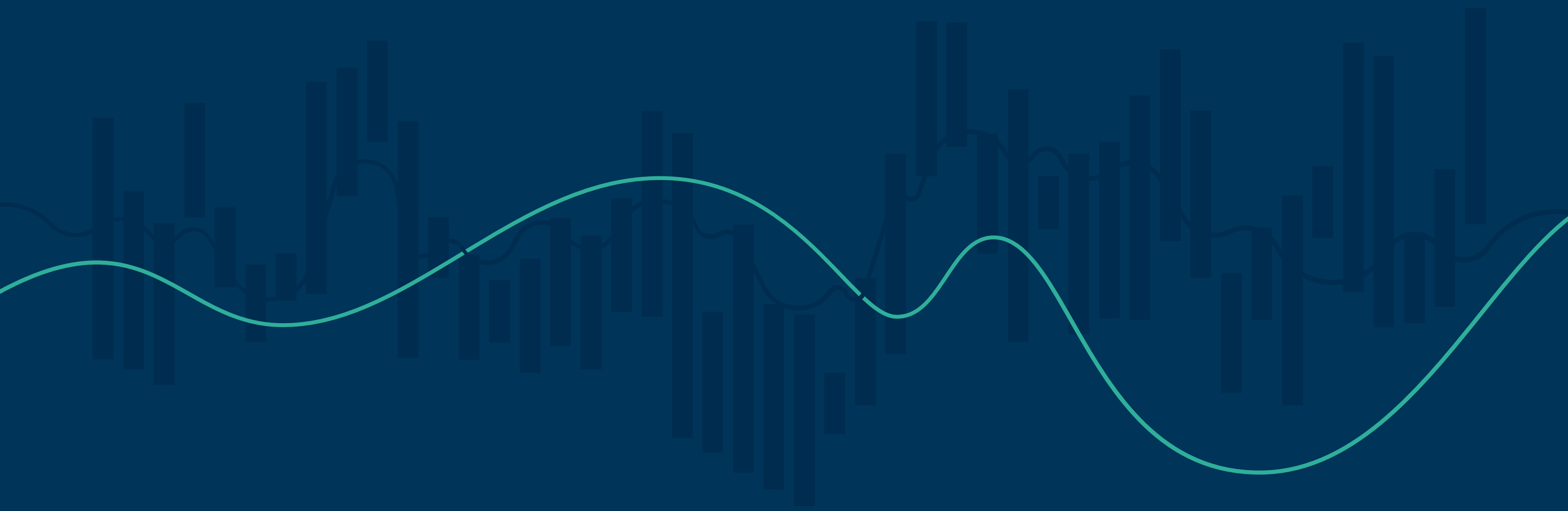
Signifyd

State of Ecommerce Fraud in Europe

How New Trends — Good and Bad — Will Shape 2022

Table of Contents

Table of Contents



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.

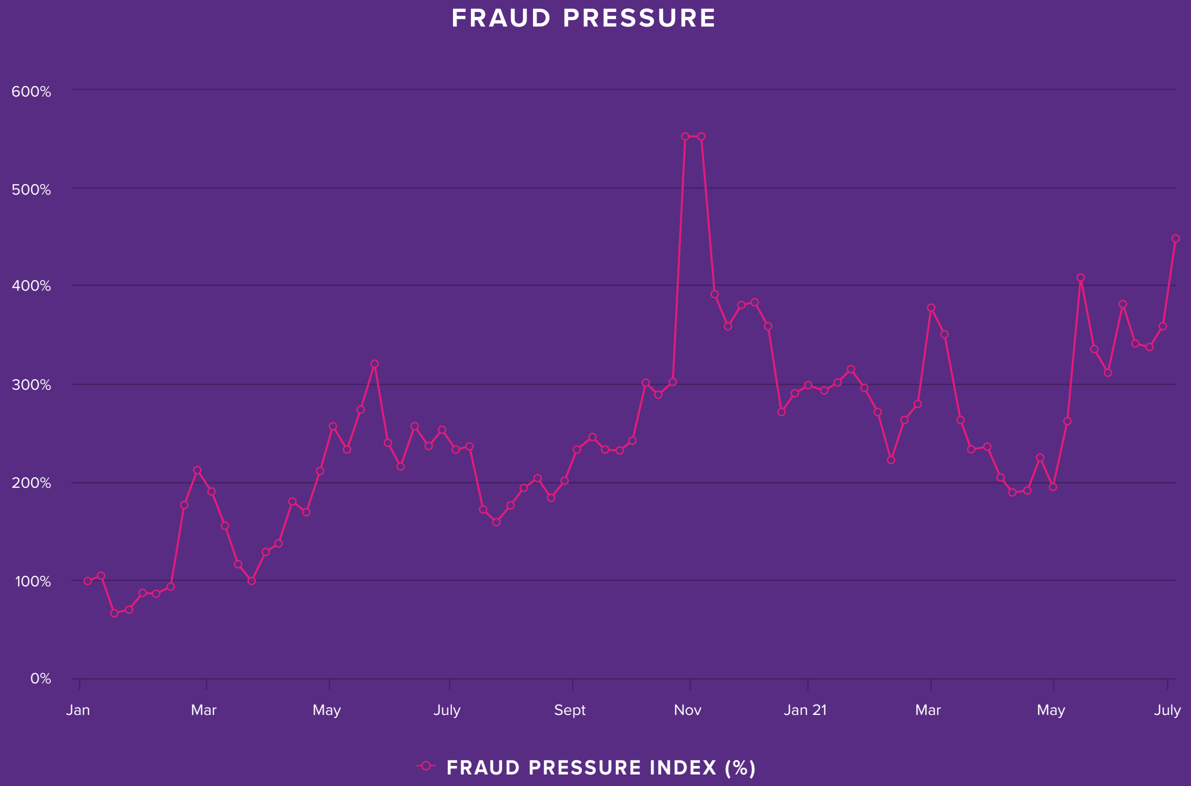
As retailers became more sophisticated at protecting their enterprises from payment fraud, fraud rings innovated, iterated and persisted. In effect, they seized the disruption of COVID-19 to usher in the golden era of online fraud. What was not new in fraud was intensified, all while European payment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

> 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 during the pandemic 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 throughout the 2021 holiday season and well beyond.

Against this backdrop of transformation, much of Europe confronted the enforcement of new payment regulations in the form of PSD2 and its strong customer authentication (SCA) mandate.

This e-book will dive into the dramatic 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.



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.

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

ToysRUs

Innovation often thrives out of the necessity, fresh perspective and urgency that disaster brings.

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

"What we were experiencing at Toys R Us, as well as a lot of the other retailers, was five to 10 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.

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

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 nimbly adapt to changing conditions

Fraud advanced in other ways during the pandemic, too, with criminals upping their social engineering game.

"The expansion of ecommerce has opened up new opportunities for criminals to scam businesses and customers," said Andrew Cregan, head of financial policy at the British Retail Consortium. "The modes of operation that criminals have used and sharpened throughout the pandemic are likely to continue until we have a higher level of awareness around these types of scams among businesses and the public."

With so many working from home — or wanting to — during the pandemic, 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.

