud on the back end of sales a priority, so that retailers' top line revenue makes it all the way to the bottom line. Liability-shift providers — particularly those who provide a guarantee against illegitimate chargebacks that happen after the purchase — give merchants the confidence to approve more orders at checkout. And they allow them to make things right for customers who have legitimate post-purchase complaints without constantly worrying whether they're being taken advantage of.

Protecting online brands from fraud doesn't require insulting your customers

Heading into 2025, successful brands realize the days when false declines were an unknown cost of doing business are over. When ecommerce represented a minor share of revenue and customer retention, merchants could rationalize enduring some lost orders as an unfortunate by-product of preventing fraud.

After all, purely from the perspective of fraud losses, stringent rules against fishy-looking orders were effective if you take the view that risk management is about only preventing fraud.

"If you don't care about revenue," Signifyd CFO Jason Eglit says, "you can solve fraud really easily — just don't accept any orders."

But the lens has shifted in an era when fraud and risk teams have evolved from being defensive shields to being business and revenue optimizers. They have seen the top-line value in accurately determining which orders are truly fraud and which are orders placed by honest and valuable customers who simply want to buy a merchant's products. They know that the dollars those wrongly refused orders represent are sitting right there for the taking.

"If you don't care about revenue, you can solve fraud really easily — just don't accept any orders."

JASON EGLIT, CFO, SIGNIFYD

$16 billion

The annual cost of false declines for online retailers

In a widely circulated study, Research 451 pegged the annual cost of false declines for online retailers at $16 billion a year. A Merchant Risk Council survey found that more than half of merchants (53%) believe that between 2% to 10% of declined orders are declined incorrectly. Another 19% say their false decline rates are higher than 10%

And while those figures are impressive — and impressively discouraging — they only begin to account for the damage done by a false decline. We've all seen the numbers indicating how many customers a retailer loses by turning away a good order. The most recent available research indicates that between 33% (Sappio Research) and 57% (Signifyd consumer sentiment survey) of consumers will stop shopping with a retailer after having an order declined for no valid reason.

It's hard to imagine a worse customer experience than being turned down for no apparent reason for a purchase of an Item that you've researched, planned on and looked forward to. And the data shows that customers don't forget those poor experiences.

A Signifyd analysis found that among loyal customers — those who have previously had at least three orders approved — a false decline is followed by a 65% decline in the number of orders placed by that customer and a 16% decline in their average order value. Moreover, 27% do not return to the merchant at all — meaning the merchant loses not just that one sale, but a lifetime of potential sales from a repeat customer.

False declines kill customer lifetime value

Even those shoppers who return are significantly less valuable as customers. Signifyd's analysis determined that the lifetime value of returning insulted customers drops by 17%, compared to those customers who were not subject to a false decline.

Overall results 2024

Metric	Before decline	After decline	% difference
AOV	$274	$232	-16%
Order Rate	1.6	0.57	-65%
Estimated CLTV	$7,837	$6,446	-17%

JASAL MOTIRAM, MANAGER OF CUSTOMER SUCCESS, SIGNIFYD

And so, future-focused retailers have accepted the challenge and built ways to dramatically reduce false declines and the havoc they wreak on a brand's financials. Jasal Motiram, Signifyd's manager of customer success, has worked with dozens of retailers, including some of the largest in the world, to tackle the problem of false declines. He recommends online brands focus on four steps to conquer the costly problem.

1

Make sure you really understand the problem:

Taking a close look at your false declines can help surface strategies and tactics to lower your false decline rate. Maybe you have a disproportionate amount of false declines on high-priced items. Maybe your system — whether automated or manual — puts too much weight on one variable, say shipping and billing address mismatch, geolocation indicators, VPN usage, without considering the order's larger context.

"Maybe you're getting a lot of insults in a specific way," Motiram says, using an industry term for unwarranted declines. "You can target that and make changes to decrease them. Categorize your false declines. Did the customer call in? Did the risk team review it and decide it was a good order? Understanding where you're committing insults can actually allow you to home in on what you need to fix."

