



E-COMMERCE AND OMNI-CHANNEL FRAUD FOLLOWING THE DIGITAL ACCELERATION

White paper presented by The Fraud Practice, Inc.

E-COMMERCE AND OMNI-CHANNEL FRAUD FOLLOWING THE DIGITAL ACCELERATION

Written by: Justin McDonald, Sr. Risk Management Consultant

Introduction	3
The eCommerce and Omni-Channel Acceleration	4
Winning and Losing Trends: Pure Play eCommerce	6
Rules versus Models	6
Readiness to Scale	9
Winning and Losing Trends: Omni-Channel	11
Evaluating Fraud Solution Providers with a Unified Commerce Mindset ...	14
Conclusion	16

A white paper prepared by The Fraud Practice Inc.

For additional updates and commentary, please visit:

FraudPractice.com

© 2021 The Fraud Practice Inc. All Rights Reserved.



Introduction

It's an understatement to say that 2020 was a difficult year, but the seismic shifts that occurred brought innovation and an unimaginable acceleration of growth in eCommerce. This is especially true in the world of retail, where the line between eCommerce and physical retail continued to blur. Throughout the pandemic, consumers flocked to the convenience and safety of online shopping, but still required the immediacy or convenience of curbside pickup. Retailers quickly learned that a true omni-channel strategy, while already important, was now a must-have for future success.

Whether pure play eCommerce or brick-and-mortar first, all retailers were forced to adapt quickly in 2020. Some were able to make the necessary adjustments to survive, but others pivoted even further and implemented strategies to grow beyond even next year's sales forecasts. What separated those who thrived from those who merely survived?

The intent of this white paper is to examine the common threads across organizations associated with success versus challenges in response to COVID-19, the economic shutdown it initiated and the lasting impacts on consumer preferences and purchasing behaviors.

Organizations that succeeded embraced the evolution of their risk management strategies to support the unexpected growth. This mindset will remain important into the future as organizations navigate online and omni-channel sales in an era of increased volume, increased risk and increased consumer expectations. Understanding what is needed to maintain success in the current eCommerce and omni-channel environment is imperative, as many of the changes we've experienced in the wake of 2020 will continue to persist.

The eCommerce and Omni-Channel Acceleration



Total retail sales in the US grew around 7 percent from 2019 to 2020 while US eCommerce retail sales increased 32.4 percent year-over-year, according to DigitalCommerce360¹. According to McKinsey², US eCommerce penetration experienced ten years of growth in three months. Many to most of the consumer retail trends and changes in response to the pandemic are expected to persist, with DigitalCommerce360 measuring continued US eCommerce retail growth of 39 percent in the first quarter of 2021.

While the acceleration of eCommerce in 2020 was unprecedented, it pales in comparison to the explosive growth of buying online to pick up curbside or in-store. This omni-channel commerce space has grown so fast, you may have seen some new terms and acronyms popping up the last couple of years. This includes:

- **BOPIS** - Buy Online Pick Up In-Store
- **BOPAC** - Buy Online Pick Up At Car
- **Click-and-Collect** - Collectively refers to either or both BOPIS and BOPAC
- **Curbside Pick Up** - Frequently used term that represents BOPAC
- **ROPIS** - Reserve Online Pick Up In-Store. Inventory is held for period of time but the payment event occurs in-store at pickup event
- **BORIS** - Buy Online Return In-Store. Huge convenience for consumers but also a major target of fraudsters

BOPIS or Click-and-Collect was not born out of the pandemic, it was already in a phase of early adoption. The pandemic, however, greatly accelerated the adoption of this omni-channel sales method by leaps and bounds. Now with less distinction between eCommerce and traditional retail, many are referring to this omni-channel phenomenon as **Unified Commerce**.

Sources:

1 - <https://www.digitalcommerce360.com/article/coronavirus-impact-online-retail/>

2 - <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-fifty-the-quickening>

Omni-Channel represented one-fifth of US eCommerce retail growth in 2020.

According to data from eMarketer³, US Click-and-Collect sales more than doubled from \$35 billion in 2019 to \$72.5 billion in 2020. Click-and-Collect grew from 5.8 percent of retail eCommerce sales to 9.1 percent over this period of time. While representing just 9.1 percent of US retail eCommerce in 2020, Click-and-Collect orders were responsible for 20 percent of US retail eCommerce growth.