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 analyse 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."

Maplin is one of the UK's best-known names in retail. In 2019, the popular electronics retailer transformed itself from a high street brick-and-mortar merchant to a pure-play online store.

Though the Maplin teams were online experts, the pandemic and the surge in order volume were new experiences, even for them. But through order automation and machine learning, they were prepared.

"Signifyd basically does the protection of the front end," said Ollie Marshall, managing director, Maplin. "So for us, it's kind of our outsourced fraud and risk team. For me it's all about automating or outsourcing things that are not our competitive advantage or that someone can do better than us."

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 upon 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.

Managing fraud and consumer abuse is squarely in that category for many successful retailers. Fraud solutions, like Signifyd's [Commerce Protection Platform](), affect change.

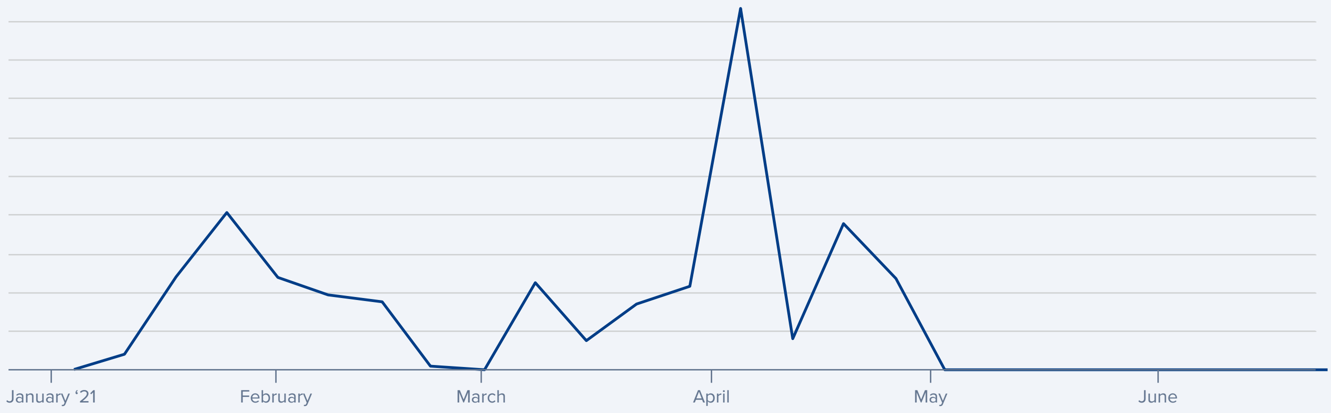
For instance, after a strong run, the number of mule fraud attempts in 2021 has plummeted by 65%, according to Signifyd data.

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.

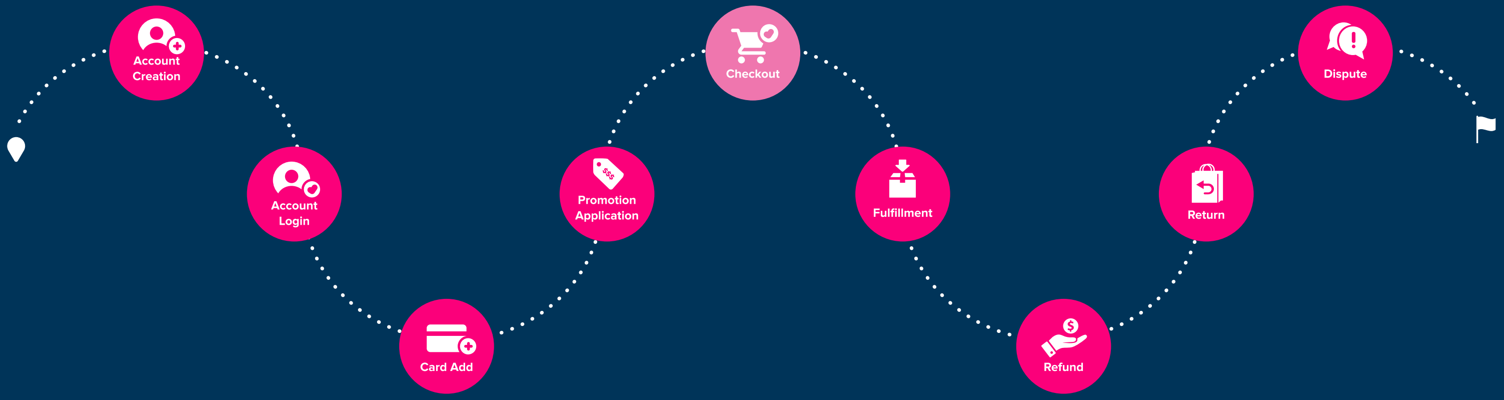
451 Research noted the trend in a May 2021 report highlighting fraud trends.

"Bad actors are broadening their focus beyond payments, targeting touch points across the customer journey," the report said. "Touch points 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 through the practice of unauthorized reselling — 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.

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

100%

in the first half of 2021, compared to 2020.

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

MAZE

“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.”

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.

Part 2: Strong Customer Authentication — a story of success and struggle

Increasing fraud pressure across Europe was a key reason the European Commission included Strong Customer Authentication (SCA) in its update of the Payment Services Directive early in the last decade.

From concept to concrete requirement has been a long and tortuous journey. Today most of Europe is governed by the more robust authentication requirement and the UK is soon to join them in the first quarter of 2022.

SCA requires that customers executing online transactions be authenticated by two of the following three ways:

- Something the user knows (like a one-time passcode).
- Something the user has (like a mobile device).
- Something the user is (fingerprint, facial recognition, typing behaviour).

The new requirement was designed to reduce fraud and thereby protect both consumers and retailers. The feared effect — and not without cause — was that the measure would add friction and drastically reduce conversions in the affected countries.

Statistics show that has come to pass. Global payments consultancy CMSPI has carefully tracked the effects of SCA on conversion rates as it's been rolled out. It found that in August SCA was causing 26% of transactions across Europe to fail.

Failure rates were hardly universal across countries, with some seeing much higher rates and with others doing better than average.

For instance, according to CMSPI's latest SCA assessment report, the transaction failure rate in Belgium was 41%. In Germany the rate was 32% and Italy was seeing 30% of transactions fail.

Signifyd also found a broad range in sales performance with Luxembourg seeing a 46% annual decline in same store online sales since the enforcement of SCA there. Italy was down 38% and Belgium was off 14%.

The culprit, according to CMSPI, is the performance of 3D Secure, the security protocol that provides the backbone for processing SCA transactions.

While the protocol has been recently updated, some merchants have been slow to embrace 3D Secure version 2.2, and even with the updated version, SCA can cause a drop in conversion, according to CMSPI.

“The key reason for this significant disruption to online commerce is due to the performance of EMVCo 3D-Secure version 2,” CMSPI reported in its monthly update in July. “Although the weighted average failure rate across Europe has improved for the month of July, this rate remains high. This suggests significant friction at checkout for consumers. Therefore, the issues merchants and consumers are facing in relation to SCA are very much alive.”