2

Adjust risk thresholds:

Does your analysis uncover areas where you are being overly protective? Are your declines indeed focused around high-value orders? Sure, more is at stake the higher the price of an item, but high-end products also potentially offer the biggest revenue reward — provided you're not turning away good orders from your best customers.

On sportswear's payment risk manager, Devanshu Agarwal, says the retailers' internal teams regularly discuss the balance between protecting the business and providing a great customer experience for shoppers who enjoy the finer things in life.

"Considering that we are a premium brand, we would want to have a high level of satisfaction from our customers, and that's why we also have a slightly higher risk appetite," Agarwal says. "We look at something like the cost of fraud. Hey, what is our cost of fraud versus what would be the uplift?"

Trading 2% more conversions for a small uptick in fraud might be a good bargain, he explains. Of course, ideally, any merchant would rather see an uplift in conversions without suffering more fraud — a promise that is much more possible today given the advances in fraud protection technology.

3

Look to technology and artificial intelligence to approve more orders:

Future-focused fraud solutions are going a long way toward eliminating false declines as a challenge for retailers. Innovative vendors, particularly the few who offer a full financial guarantee along with their automated decisions on whether to ship an order, mean that online brands can fulfill orders with confidence.

Such fraud protection solutions depend on vast amounts of transaction, historical and behavioral data to understand the identity and intent behind each order. Signifyd's Commerce Protection Platform, for instance, analyzes a significantly larger set of signals than a single merchant or legacy fraud systems can. That greatly expanded vision provides the intelligence needed to instantly sort the good from the bad when it comes to online orders, assuring that legitimate customers are not insulted. It also means retailers can ship approved orders that appear menacing on the surface knowing they'll be made whole should the order turn out to be fraudulent.

"There are over 1,000 features that the model takes into consideration and thousands of data elements within those features," Motiram says of Signifyd's solution in particular. That sort of insight dramatically changes the risk calculation for shipping an order in which an isolated signal might appear to be off when all else is well.

Consider the difference Philips Electronics experienced when the global brand took a new approach to selling and fraud. Historically the brand sold through brick-and-mortar stores and other brands' websites. When Philips started selling directly to consumers online, they were converting only about 40% of their orders, in part because good orders were being turned away, according to Ivone Miranda, Philips consumer experience engagement and care lead. Soon after adopting an AI-driven solution with a financial guarantee, Philips conversion rate was at 75% and on its way to a better than 90% rate.

4

Take calculated risks:

With improved visibility into patterns that provide a warning that an order is fraudulent or reassurance that an order is not, merchants can open up to a greater extent than ever before. And in particular with a financial guarantee, merchants can feel free to experiment by approving some orders that might look fraudulent on their face.

Once the order is shipped, a merchant or its fraud protection provider can track its performance to tell the rest of the story. Did the order result in a chargeback? If not, it's a sign that the model being used to assess the fraud potential of orders is too stringent — and costly.

"That's what Signifyd does to improve performance," Motiram says. "We take calculated risks, and we continue to refine the system. If there are no chargebacks, then we adjust the threshold so that we can open up for more approvals."

A single brand could consider the same approach, though without a very large set of transaction data and without an entity providing a financial guarantee, taking calculated risks could turn into an expensive experiment.