Forecasts from eMarketer predict that Click-and-Collect, or BOPIS and BOPAC, are more than just a flash in the pan. After US Click-and-Collect revenue doubled in 2020, it is expected to nearly double again by 2024, when it will represent 11.7 percent of US retail eCommerce sales.

While many consumers might have tried BOPIS for the first time in 2020, most will continue utilizing this omni-channel shopping method into the future. For goods that are bulky and heavy, BOPIS eliminates consumer shipping costs, even when a good is shipped to store. Overnight and other rush delivery options are expensive. For items currently in-stock, BOPIS offers immediacy with no shipping costs. Additionally, a physical retail presence offers consumers peace of mind when it comes to returns. Consumers are more likely to purchase an item online knowing they can complete a return in-store if it's not the right fit. Exclusively eCommerce merchants have partnered with drug stores and others to offer a physical location for dropping off items to return with this in mind.

According to Sift network data, between 2019 and 2020, fraud rates in omni-channel retail increased 50% and the average value of fraudulent orders increased by 9%.

For some industries, BOPIS was the jumpstart they needed to grow their digital channels. Industries like grocery and fast food had struggled to grow eCommerce and mobile channel sales, but now that many consumers tried BOPIS at their grocery store or favorite quick service restaurant (QSR), they're hooked.

For these reasons and more, the expectation is that BOPIS will continue to grow, just not quite at the rapid pace of 2020. Likewise, consumers who greatly increased their online shopping in 2020 aren't going to suddenly revert back to pre-pandemic behavior. For many consumers, COVID was the catalyst to conduct more eCommerce and try BOPIS, but now that the convenience and benefits are realized, consumers' preferences have changed. Unfortunately, what's convenient for consumers is also exploitable by fraudsters, with unified commerce presenting expanded opportunities for committing various fraud schemes.

Sources:

3 - <https://www.emarketer.com/content/click-collect-already-popular-option-finds-new-gear>

Winning and Losing Trends: Pure Play eCommerce

According to Sift network data, the device types that fraud occurred from most in 2020 were:

1. Mobile (iOS, Android) - **62%**
2. Desktop (Mac OS, Windows, Linux) - **36%**
3. Other (Consoles and other platforms) - **2%**

The average order value of a chargeback was \$241.99 in 2020, according to Chargeback Data Scientists.

Multi-channel retailers needed to quickly adopt an omni-channel strategy or expand their existing one, but pure play eCommerce retailers needed to quickly pivot as well. Similar to those in the omni-channel environment, eCommerce merchants had varying levels of success as they navigated the rapidly changing landscape. 2020 was not a temporary adaptation, rather an accelerated evolution, and this is true for pure play eCommerce as well.

While eCommerce-only merchants weren't reliant on BOPIS, they faced many of the same challenges in terms of increased customer risk profiles, increased volumes and increased consumer expectations in terms of user experience and fulfillment. For many, March, April and subsequent months in 2020 brought online transaction volumes similar to that of the holiday season, only with little notice or time to prepare.

Seemingly overnight, risk management strategies fell apart. Consumer patterns completely changed in response to a black swan event. Consumers were purchasing more frequently, purchasing with notably higher average order values (AOV), and purchasing goods they typically hadn't purchased online before. This brought waves of new customers, as casual and even first-time eCommerce shoppers became "whales."

Rules Versus Models

Rules lists and risk models deteriorated at a pace like never before seen. Fraud and good customer purchase patterns typically morph overtime, but 2020 was an abrupt paradigm shift. Velocity thresholds had to increase, policy rules had to change, and there was little-to-no historical data analysis to support the eCommerce channel's "new normal."

Fraud has always been a moving target, but now this movement was vast and rapid. It was significantly more difficult to detect high risk versus “new normal” transaction patterns. Depending on the organization, the issues resulting from these challenges manifested in one of two ways:

1. Higher fraud losses from inability to stop fraudsters hiding in elevated order volumes and higher average order values amongst legitimate customers
2. Higher sales insults and sales conversion issues from merchants tightening or not touching their controls as online activity skyrocketed



Fraud is a moving target, but in 2020 that movement was especially vast and rapid.