The August report did note that the failure rate under SCA has fallen since August 2020, when it stood at 35%. But even today, the rate of loss means European retailers stand to lose €82 billion a year due to lost conversions.

Like fraud protection in general, the key to balancing security and customer experience with SCA starts with technological innovation, like Signifyd’s Payments Optimisation solution.

European retailers stand to lose

€82 billion

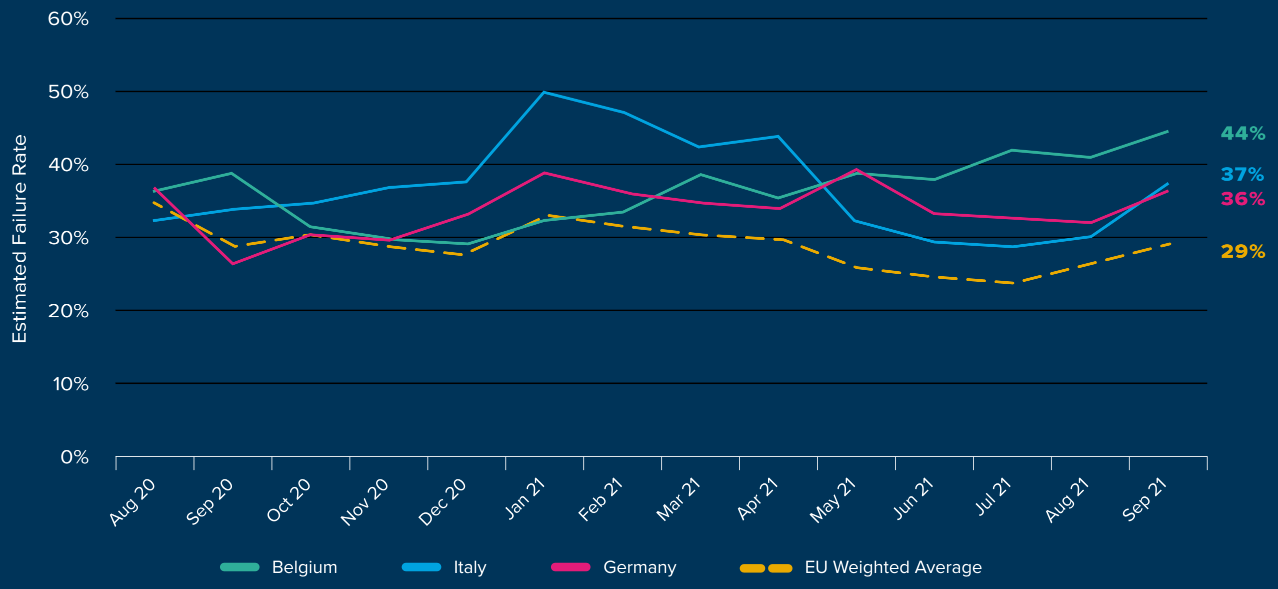
a year due to lost conversions

Signifyd’s technology and adopting best-in-class SCA strategies, in fact, provide the most direct path to realizing the promise of SCA without compromising top-line revenue.

Successful SCA is not a passive pursuit. The regulation comes with a number of exemptions and exclusions, depending on the value of the transaction, the level of risk involved, the location of the buyer and the various financial and payment institutions involved and whether the payment is a recurring payment, for instance.

Some transactions can be designated as trusted under SCA, as long as a consumer expressly tells their card-issuing bank that they don’t want extra scrutiny applied when they are buying from a certain merchant — and as long as the bank agrees that SCA won’t be applied.

EVOLUTION OF FAILURE RATES



What PSD2's new SCA requirements mean for retailers

Q&A with the British Retail Consortium (BRC) & Maplin

While the early effects of SCA have become painfully obvious for merchants still adjusting to the new reality, the long-term effects are still unknown.

Nowhere is the extent of the mystery deeper than in the United Kingdom, where enforcement of the robust authentication process does not take effect until March 2022.

We sat down separately with two retail professionals who are intimately familiar with the concerns of merchants to gain a better perspective of what this coming change will mean for UK retailers.

The first is Andrew Cregan, head of finance policy for the British Retail Consortium (BRC). And the second is Ollie Marshall, managing director of Maplin.

The BRC is the key retail trade association in the UK. Maplin is one of the UK's best-known retailers, specialising in electronics.

The interviews have been edited for clarity and brevity.

Andrew Cregan

Signifyd

What are the key areas BRC members have expressed concerns around in 2021?

Andrew

When it comes to payments, I think most of the concerns have been around how the industry should adapt for strong customer authentication and how businesses can maintain frictionless customer journeys online.

Signifyd

Are there any concerns around the added layers of security being put in through SCA that could impact the customer experience?

Andrew

With strong customer authentication, the biggest risk to businesses is that solutions are put in place in order to meet the rules that aren't practical for or intuitive to customers.

When customers start a new authentication process that they haven't been through before, that can actually be a trigger that leads the customer to believe that they may be encountering a potentially fraudulent or suspect transaction.

There are some solutions to comply with strong customer authentication rules that have been explored that just wouldn't be practical. But largely those have been put to bed.

Overall, the solutions which have been put in place have the potential to work well. A key factor for success is that all aspects of the payment ecosystem are ready and that there is effective communication and interoperability amongst the players.

The experience for the customer must be straightforward, but also it must be communicated well beforehand, so that it's fully understood.

Signifyd

What does the near-term SCA future look like?

Andrew

The ways in which strong customer authentication is implemented between now and the final enforcement deadline will be extremely important as to the impact it will have on fraud. It will also affect customers' perception of ecommerce in terms of its convenience and ease of use. This will shape the tendency of people to want to shop online.

Even before the enforcement deadline we'll continue to see increases in SCA requests. And therefore I suspect we will start to see more and more ecommerce transactions declined as they may not be SCA compliant. What's critical now is that the banks, and the card companies and retail industry work together to ensure that there's seamless communication among all parts of the payment chain.

Signifyd

Were you surprised when the SCA was pushed back again?

Andrew

The EBA (European Banking Authority) pushed back the deadline for the European Union as the FCA (Financial Conduct Authority) has done here in the UK. And although we might be at a point now where the enforcement deadline has come into force across the European Union, I think individually within the member states, there is a patchwork of actual enforcement activity. There are, therefore, different pictures across different markets or EU member states.

Here in the UK, the industry has been supportive of the delay in implementation given the bottlenecks in the process of preparing for strong customer authentication.

One of those bottlenecks was getting the Information Commissioner's Office (ICO) to agree that it would be possible to use behavioural biometrics without the explicit consent of the customer. If explicit consent were required, it would have essentially sunk the behavioural biometric option. As a result, we now have an authentication factor that's un-intrusive and can work in the background.

The security measures involved in 3D Secure 2 will be the active element of SCA stopping fraud when a card transaction is involved.

Static passwords could have led to huge basket abandonment and disappointment. It would have been an extremely bad outcome for businesses and for consumers alike.

The ICO has made the right decision to allow behavioural biometrics to do their thing in the background, meeting SCA requirements without a damaging level of intrusion in the payment process as would have been the case with static passwords.

