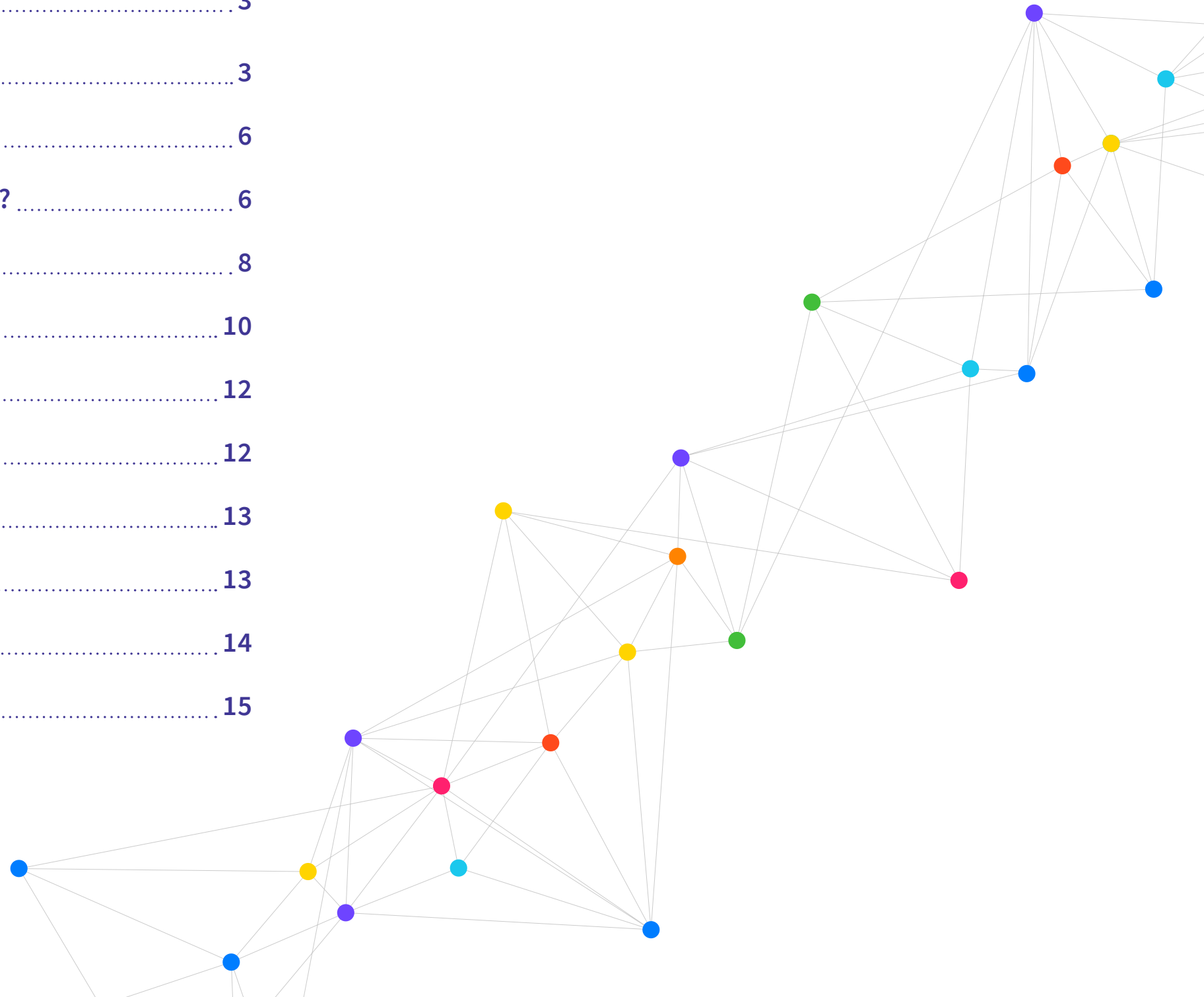


*Fighting Festive Fraud This Holiday Season*

*Reject Bad Actors, Identify Good Customers – In 2022 and Beyond*

# Table of Contents

Introduction .....	3
2021 Global Overview .....	3
Where Does Fraud Fit In? .....	6
How Does Fraud Affect Revenue and Profitability? .....	6
What Are The Latest Fraud Trends? .....	8
Fighting Festive Fraud – The 2021 Battle .....	10
Enter The Ring with Ekata .....	12
Ekata Identity Engine .....	12
Ekata Account Opening Solution .....	13
Ekata Pro Insight .....	13
Make Your Case – and Celebrate .....	14
Learn More .....	15



## Introduction

It's that time of year again - the holiday season. As retailers and consumers alike gear up, it is vital to remember: fraudsters don't vacation! Still, this is no time to fret. With the right strategies, actions, and technologies in place, you can make 2022 your most successful holiday season.