Everyone had to adapt, the question was how quickly an organization could pivot. Organizations with a model-based fraud scoring or custom modeling solution were, in general, in a better position to adapt quickly relative to merchants utilizing a rules engine as their primary risk architecture.

Those with rules engines had to redesign, replace and write new rules. In many cases, this meant scrapping half or more of the existing rule set. It's not uncommon for merchants to be managing repositories of more than 100 rules with decision trees and nested rule sets that vary based on customer or order characteristics. The magnitude of these operational risk changes would be difficult to manage in any environment, but was especially challenging at a time when organizations were also transitioning to work from home.

Those with modeling-based solutions took some time to adapt, but were generally able to deal with the abrupt changes in good customer purchase habits more quickly and efficiently. Machine Learning components helped make sense of rapidly changing data trends, allowing analysts and data scientists to put more emphasis on supervising the changes to their models.

The fluidity of model-based fraud strategies typically led to a quicker adjustment than a more rigid, rules-based approach as eCommerce morphed to a new normal.

Due to operational constraints, organizations relying on legacy and rules-based platforms were more likely to suffer a hit to sales conversion, being forced to rely more on old patterns while the new behavior was being digested, analyzed and converted to new rule sets and thresholds. These organizations may have been able to layer on temporary rules like Band-Aids, attempting triage while they worked on a more permanent fix. This approach cut losses, but typically while infringing on legitimate customers and creating additional tech debt.

Life wasn't easy for organizations with modeling-based risk platforms, but in many ways the transitions were less abrupt. It still took time to adapt, but leveraging a platform that continuously monitors changing trends and customer purchase patterns helped accomplish this more seamlessly. **A supervised Machine Learning model-based approach was best positioned to deal with the abrupt changes in good customer purchase habits more quickly and efficiently.**

Whereas rules engines tend to be more rigid, typically having hard thresholds (such as a shipping address being used three times in 24 hours), model-based solutions are often more fluid by looking at patterns and high-risk activity based on rolling averages and the number of standard deviations something is away from the norm. Whereas rules engines require an analyst to identify a trend change, perform analysis and edit or implement a new rule, Machine Learning automates much of this process.

What takes weeks to recognize, analyze and implement with a rules-based strategy may only take days with a model-based strategy. This is extremely significant when considering that an organization is dealing with increased fraud losses, decreased sales conversion rates, and/or increased manual review rates during the time it takes to get their risk management strategy back on target.

"Rapid market changes and disruption always attract fraudsters, who regularly hide behind unexpected upticks and declines in online order volume, and exploit shifts in customer behavior. With automation in play, cybercriminals can execute coordinated attacks at inhuman speed and scale - attacks that can only be prevented by something equally fast and flexible. That's what you get with machine learning models: the adaptability, intelligence, accuracy, and efficiency required to fight fraudsters wherever, and whenever, they show up."

Kevin Lee, VP of Digital Trust & Safety Advocacy at Sift

Readiness to Scale

A risk management strategy is never complete. It is always adapting and preparing for the next stage of evolution. Fraud trends and attacks are dynamic and sophisticated, and successful risk management strategies must be as well. Being prepared to grow, scale and evolve was the second major factor that contributed to an organization's ability to succeed during 2020.

Operationally efficient merchants prepared for the next few years of growth had the infrastructure in place to handle 2020's rapid digital transaction growth. Those who put off these investments struggled to keep pace with elevated volumes.

The merchants most well prepared for the black swan event of 2020 were those who were already operationally efficient and had a three- to five-year scalability plan already in place. There are two primary aspects to operational efficiency: maintaining a manageable manual review rate and efficiently performing post-transaction reconciliation and analytics to maintain effective automated risk screening.

When preparing for seasonal sales volume increases, merchants hire more review agents, knowing that the number of manual reviews will increase with volume. Without time to prepare for the sudden increase in online transaction volume, merchants faced two options: be able to handle increased review volume or maintain a lower manual review rate. Those who were more operationally efficient and built-to-scale were much better prepared to take on this sudden, increased volume. This was true for a small and medium merchant that keeps a 5 to 10 percent review rate, as well as for an enterprise organization that must keep order reviews closer to or below 1 percent of their transaction volume. Whether managing reviews entirely in-house, outsourcing to a vendor or utilizing a mix of both in-house and third party providers, the increased order review volume represented a significant increase in risk management costs.