That's been a good outcome, but it took a long time to get to it. Hence one of the reasons for the further delay.

Ollie Marshall

Signifyd

How do you see SCA affecting fraud and the types of attacks you might see?

Ollie

Generally speaking, I'm very pro-bringing-in-all-this-stuff, making it hard for fraud to take place, however, there is going to always be a trade-off there by making the checkout experience high-friction.

I'm pleased that it got delayed because I think the market was not ready. And what I'm seeing, I'm talking to software vendors and lots of different people, a lot of technology is now starting to spring up to make sure that we get all the benefits of SCA, but still can check out with your fingerprints, for example, and don't have to go through this big laborious multifactor authentication.

I don't think it's going to be a big, big problem when it does kick in. I actually had a demo from Signifyd with some new stuff they've come out with. So we will be working with someone around this that is making the two-factor a lot more seamless than having to type in an SMS code and all that rubbish.

Signifyd

Is there any particular kind of attack that you think SCA will be particularly good at filtering out, or not particularly good at?

Ollie

On the harshest end of the two-factor authentication, it's going to be the case that no fraud can get through, generally speaking.

It's worth saying, in one aspect, some fraud will still get through, which is like the friendly fraud.

Then there's someone stealing your credit card based in X faraway country. That stuff should just be stopped in its tracks. And the real consideration is going to be: But how do we still make it so that the checkout experience is still quite frictionless?

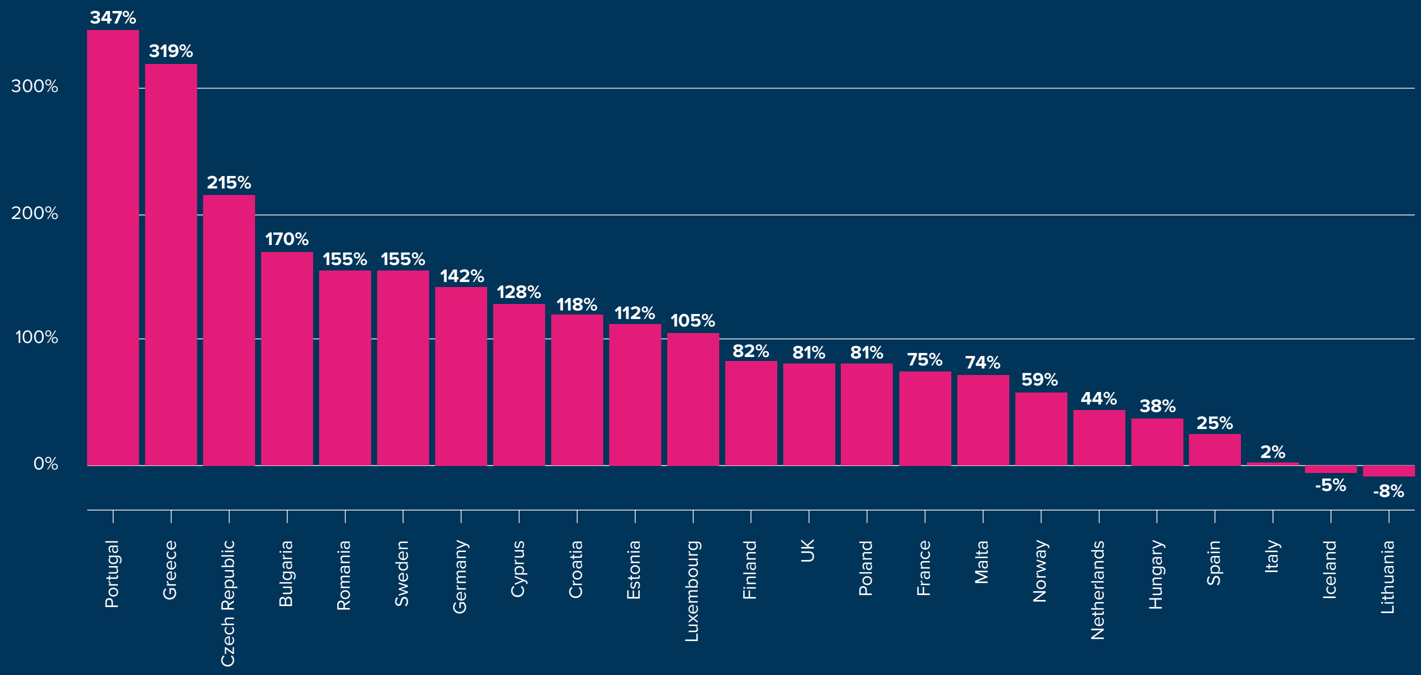
Signifyd

To what extent do you see SCA affecting the customer experience?

Ollie

So I'm actually optimistic that by March 2022, there are going to be different solutions out there that people will already be using. That's going to make stuff quite seamless. I'm personally not anticipating that it's going to be this like doomsday cut-over, where everyone starts getting pinged with SMS. So for me, I'm not worried about that, but maybe I'm being optimistic.

FRAUD PRESSURE ON LOW VALUE TRANSACTIONS



Fraudsters have dramatically increased their attacks on low-value transactions since the enforcement of SCA in much of Europe. Smaller order values are exempt from SCA and therefore make for easier fraudulent purchases. What fraudsters don't get in value, they make up for in volume. This chart shows the change in fraud pressure by country after the enforcement of SCA.

Successful SCA starts with a robust fraud prevention strategy

As powerful as SCA done right can be, it's not an end-all when it comes to fraud. In fact, the foundation of a successful SCA strategy is a best-in-class fraud protection solution and strategy.

Think about it. Yes, SCA, when it is in play, shifts liability. But if the bank is hit often enough by fraud, it will tighten up its standards for approving orders, meaning fewer sales for the merchant.

Beyond that, remember that one of the key strategies to living in a world with SCA is to wisely lean on exemptions and exclusions to avoid SCA checks for as many orders as possible.

What is the one thing we know about those orders? They are not being protected by SCA and so a retailer needs to find an alternative way to protect itself and ideally shift liability elsewhere.

Beyond that, consider the following three SCA points:

1. Low fraud rates are required for key exemptions that allow consumers and merchants to bypass SCA.
2. SCA does not cover every transaction a merchant will process — far from it.
3. Fraudsters are innovative and entrepreneurial. SCA may prove a barrier initially, but professional fraud rings will find an alternate path of attack.

Consider the SCA exemption for low-value orders, in particular those of €30 or less.

Signifyd data shows a significant increase in fraud pressure on those orders in countries where SCA is currently being enforced. Fraud pressure targeting low-value transactions in Portugal and Greece is up more than 300% since the new payment regulation began being enforced in those countries.

Signifyd's Fraud Pressure Index is based on the change in volume of orders considered to be very high risk. Very high risk orders are assumed to be fraudulent orders, given the amount and severity of red flags they contain.

Based on the index, fraud pressure was up by triple-digit percentages in 11 countries where SCA is enforced, including Sweden (155%) Germany (142%), Croatia (118%) and Luxembourg (105%).

It's another sign of fraudsters' perseverance and creativity and a reminder that keeping payments secure and customers happy with seamless transactions is an ongoing battle on multiple fronts.