The before and after picture looks good for pre-authorization fraud review

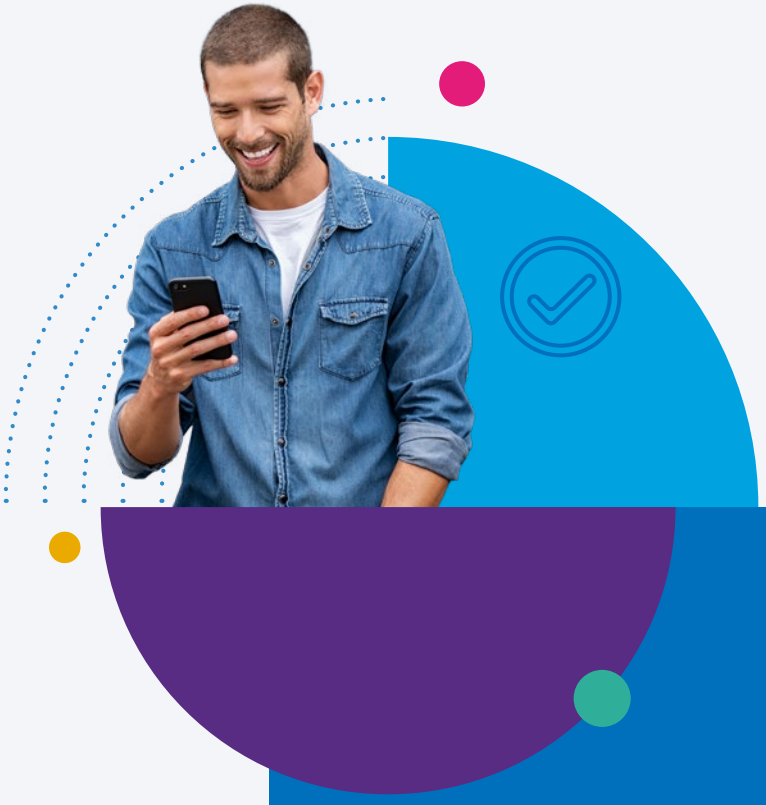
As ecommerce becomes a bigger piece of the profit picture and the market continuously grows more competitive, merchants are pulling seemingly every lever to increase conversions and build more customer lifetime value.

Retail leaders have enhanced marketing and merchandising. They've deployed sophisticated AI to personalize product discovery, site search, marketing messages and promotions. They've fine-tuned their inventory to have the right product at the right time at the right price.

But all this time, an area ripe for improved customer experience has been hiding in plain sight. The neglect it has suffered has resulted in a ton of lost business. The missed opportunity? Fixing fraud and bank authorization declines.

Signifyd Vice President of Global Partnerships Will Wyatt says allowing more good customers to successfully transact can transform a retail enterprise's business. And what could be more logical? Letting more people buy stuff from you is good for business. In fact, when you think of it that way, what business wants to turn willing customers — willing to buy — away for no good reason?

But if it were so simple, everyone would have done it by now. Allowing more online shoppers to transact on a digital site requires walking the fine line between maximizing approval rates and minimizing risk — particularly in a time when online fraud is growing steadily. After all, the more suspect orders you allow through, the better your chance of becoming the victim of fraud.



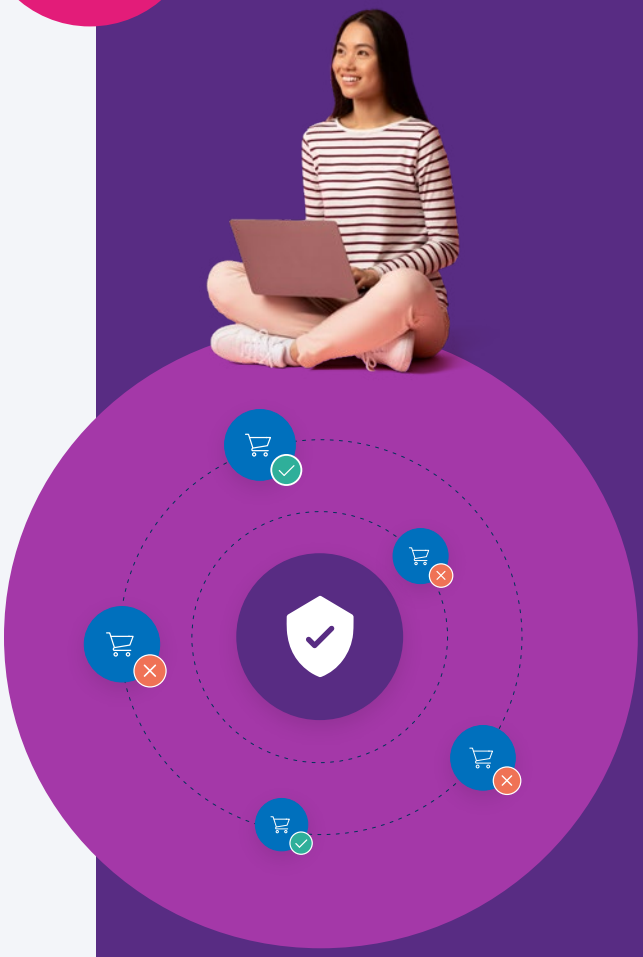
Given the set of circumstances in this particular time, the case for instituting pre-authorization fraud protection is stronger than it's ever been. Moving to pre-auth, as it's commonly called, should be a strategic imperative that enhances security and improves authorization rates by as much as 3%, according to a Signifyd analysis, and as a result increases revenue potential.