Across Sift's network data, site credits and gift cards were among the top items purchased fraudulently by cybercriminals.

Operational performance influenced sales conversion as well. Merchants not prepared to take on additional order reviews likely declined many of these orders. Many organizations purged their review queues when they became unmanageable, which resulted in each flagged order either being auto-declined or auto-accepted.



Operational activities around reconciling data, updating negative lists and re-presenting chargebacks were also impacted, and failure to keep up with these activities further hindered the ability to adapt automated screening in accordance with the changing trends and purchase behaviors. For the less operationally efficient merchants, this propagated a continuous cycle of operational strain. Failure to perform operational tasks that maintain automated risk management effectiveness led to issues with fraud losses, sales conversion and unmanageable review queues.

Years of eCommerce growth were accelerated and condensed into a period of just a few months. Organizations that were only prepared for the next year of projected sales growth fell short in terms of operational performance, as online sales volumes shattered expectations. Merchants that maintained operational efficiency with more manageable review rates were also much better equipped to handle the increase in volumes and increase in reviews. Here is a simple case in point:

Two large merchants normally have **100,000** transactions per month. One maintains a **5%** manual review rate while the other typically reviews **10%** of online order attempts. Both merchants see their transaction volume double during the pandemic. All else equal, the merchant with a **5%** review rate sees order review volume double from **5,000** to **10,000** reviews per month, an increase of **5,000** reviews. The merchant with a **10%** review rate sees order reviews double from **10,000** to **20,000**, an additional **10,000** orders that must be reviewed per month.

Winning and Losing Trends: Omni-Channel

Communication between physical and digital channels and the ability to leverage pick up and in-store signals for screening orders placed in digital channels are critical to omni-channel success.

The primary factors that dictated success versus failure for pure play eCommerce merchants were also relevant for omni-channel merchants, but these organizations faced additional challenges as consumers and businesses quickly adapted or expanded to unified commerce. Omni-channel organizations with a model-based solution at the core of their risk architecture were better equipped to handle the rapid pace of change than those relying on legacy and rules-based systems. Those who already championed operational efficiency and had multi-year scalable systems in place were also the best prepared to take on the increased transaction volumes and accompanying operational loads.

Specific to omni-channel, organizations that practiced a true unified commerce approach were better set up for success. Many enterprise online retailers were brick-and-mortar first, and many of these merchants maintained a traditional Loss Prevention (LP) or “Shrink” focused mindset. Since the early stages of eCommerce, digital channels have frequently been carved out as a different department or sub-department where risk is managed differently and independently. This separation of the online and physical worlds created additional challenges.

In 2020, these two worlds collided. Separately managing physical LP versus digital channel fraud created issues as commerce unified across channels. For many organizations, the left hand didn't know what the right hand was doing. Reduced cross-channel visibility makes risk management less effective and more difficult for omni-channel. Increasing visibility and enabling effective communication between these realms improves risk management and fraud detection capabilities.

Many merchants were considered essential and traditional brick-and-mortar loss prevention practices were still important. The key was whether information collected in the physical channel could be cultivated as risk signals and communicated to the digital channels to be effectively leveraged with automated screening.



***Common Pain Point:
Pre-pandemic, a multi-channel merchant may have had 1-2 days between the online order date and when products leave the warehouse. During the pandemic, multi-channel merchants strived to offer same day in-store pickup, often within 1 hour of the order time when items are in-stock at the store.***

This is where merchants with previous BOPIS/BOPAC experience were more likely to be successful. An established multi-channel electronics retailer may have been checking government IDs for all pickup persons while maintaining checks for high velocity counts on a pickup person's name across retail locations. A merchant who rushed to start curbside pickup for the first time in 2020 may not have implemented this from the start.

The first step to encourage omni-channel success was to collect signals that transcend online orders and physical pickup. The next step was effectively making use of these signals. While such signals could feed a rules engine or a model-based solution, modeling platforms were typically better at deriving value from these signals, particularly when Machine Learning was involved. Taking a narrow, eCommerce-focused view for BOPIS or BOPAC orders ignores many potentially valuable risk signals.