> “I have learned that strong authentication is not a full guarantee to stop fraud.”
>
> OLIVIER EROL, FRAUD MANAGER AT BACK MARKET

Olivier Erol, fraud manager at Back Market, a Signifyd customer and Paris-based electronics retailer, said he discovered SCA’s limitations early on.

“I have learned that strong authentication is not a full guarantee to stop fraud,” he said.

Besides payment fraud, there is friendly fraud, as we mentioned, and policy abuse.

During the pandemic, Signifyd has detected a dramatic spike in non-payment fraud, such as false claims by customers that an ordered item never arrived or that what did arrive was unsatisfactory for some reason.

In fact, in the course of the pandemic, Signifyd’s Consumer Abuse Index reached levels five times what it was prior to the pandemic. The index measures the rise and fall of abuse rates of legitimate cardholders by examining chargebacks challenged by Signifyd and successfully won. The index assumes winnable chargebacks are highly likely to be consumer abuse.

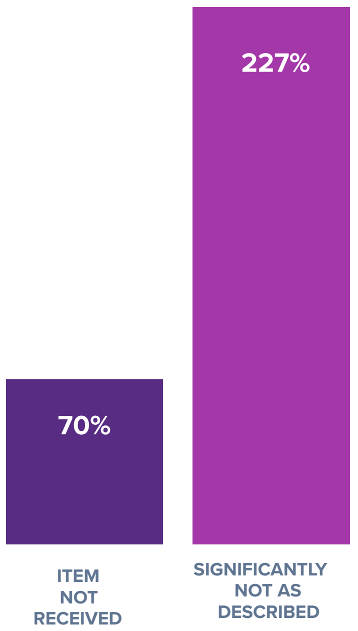
While the Consumer Abuse Index is global, the trend is even more dramatic in Europe. Signifyd data shows that the number of suspicious claims that an item arrived in unsatisfactory condition increased by 227% from the first half of 2020 to the first half of 2021. Suspicious claims that an item was not received were up 68%. A suspicious claim is defined as a claim that Signifyd determines comes with enough red flags to be formally challenged.

Furthermore, in 2020 more than 30% of consumers surveyed in the United Kingdom by Signifyd said they had falsely claimed that an order never arrived or that the item was unsatisfactory in order to keep the item and claim a refund.

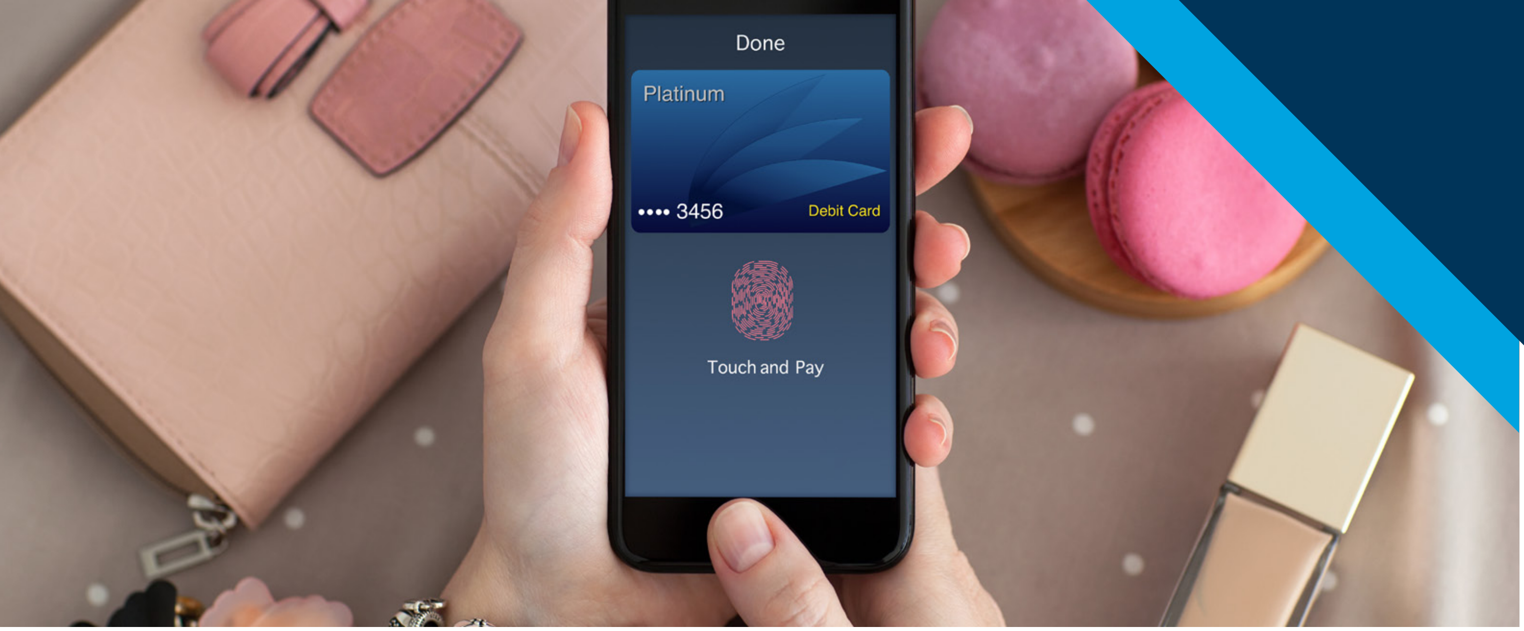
While those findings can’t be attributed to SCA, which is not yet being enforced in the UK, they are a strong indication of a growing trend that could reasonably be expected to accelerate in the SCA era.

It’s better, then, even for retailers with top-notch SCA strategies in place, to also watch their unprotected flank.

YEAR-ON-YEAR COMPARISON OF FALSE INR AND FALSE SNAD CLAIMS



More than 30% of consumers surveyed in the United Kingdom by Signifyd said they had falsely claimed that an order never arrived or that the item was unsatisfactory in order to keep the item and claim a refund.



Exemption management powers excellent SCA customer experience

While it seemed for a time that SCA would never arrive, enforcement has become very real across much of Europe.

Now that it is here, retailers are best served by embracing the best way to carry out SCA while still providing a top-notch customer experience.

The answer: Intelligent exemption management.

First understanding and then wisely deploying exemptions will allow a significant proportion of transactions to be exempted from SCA. That means customers will not face step-ups or even the need to leave a retailer's site in some cases.

In general, exemptions and the closely related exclusions are in play when the following conditions are met:

- The order is low risk and low value.
- The merchant and its bank have maintained a low fraud rate and the transaction meets certain value limits.
- The transaction is considered "out of scope." The list for these exclusions includes phone or email orders, prepaid card transactions and transactions when the acquiring bank or the issuing bank are outside the European Economic Area — or "one leg out transactions."

One other exemption is available, but a consumer's bank must agree to allow it in order for it to be applied.

It's called the "Trusted Beneficiary" exemption. It can be applied when a consumer expressly tells the bank that issued their credit card that they don't want extra scrutiny applied when they are buying from specific merchants. Again, the issuing bank can refuse to allow the exemption.