To back up for a second, authorization is a key point in the online payment process. It's when the credit card issuing bank ensures that the basics are covered — that the credit-card account contains sufficient credit to complete the transaction, sufficient account details are present, the account is not expired, etc.

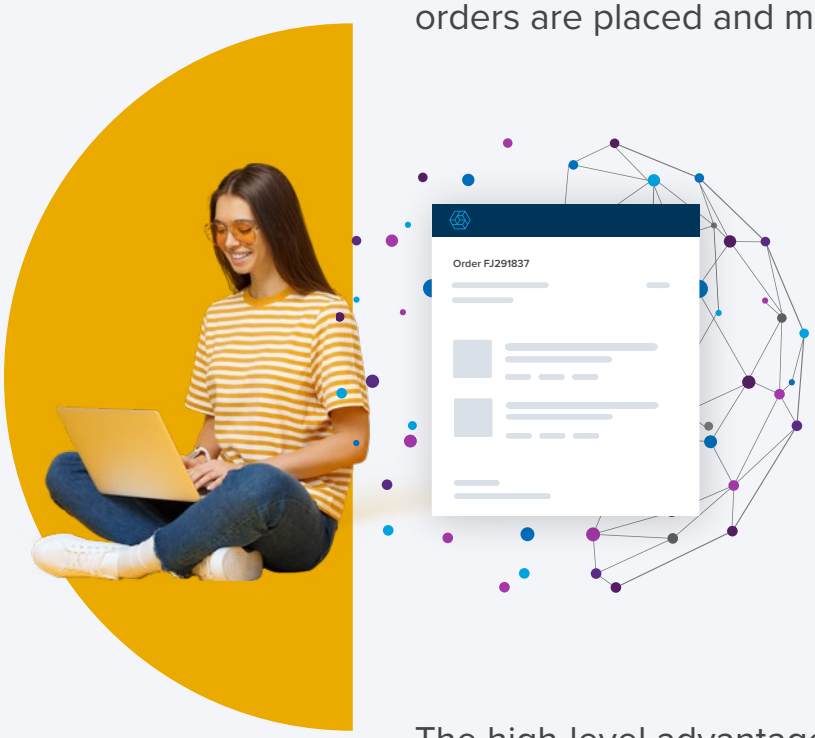
Fraud review can happen before authorization or after. Conducting fraud review before authorization unlocks a number of advantages for online retailers, beginning with providing significantly richer data at the authorization stage, which leads to an increase in successful authorizations.

3%

Improvement in authorization rates



Think about it: If an issuing bank makes an authorization decision before fraud review, it must rely only on the data it has, which is somewhat limited. When a bank makes a decision under the pre-auth scenario, it not only has its own data, but it benefits from the rich transaction and historical data that Signifyd, for instance, considers in its review. Signifyd reviews orders for fraud using thousands of signals and has insight into the product purchased, device used, shipping and billing address, velocity with which orders are placed and many others.



The high-level advantage: Relying on more data leads to better decisions and launches a virtuous cycle. When banks see that a particular merchant is sending high-quality, clean transactions to them for authorization, their confidence grows and they approve more orders from that merchant.