## 2021 Global Overview

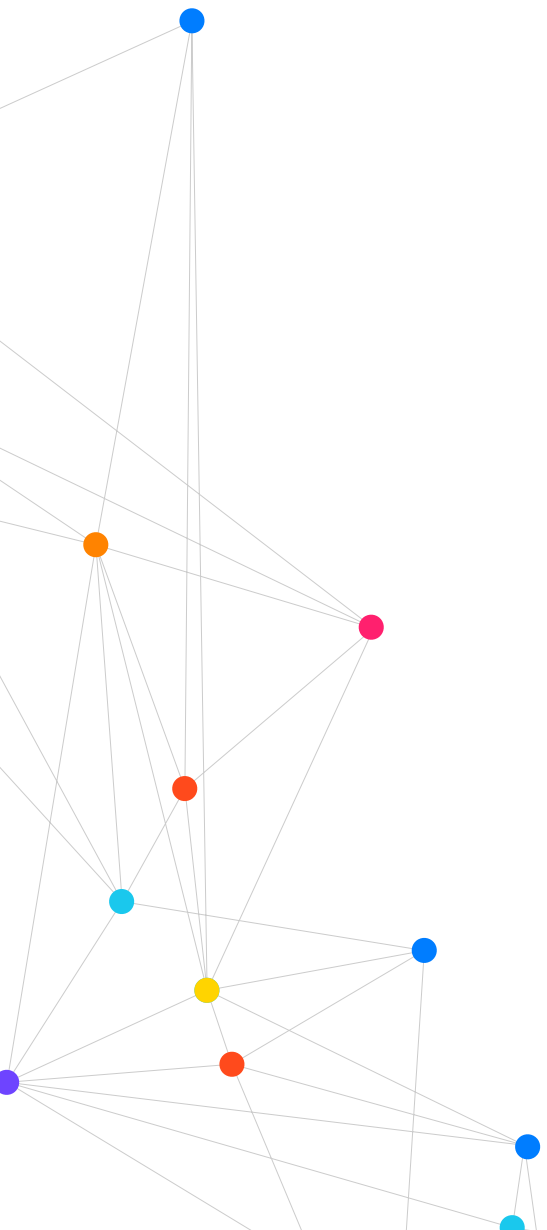
To prepare for the onslaught, let's take a quick overview of what we saw during 2021 and then best address the various ways merchants can refine their process for assessing consumer behavior and, in turn, fraud.

### Let's begin, shall we?

Interestingly, despite retail shopping returning to somewhat regular operations in 2021 - a year on from unprecedented global lockdowns - the holiday season shopping results last year were anything but normal. Indeed, the pandemic had not - and still hasn't - ended; with virus variants threatening surges at every turn. Moreover, inventory shortages caused by broken supply chains plagued the season. In fact, while [a survey conducted](#) late last year found that **45%** of American consumers had never before considered how their products were made and delivered pre-pandemic, it is now near-impossible to discuss retail without hearing about the supply chain. Subsequently, inflation heated up and labor has become increasingly hard to find globally, driving up wages.

Still, digital shopping accelerated further. According to recently released [Salesforce data](#), online holiday sales across November and December 2021 rose **5%** year over year worldwide to \$1.4 trillion and **9%** in the U.S. to \$257 billion.





**49%**  
of U.S. shoppers took  
advantage of early holiday  
promos and sales before  
Thanksgiving

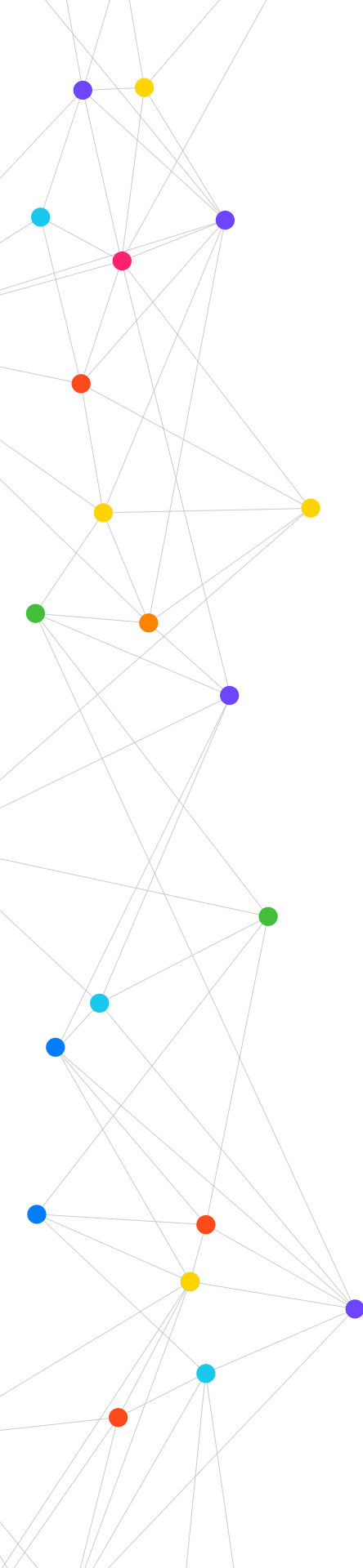
**63%**  
of Americans  
taking advantage of  
pre-Thanksgiving sales