Needless to say, merchants have their hands full trying to manage all these exceptions to the SCA rules. Again, though, there is an answer in innovative technology.

Signifyd's Payment Optimisation solution, for instance, includes Dynamic Exemption Management, which relies on transaction data from its vast Commerce Network to automate exemptions. The solution performs Transaction Risk Analysis (TRA) to ensure there are no fraud red flags. In that way the solution maximizes the number of transactions that are SCA exempt and routed down a friction-free path to payment, avoiding the sometimes troublesome 3D Secure.

The alternative path maximizes authorization rates, which optimizes revenue for merchants and markedly improves the experience for their customers.

Part 3: The many faces of modern ecommerce fraud

Now that we've set the stage for what's to come, let's take a deeper dive into some of the fraud trends that gained prominence in the course of 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 possibly 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.

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.

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

Synthetic identities

The wealth of purloined personal information floating around during the pandemic fuelled 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. 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 manufactured person they made up 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."

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 (ECOMMERCE, 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, at a centralised locker or other location. The behaviour persists today.

Signifyd global data shows that the category of transactions that includes click-and-collect increased by 210% since world health officials declared the pandemic.

And with the click-and-collect spike and continued popularity came a great opportunity for those with a criminal bent. Online orders that are later picked up 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. Retailers need to adjust — if they haven't already.

In short, said 451 Research of click-and-collect orders, "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."

No question, retailers need to consider the new vulnerabilities as they launch or expand click-and-collect.

"In these situations, it's important for businesses to have a robust set of systems and processes in place to ensure that when they're handing over goods to customers that those customers can prove that they are who they say they are," said Cregan of the British Retail Consortium.

Better still when it comes to click-and-collect are innovative systems that are able to detect fraudulent intent at the point of purchase — in this case, the merchant's website.

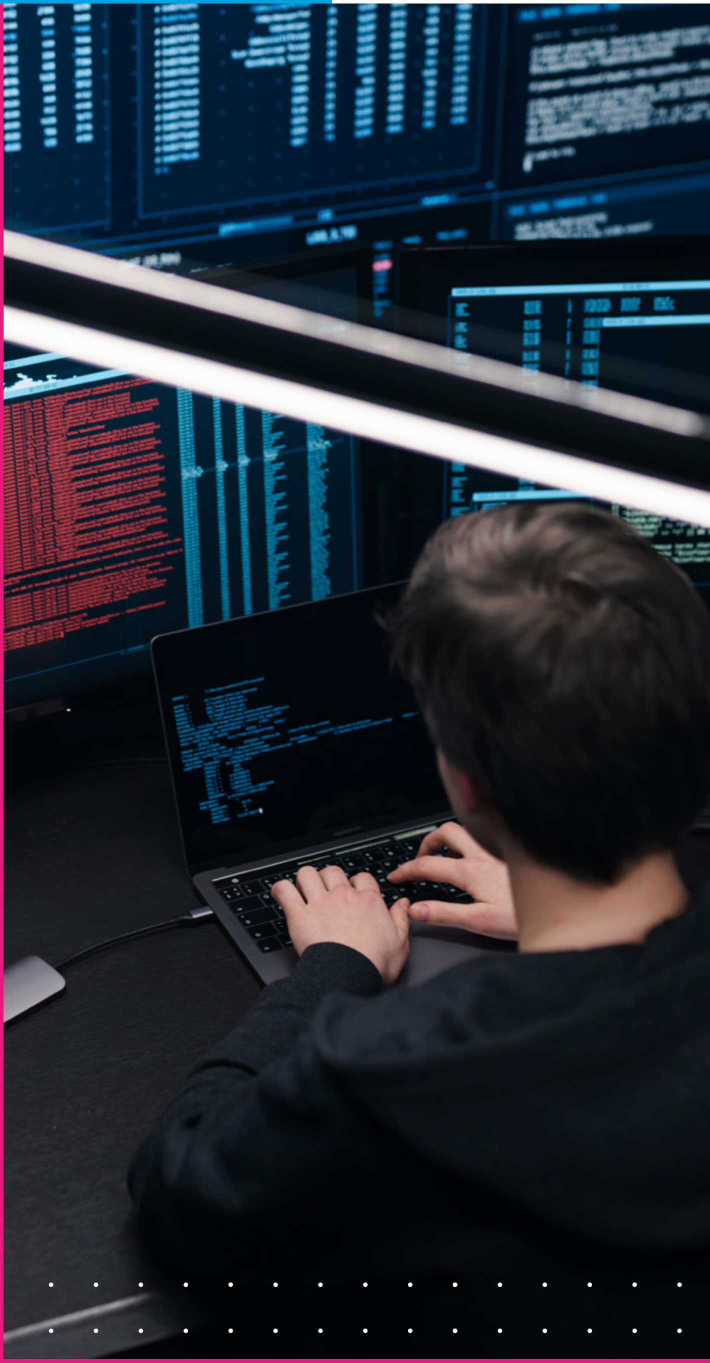
Policy abuse

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 said. "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 alway 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 — PlayStation 5, 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 UK 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.

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.

Returns in general have been a growing concern for merchants as online shopping has exploded. While the return rates for brick-and-mortar purchases generally run in the single-digit percentages, that figure skyrockets when it comes to ecommerce. Online returns can easily run in the 25% to 40% range, depending on the vertical.

But the problem is even deeper when you consider that some portion of those returns are fraudulent. In fact, the National Retail Federation, working with Appriss Retail, determined that 7.5% of online returns are fraudulent.

Now add in associated costs — shipping, inspecting and disposing of bogus returns — and return scams cost retailers billions of euros every year.

Return fraud 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. Maplin has received cans of beans as stand-in for returned electronics, for instance. In another notorious case, a potato stood in for an iPhone. No doubt the retailer was fried.

Fraud stories from the Signifyd vault

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.

Old college try

In early 2021, the students at Brunel University in West London suddenly seemed exceptionally acquisitive.

Dozens of products, purchased from merchants on Signifyd's Commerce Network were ordered to be shipped to the halls of residence on Kingston Lane, Oxbridge, at Brunel.

But why? Was it students settling into their temporary homes? Was there a reselling scheme underway to help with pizza and beer money?

The airpods, electric scooters, designer sneakers and other apparel were all being ordered from IP addresses at the university. They were being purchased at an unusual pace and through an unusual payment method — credit cards issued in Taiwan and Hong Kong.

And there was one other unusual thing about the deliveries: Because of COVID-19, the Brunel halls of residence were closed. Students were staying off campus.

The orders were, in fact, the work of a sophisticated fraud ring that moved quickly among merchants so that large volumes wouldn't be an immediate tip off. They also knew that they could have orders shipped to the university and no one would be the wiser because the campus was all but deserted.

The ring, however, was not sophisticated enough to outsmart Signifyd. Its machine-learning solutions and its risk intelligence team quickly put the pieces together and shut the fraud ring down.

Single parent mule

After losing her job to pandemic cutbacks, a woman living in the U.S. state of Pennsylvania 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 U.S. basketball fan — a big one — bought €9,000 worth of souvenirs autographed by the late Los Angeles 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 €17,000 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?