Omni-channel signals effective for screening Click-and-Collect orders:

- Velocity of Use and Velocity of Change checks around the pickup person's name across all physical store locations (when the name is consistently validated by presenting Government issued ID)
- Negative list for pickup person's name (assuming ID check at pickup event)
- Recognizing when IP or mobile geolocation is in very close proximity to the pickup store location
- Quantifying distances between billing address, IP geolocation and pickup location
- Maintaining negative lists and velocity counts on name of person physically returning items purchased online
- Performing post-transaction analysis to identify online orders associated with high number of returns in-store
- Considering the duration of time between the online order date and the time of an in-store return
- Ensuring the order or transaction ID associated with an in-store return has not already resulted in a chargeback and ensuring all chargebacks associated with orders already returned are disputed



Brick-and-mortar loss prevention leadership needed to communicate with digital fraud prevention management, and for many organizations this had never been done before. With unified commerce, signals needed to be cultivated and communicated across these channels which means across separate business departments. Relevant risk signals go beyond purchase and pickup to events to also include in-store returns. This presented new operational challenges and the organizations who best handled these challenges deployed new operational procedures accordingly.

Operational improvements to support Unified Commerce:

- New Standard Operating Procedure (SOP) documents and increased training on requiring and validating government IDs of pickup person
- Associate training and SOPs from Loss Prevention department specific to in-store returns on online orders, including the collection and validation of identity data of returning party
- Training for review agents around additional signals and tactics for performing manual order review on BOPIS orders
- New review queue management features to prioritize or separate BOPIS from traditional eCommerce orders that are flagged for review
- Ability for in-store Loss Prevention managers to add pickup person to negative list and escalate specific issues to digital fraud managers based on patterns they see on the floor
- Ability for LP managers or sales associates to lookup online order details related to in-store returns

Evaluating Fraud Solution Providers with a Unified Commerce Mindset

When comparing 3rd party providers, vertical-specific omni-channel experience is more meaningful than general omni-channel experience.

The changes that merchants experienced and the risk management improvements they implemented in 2020 were more than a short-term, quick fix. Unified commerce and BOPIS are here to stay. Online and omni-channel sales growth were pulled forward but will also remain elevated and continue to grow from here. With this in mind, it is important merchants consider omni-channel as they continue to grow and evolve their risk management strategy, both from an in-house and third party provider perspective.

Following the digital acceleration and explosive growth of BOPIS, omni-channel merchants need to consider how to maintain an open line of communication between their digital and physical channels, and consider how their fraud solution vendors will help them accomplish this. When evaluating vendor solutions with a focus on unified commerce, it is important to understand the solution provider's omni-channel experience and expertise. Having omni-channel experience overall is important, but omni-channel is as broad as retail itself. Vertical expertise within the omni-channel environment is even more critical.

Just as the base risk model should differ between electronics and apparel eCommerce merchants, omni-channel base models should be vertical-specific as well.

Expect many vendors to tout their omni-channel experience, but dig deeper. Find out the specific vertical markets or industries where they have the deepest omni-channel expertise. Omni-channel risk management and fraud patterns are very different across various industries. Grocery and quick service restaurants, for example, typically have lower margins, lower price points and more focus on containment, whereas electronics and home improvement merchants have higher price points and need to put more emphasis on preventing first-time fraud.

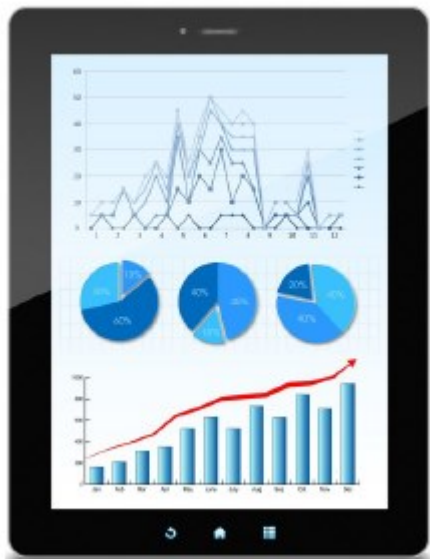
Specific to model-based fraud scoring vendors, it is important to understand the customization of base risk models for the omni-channel environment. Having one omni-channel focused risk model applied to all omni-channel merchants is very different than having an apparel merchant, electronics merchant and food/QSR merchant model, where each is specifically designed for unified commerce.