On the flip side, the merchant realizes significant savings in unnecessary authorization fees. Because orders are reviewed for fraud before authorization, a high percentage of problem orders are weeded out before they move on to the authorization stage, a transaction milestone that causes a modest fee to apply whether or not an order is authorized by the issuer. This advantage has become all-the-more important in an era when sophisticated fraud rings have fully embraced malicious bots. While authorization-related fees are modest, they can add up quickly, particularly in the midst of a rapid-fire carding attack resulting in a high volume of orders.

Now let's dive a little deeper into five ways moving to pre-auth is a conversion and revenue-increasing lever to pull:

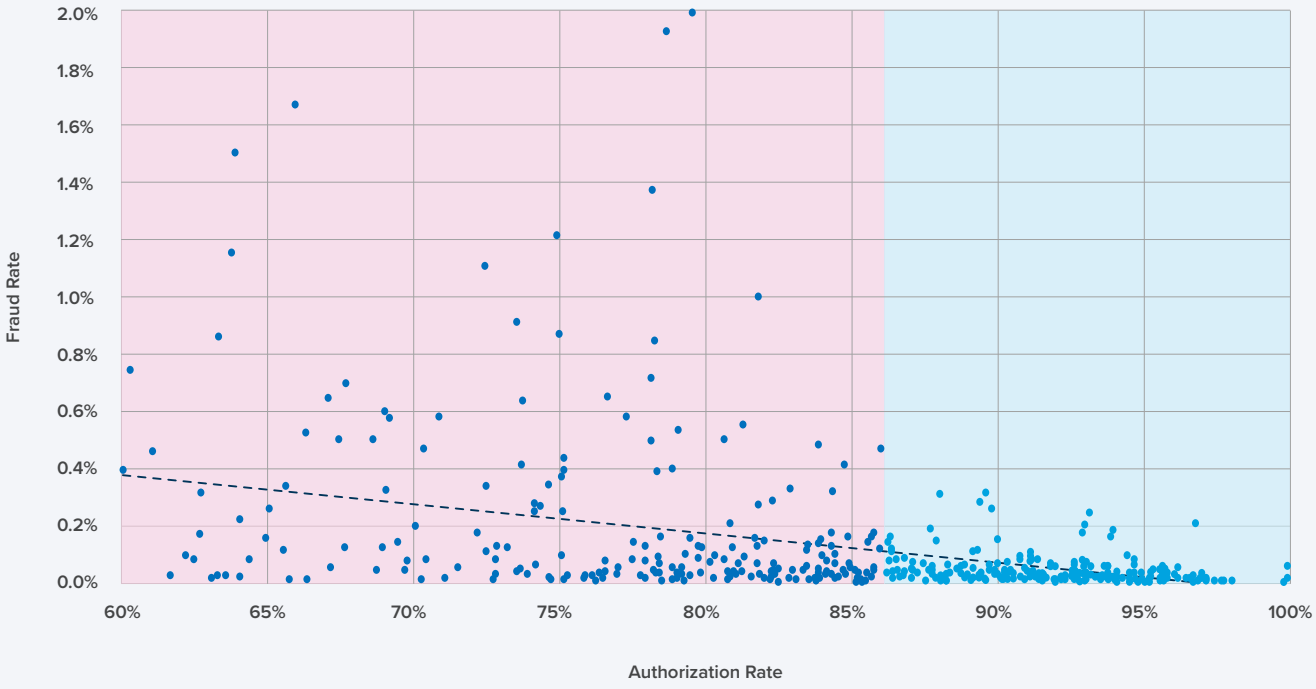
1

Sending clean traffic to issuers inevitably improves authorization rates:

A Worldpay analysis found a direct, negative correlation between authorization rates and fraud rates. As a merchant's fraud rate goes up, their authorization rates go down. Issuing banks have a very low tolerance for fraud on their cardholders, so they put controls in place to make sure that consumers have little chance of falling victim to fraud because a risky merchant accepted fraudulent payments. That means, the cleaner your traffic, the less friction an issuing bank will add in the name of protecting its cardholders from fraud.