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 resellers. And they went to work.

Scalpers set the bots loose, buying thousands of PS5 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 locations 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 DHL or FedEx.

Part 4: 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 outdoors goods emporium, faced its challenge at the height of the pandemic when its online orders increased by 50% overnight.

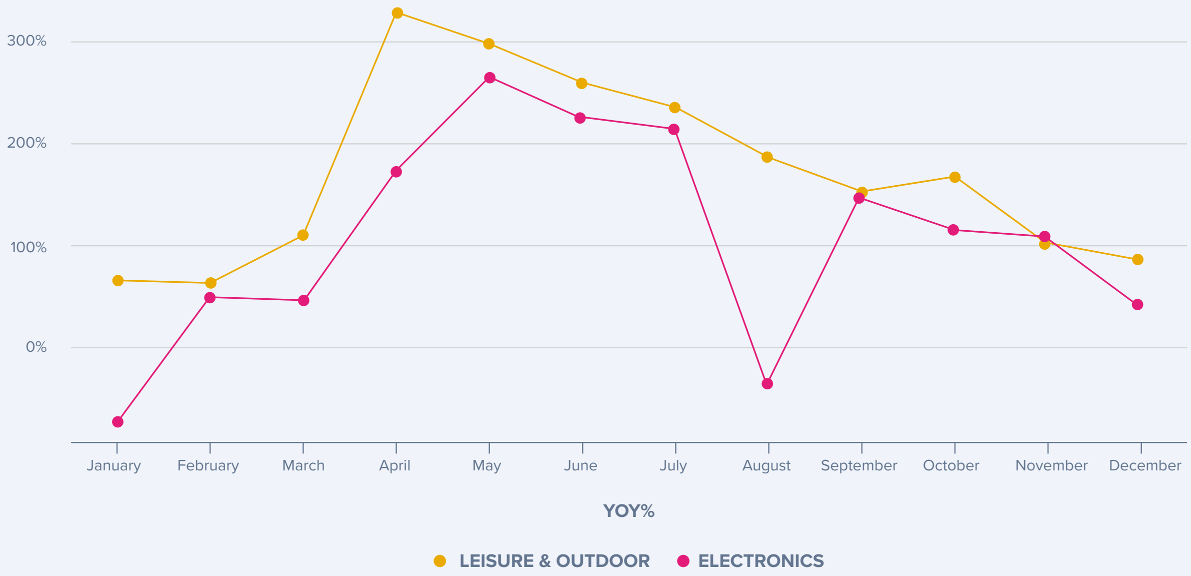
Risk team members were reviewing a quarter of the orders coming in, often calling customers to try to verify their identities.

"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%.

As importantly, Signifyd's order automation ensured that even with the online order explosion Mack's could maintain the excellent customer experience that it is known for.

YEAR OVER YEAR ECOMMERCE GROWTH — LEISURE & OUTDOOR AND ELECTRONICS SALES



UK electronics retailer Maplin also maintained a competitive edge through order automation. The Maplin team quickly discovered that its shift from omnichannel to all-online sales couldn't be successful without a robust solution that could quickly review orders for fraud and have them swiftly on their way to their intended recipient.

Maplin's Marshall said he and his team knew right away that its payment gateway's fraud monitoring would not be sufficient and so they turned to Signifyd.

"We've always taken the approach that we want just a plug-and-play solution, which Signifyd is for us. In a way I don't have to think about it too much," Marshall said.

Both Maplin and Mack's have their biggest sales peaks concentrated during a few months of the year. For Maplin, it's the traditional holiday season, or Q4.

For Mack's, it's duck-hunting season — roughly November to January — when it does 70% of its business.

All of which provides a playbook for all merchants, who see their own scaling challenges, particularly in the new era of ecommerce that was ushered in by COVID-19 lockdowns.

Avoiding the holiday holdup

As retailers around the world prepare for the holiday crush, they can dissect how Maplin and Mack's embraced automated order flow and fraud review fuelled by machine learning.

In Signifyd, Maplin and 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.

No question, returns are a growing challenge for online retailers. Marshall said return abusers are ingenious, using the shipping receipt to receive a refund before the "product" they shipped back is received and reviewed. There are various ways to pull off the scam.

"Some favourites are, you know, sending those cans of baked beans that weigh a similar weight to a PlayStation they bought," he said. "Therefore, they get the money, generally speaking."

Additionally, Signifyd's Commerce Protection Platform future-proofs an enterprise's fraud and risk management with Payment Optimisation. The solution, for instance, finds the most efficient way to route transactions to ensure compliance with regulations such as SCA, while providing 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," Mack Prairie's 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%.

Across Europe, ecommerce sales increased 31% when you compare figures for 2020's pandemic months with the prior year's sales.

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.

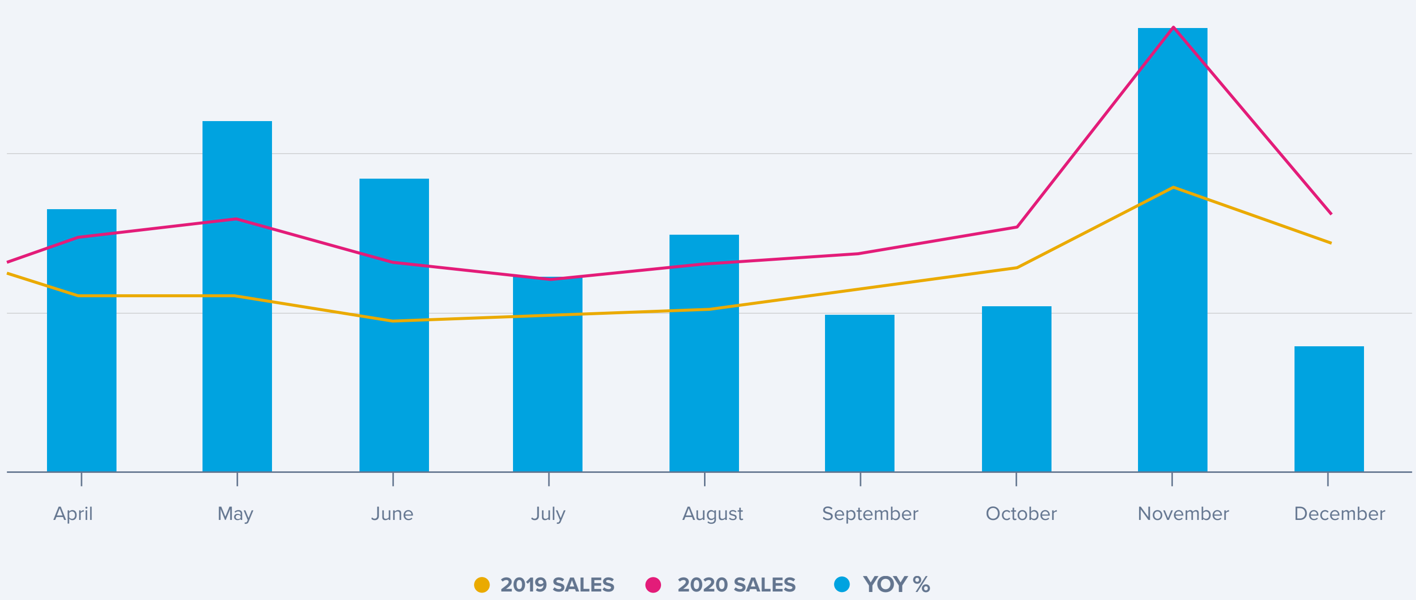
"Even though this year we saw the largest growth in our Sonos ecommerce sales through the holidays, I found it to be the most stress-free holiday season that we've had, in part because of the automation we were able to deliver with Signifyd," Harris said. "It felt like the least stressful holiday season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

Marshall at Maplin also sees a big holiday season in 2021 — thanks to the accelerated shift to online shopping brought on by the pandemic.