Next determine what makes risk models for omni-channel different than pure play eCommerce risk models. Some providers will support custom data fields and those custom data fields can be omni-channel focused. This may not provide as much value as a model that is designed to incorporate the pickup person's name and phone number to make use of these data points in velocity and other checks.

Link analysis and other case management platform features that support omni-channel data points will improve and expedite Click-and-Collect order reviews.

Data sharing capabilities are also important and play a major role in the value proposition of a third party service provider, particularly when there is an emphasis on detecting first-time fraud. It may be the first time a merchant has been presented a given pickup name or phone number, but the 10th time the vendor has seen this data point across their network in the last few days.

With respect to shared data networks there are two key considerations: breadth of network and support for omni-channel specific data fields. Breadth of network should consider both the size of the vendor's client list and the relevancy of the data. For example, utilizing the vendor with the most clients overall may not be as valuable as leveraging the data sharing network with the most clients in your industry. Support for omni-channel data fields is of course important for omni-channel commerce. While a shipping address is valuable for eCommerce, recognizing pickup mules in a fraudster's network provides more value for BOPIS orders.



Lastly, consider whether the vendor offers any interface or platform, for either or both performing manual reviews and understanding model decisions or performance. The user interface can show extensive data, provide order link analysis tools and support other features to help risk management teams understand and improve model decision making, as well as help agents perform more effective and efficient manual reviews. Ask vendors what specific omni-channel data points are supported within their user interface for link analysis and performing order review. There is tremendous value in a review agent being able to select an order pickup name or phone number and see all orders using this pickup person, including the number of different payment cards, emails and other data points across these orders.

Conclusion

Three critical factors greatly influenced how well equipped an organization was to handle the changes and challenges brought on by the COVID-19 pandemic with respect to digital channel and omni-channel risk management:

- 1. Flexibility to adapt the risk management strategy, which was generally easier with Machine Learning model-based platforms compared to rules-based platforms**
- 2. Readiness to scale and level of operational efficiency at the onset of the pandemic**
- 3. Ability to cultivate and communicate signals across physical and digital environments, merging physical loss prevention practices with eCommerce risk management**

The lessons learned in 2020 will be valuable throughout 2021 and beyond as unified commerce and BOPIS has established itself as a convenience for consumers and necessity for multi-channel retailers to support. Some retailers made lemonade in 2020, expanding sales and implementing new procedures to support a successful omni-channel strategy. Others held on and grinded through the pandemic with increased operational strain and a diminished user experience.

Regardless of whether an organization thrived or just survived in 2020, their risk management strategy is never complete. Effective risk management strategies plan for obsolescence and always look to evolve. If unified commerce is important for an organization, then it must be incorporated in their risk management strategy. Finding solution partners that support omni-channel risk management will be an important factor influencing success with unified commerce.

About the Fraud Practice

Are you looking for answers or solutions, for eCommerce payments and fraud management? Give us a call for a free introductory consultation to see if we can help you. Even if we can't meet your needs we most likely know someone who can, and we are happy to provide you with contacts of reputable firms and individuals servicing the space.

David Montague,
Founder

The Fraud Practice is a privately held US corporation based in Palm Harbor, Florida. The Fraud Practice provides training, research, and consulting services on eCommerce payments, fraud prevention, and credit granting. Businesses throughout the world rely on The Fraud Practice to help them build and manage their fraud and risk prevention strategies.

For more information about The Fraud Practice's professional training and consulting services, please visit www.fraudpractice.com.

For additional information about The Fraud Practice's online training programs and to register in a course of Certification Track, please visit www.CNPtraining.com.

The Fraud Practice Inc.

www.fraudpractice.com

www.CNPtraining.com

Toll Free: 1.888.227.0402

Telephone: 1.941.244.5361

Email: Questions@fraudpractice.com



E-COMMERCE AND OMNI-CHANNEL FRAUD FOLLOWING THE DIGITAL ACCELERATION

White paper presented by The Fraud Practice Inc.

© 2021. The Fraud Practice, Inc. All Rights Reserved Subject to Terms of Use available at <http://fraudpractice.com/terms.html>. The Fraud Practice Inc. name and logo and all other names, logos, and slogans identifying The Fraud Practice's products and services are service marks of The Fraud Practice Inc. All other trademarks and service marks are the property of their respective owners.

Images Copyright © iStockphoto LP