Falling fraud rates mean rising auth rates

Worldpay found a direct relationship between low fraud rates and high auth rates.



2

Moving to pre-authorization fraud review can significantly reduce false declines, also known as customer insults:

While issuers have a ton of data on the spending patterns of their consumers, they actually have very little data on any given transaction. Having only a timestamp, merchant identifier and dollar amount, sometimes leads an issuer to falsely decline an order simply because of insufficient data. By working with merchants pre-authorization, Signifyd can share data with issuers like Capital One, Discover and others. These data insights, such as Signifyd's risk score and the fact that Signifyd has accepted liability for a transaction, give issuers enough confidence to relax their fraud controls.

3

Moving to pre-authorization can stymie unauthorized reseller schemes that rely on bots for rapid-fire purchases:

Few customer experiences are worse than trying to place an order for a popular item, only to be told the item is no longer available. Unfortunately, if a merchant places fraud controls post-authorization, bots and other large-scale resellers can snatch up inventory without being detected — leaving loyal customers out of luck when it comes to purchasing their favorite items. By putting controls before payment authorization, merchants can identify and block fraudsters, resellers and other unwanted buyers before they make off with popular inventory, keeping it reserved for the right customers for the brand.

4

A pre-authorization fraud review strategy reduces merchants' interchange costs:

Merchants end up paying significantly more to their payment processors when they send every transaction through to authorization and pay the associated fees on each order. Consider a card-testing attack, which often involves an automated assault of small value orders in quick succession. The aim is to identify valid stolen credit card information. While the authorization fee for each transaction may be relatively low, a wave of thousands of rapid-fire transactions could be devastatingly costly for an online brand. By sifting out the worst transactions before sending them through the network, brands can reduce their costs.

5

Deploying pre-authorization fraud controls improves fraud-protection models' performance:

The advanced fraud systems deployed by future-focused retailers thrive on data. It's the data that allows their sophisticated models to render a decision on a transaction — whether to approve it, decline it or possibly take a closer look. The models become automated experts at fraud review through training data. The more opportunities fraud-protection models have to see the good, bad and the ugly, the better they'll be at identifying patterns in the future. That means merchants are failing to fully optimize their models if they review only orders that have been approved at the authorization stage.

Why they do it: Fraud fighters are a special breed

Certain professions draw their practitioners closer together than others: first responders, medical workers, military members, educators and, yes, risk and fraud professionals. The bond comes from a common mission or common enemy or a common desire to help those who need help.

For those on the front lines of fraud and risk, you can sense the camaraderie walking the halls of the Merchant Risk Council's (MRC) annual conference in Las Vegas. It is one place where professionals, often from competing enterprises, come together to share the best of what they've got and to learn from those who maybe haven't seen it all, but certainly have seen a lot.

"One of the things that's unique about the MRC is it's collaborative," Tim Potvin, director of customer success at IPQS, says on the last day of the 2024 gathering. "When I was back in my office trying to stop fraud, I felt alone. I can't raise my hand because somebody's stealing from me and I need help. But here you can ask that question, whether it's cross-border, whether it's IP spoofing. It doesn't matter what the use case is, somebody here has already experienced that. And people will stop and talk to you about it because, again, we all want to come together and defeat what we can when it comes to fraudulent activities. I don't think there'll ever be a day with a silver bullet and it's just stopped and we're all happy. But we can frustrate them and make them have to change their tactics."

Working to prevent ecommerce fraud while ensuring that good customers are able to easily buy the products they want and receive them quickly is a game of cat-and-mouse, an arms race, a round of whack-a-mole. Pick your common analogy. And yet fraud fighters come back day after day, attack after attack, defeat after defeat with determination and a sense of purpose.

Why? How do they do it? What got them into fraud-fighting in the first place and what makes them stick with it? We decided to ask a few.

"For me, it's the curiosity and it's the understanding of human behavior. Why is somebody doing this? How are they getting away with it, and what can we do to stop them? So I think there's two elements to it.