> What were once considered benefits of purchasing digitally are now habitual practices that will prevail in holiday retail indefinitely.
>
> **JENNIFER RYAN, MARKETING DIRECTOR**
>
> astound COMMERCE

YEAR-OVER-YEAR CHANGE IN ECOMMERCE SALES — THE PANDEMIC MONTHS



"The year-on-year growth is very big," he said. "After 2020 going into 2021, there's a very significant uptake of what is now the new normal for us in terms of level of orders and revenue on a monthly basis. It left us with much higher levels than what we were doing pre-COVID."

Holiday sales could easily increase 3x over non-holiday sales. And of course, that increase will come off of the higher post-pandemic baseline.

Independent digital commerce specialist and Signifyd strategic partner Astound Commerce talked with Signifyd about the new era of ecommerce. "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.

Fraud's seasonal shift, vertical-by-vertical

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 compared to pre-pandemic levels, ecommerce fraud pressure was up more than 460% in Europe, as we headed into the 2020 holiday season.

But of course that wasn't true for every retail vertical, nor was it true for any given point in time. In fact, during the summer of 2020, the increase in fraud pressure in Europe was as low as 10% over pre-pandemic levels.

Again, Signifyd's Fraud Pressure Index, from which these numbers were derived, looks at the fluctuation in very high-risk orders, which are presumed to be fraudulent.

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 jewellery, outdoor goods, home improvement — might see their big order surges in seasons other than the holiday season.

February for jewellers, 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 will find a way

Fraud will follow the path of least resistance. Throw up one barrier here, the fraudsters will attack over there.

And so shifts in fraud pressure can be influenced by the type of transaction as well as the vertical in which an order is being placed.

Consider, for instance, strong customer authentication (SCA) which has rolled out across much of Europe and will be enforced in the UK beginning in March.

While the robust, two-factor-authentication-based approach can be a powerful way to prevent fraud when it is applied to transactions, it is not applied to all transactions.

Mail order and phone orders are not subject to SCA. Neither are purchases made with anonymous payment instruments — a complicated way to say prepaid gift cards.

And then there are those exemptions that we covered in Part 2. By definition, exemptions are not subject to SCA and there is strong evidence that fraudsters across Europe are taking advantage of that fact. Remember the data we discussed earlier that showed a marked increase in fraudulent activity on low-value orders (those of €30 or less).

> 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 PUCCETTI, COO**
>
> blue acorn iCi
> an Infosys company

Part 5: 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 here and with spikes in daily order volume creeping higher.

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

Risk Analyst Frederikke Rasmussen explained it this way: "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."

Instead, when predicting what fraudsters will be up to this holiday season, Signifyd's 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 ecommerce landscape has changed through the course of the pandemic.

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."

> 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**

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, Manager of Risk Intelligence Luz Cervantes is seeing a spike in it and is anticipating the scheme 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."

Merchant insight: How Maplin sees current and coming fraud trends

Did we mention that online fraud is constantly evolving?

Fraudsters find an opening, exploit it, share the opportunity with their fellow fraudsters. And when the scheme is discovered and the vulnerability is plugged, the fraudsters move on.

Ollie Marshall, managing director of Maplin, explained that during holiday 2020, the retailer saw attacks targeting game consoles.

But today or tomorrow it could be anything.

"It's kind of a moving target, in that these holes are going to continue to open up."

Electronics, Maplin's core business, are a big fraud target in general, he added.

"So we're in consumer electronics — probably one of the worst categories to be in, in terms of fraud. What we sell, it's obviously high value, relatively small, very resalable, all the characteristics that fraud loves. Year-round we sell hot products. We just obviously expect all our systems and Signifyd to be able to look after us."

As for types of fraud, it's something of an arms race — stop one form of attack and fraudsters will shift to another.

Maplin recently saw a spate of carding attacks — automated assaults in which bots rapidly and repeatedly order from a website with stolen credit card credentials.

Unauthorized reselling has been a threat and a sign of the times. With supply chains strangled, certain hot products are in short supply.

"That actually did result in people effectively wholesale buying from us," Marshall said, "and then presumably reselling it. So, that's not desirable for us."

Attempts at falsely claiming an ordered item was never received and fraudulent return attempts are a constant battle, he said.

And while in some ways fighting fraud, with fraud rings changing targets and tactics, is a never-ending effort, Maplin has been successful, working with Signifyd, at turning away the attacks as they come.

"All solvable," as Marshall put it, "which is something worth saying."

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 6: 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 defence.

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 centre 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 partially shielded from the ill effects of an economic downturn or a strategic misstep by the business.

Onlines 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 centres 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 omnichannel experiences like click-and-collect 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 MOUGHTY, FORMER DIRECTOR OF ECOMMERCE**
>
> LACOSTE

Part 7: Assessing your fraud maturity

As we've seen, the ecommerce landscape is one that is continually shifting, and with the enforcement of SCA, merchants now must figure out what the right SCA strategy looks like for them and their customers — otherwise, they risk falling victim to SCA-induced friction and turning away their hard-earned customers to competitors offering a smoother checkout experience.

All is not lost though. In fact, for merchants, determining what the right SCA strategy looks like for them involves some research and a little soul searching.

This SCA checklist outlines everything merchants need to know and what else they must consider to determine what the right SCA approach means for them and their customers, including:

- What your average basket size is
- Knowing where your customers are
- What your payment service provider's performance and protection details involve

Get the Full Checklist

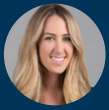
Produced by:

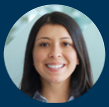
Mike Cassidy,
Head of Storytelling

Alyssa Gray,
Product Marketing Manager

Ping Li,
Vice President of Risk and
Chargeback Operations

Ben Davidson,
Manager of Risk Intelligence


Ashley Kiolbasa,
Director of Product Marketing


Luz Cervantes,
Manager of Risk Intelligence

Irish Show,
Lead Risk Analyst

Colin McCloskey,
Lead Risk Analyst

Frederikke Rasmussen,
Risk Analyst

Phelim Killough,
Data Analyst

With contributions from:

FIS blue acorn iCi an Infosys company astound COMMERCE MAZE

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 the Digital Commerce 360 Top 500 lists. Signifyd is headquartered in San Jose, CA., with locations in Denver, New York, Mexico City, São Paulo, Belfast and London.

Signifyd

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

SUPPORT
www.signifyd.com/contact