There's the curiosity and the investigation and analysis. For some people really getting into that detail is something that's really interesting and you're wanting to get to the root cause. But I think there's also the more cultural side of it in terms of, you want to make sure that you're doing the right thing. You want to protect. You want to save, make people feel that they're secure. So for me, a combination of those two things is what gets people really passionate about the topic and wanting to do the right thing."

CATHERINE TONG,
CO-FOUNDING PARTNER

Allyiz

"What I'm doing at Signifyd is I'm managing the risk intelligence team. It's a group of fraud-fighting ninjas, really, focused on fighting the battle against fraudsters and making sure that we are one step ahead, putting our fraud thinking cap on — if you want to call it that — and really understanding fraud, fraud modus operandi and fraud patterns.

And then investigating those and saying, 'Hey, this is how fraudsters operate, this is what they do, this is what they're targeting, this is what they're after.' And then we work with our data science partners to say, 'We can feed that back into the machine learning model. So it's really data storytelling, really deep diving into the data to do the storytelling, understanding the fraud insights and sharing those with our partners across the company and with our customers as well."

XAVI SHEIKROJAN,
SENIOR MANAGER, RISK INTELLIGENCE

Signifyd

"When you get a payments leader that sees payments as a revenue generator, you begin to look at payments from the prospective of driving sales and increasing conversion. This thought process is what takes you to the next level."

BLAKE WHITSON,
VICE PRESIDENT OF OPERATIONS

BRAINLY

"I just found it fascinating. It changes and it changes rapidly and it's not a boring job. So that's why I'm still in it now with Microsoft and continuing to look at how can bad actors exploit products. And they're genius. And so bad actors are probably some of my favorite 'coworkers' in a way.

They challenge me every single day. So that's how I kind of stumbled into this but ended up loving it. I'm stopping bad actors, but I'm also facilitating, I hope, a great customer journey for customers too. It's not just how many bad actors did I stop and the money potentially saved, which is super key, right? But also, how did I facilitate a great customer experience? I always tell my team of PMs, ideally, we should be like "Men in Black." No one should see us, but hopefully, the world is safer with us. But it's still good internally to make sure that both sides of that are seen. And I think that's key to strategy. You've got to be able to manage it up to senior leadership — how does this really help facilitate their business and their goals as well."

KELLEY ANDERSEN,
DIRECTOR OF PRODUCT, PAYMENT FRAUD AND RISK

Microsoft

"I saw that Etsy was hiring. And they were hiring up their very first risk team, and they needed somebody to come in and process chargebacks. And so I applied for it, I put my resume, you know, out there.

And I just Googled my way through it, I ran from my job that was ending to interviews with them, shoving a sandwich in my face on the train. And I managed to make it through the interview because they were looking for really raw, junior people who could do this to hire their first team. And so I managed to get myself in the door there. I would say, in our industry, there's not a lot you can't Google. Doing the research and knowing how things work, even if it's not at the company you're interviewing at, is going to get you in the door for a lot of the more junior roles. And then having some of those tech skills is just immeasurably important. Whether it's knowing how to use BI tools, like Tableau or SQL, things like that. That's going to get you to a point where you can not just apply some of what you've learned in the domain-specific knowledge, but being able to scale it effectively, and show that worth and value with the skills you need to be effective immediately, rather than looking like you need someone to train you from scratch."

TARA MITCHELL,
SENIOR DIRECTOR, CHARGEBACKS AND ABUSE RECOVERIES

Signifyd

Signifyd is the leader in commerce protection

Signifyd's Commerce Protection Platform is a holistic solution addressing key challenges emerging in the post-pandemic era. The platform protects the entire buying experience from account creation and log-in, to checkout and returns. Powered by a Commerce Network of thousands of merchants worldwide, Signifyd leverages behavioral and transaction intelligence from billions of orders to provide an understanding of the identity and intent behind every order.

The powerful technology and Signifyd's superior data science team and award-winning customer success team make the Commerce Protection Platform the ideal solution for the world of new and emerging fraud and commerce trends.

Learn how Signifyd can help you grow at www.signifyd.com

Signifyd