**45–50%**  
of EU residents are more  
comfortable with online shopping

To account for the success of the season, it is important to note that the holiday shopping season has stretched. This appears to have happened globally. To combat product availability and inventory issues, savvy retailers began marketing early, urging consumers to order early, creating incentives. According to the National Retail Federation and Prosper Insights data, **49%** of U.S. shoppers took advantage of early holiday promos and sales before Thanksgiving. Meanwhile, Numerator data shows more dramatic early shopping trends still, reporting **63%** of Americans taking advantage of pre-Thanksgiving sales.

Therefore, with the dominance of Cyber-5 - the five days between Thanksgiving and Cyber Monday - now diminishing, is it any wonder that some [six out of 10 retailers \(59%\)](#) say they plan to start seasonal marketing before November this year?

Meanwhile, all across the European continent, shoppers are increasingly turning online for their holiday shopping. Indeed, Ekata's very own Director of Account Management EMEA, Anthony Mannino states that some **45-50%** of EU residents are more comfortable with online shopping, and **71%** of UK shoppers said prior to the 2021 holiday season that they planned to shop online.



Just like their American counterparts, [21% of people in the EMEA region](#) started their holiday shopping as early as June, with **49%** saying they confirm online that an item is in stock before purchasing - hello, supply chain chaos!

Across the APAC region, with differing holiday seasons, similar trends were forecast and came to light. In Australia, an island that [ranks 10th in ecommerce sales](#) worldwide, online shopping rates rose by **62.8%** from January 2020 to January 2021; and [71% of Australian consumers](#) purchased their Christmas gifts through third-party sellers on online marketplaces - crediting better prices, better product selection, and faster delivery due to more products locally available and in-stock. In Australia and New Zealand, Black Friday and Cyber Monday sales continue to grow, with online spending rising **22.8%** in 2021, [totalling over \\$8 billion in spend](#).

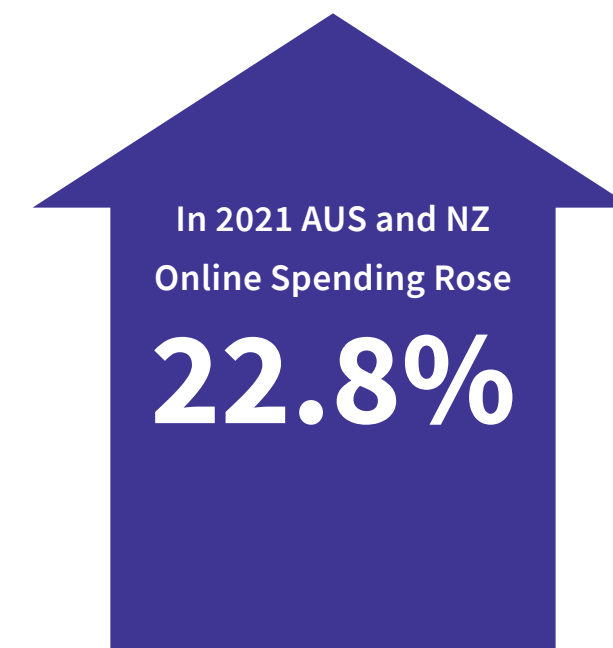
Concurrently, in Asia, November sales growth was modest at the beginning of the month, with sales starting to come through the Monday before Cyber Weekend, with Cyber Monday showing the strongest YoY growth **(+85%)** and sales peaking on Black Friday **(+31%)**. While interest remains high in Asia, [conversion rates are down \(by 26%\)](#) due to stock shortages and logistical challenges.

Importantly, Singles Day saw an **8%** growth across Asia, but China showed declines of **23%**, with average order value down **22%**. This reflects weaker demand and serious uncertainty brought on by the pandemic.

## PAY AND RECEIVE – AN EVOLUTION

2021 saw the continual evolution of consumers embracing new ways to pay and receive their goods, driven by the need to be adaptable and merchant modernization. The Buy Now Pay Later phenomenon shows no signs of slowing down; with [Salesforce data showing a 29% YoY growth](#) during Cyber Week, with [AfterPay reflecting similar data at 30% growth](#).

Finally, adoption of the Buy online, pick up in-store (BOPIS) movement continued into 2021. Also known as Curbside Pickup, this way of receiving goods was encouraged by retailers as a way to still shop during Covid surges, while reducing the shipping costs of ecommerce. Consumers took to the curb at an increase of **68%** from October to December 2021 compared to the same period in 2020.



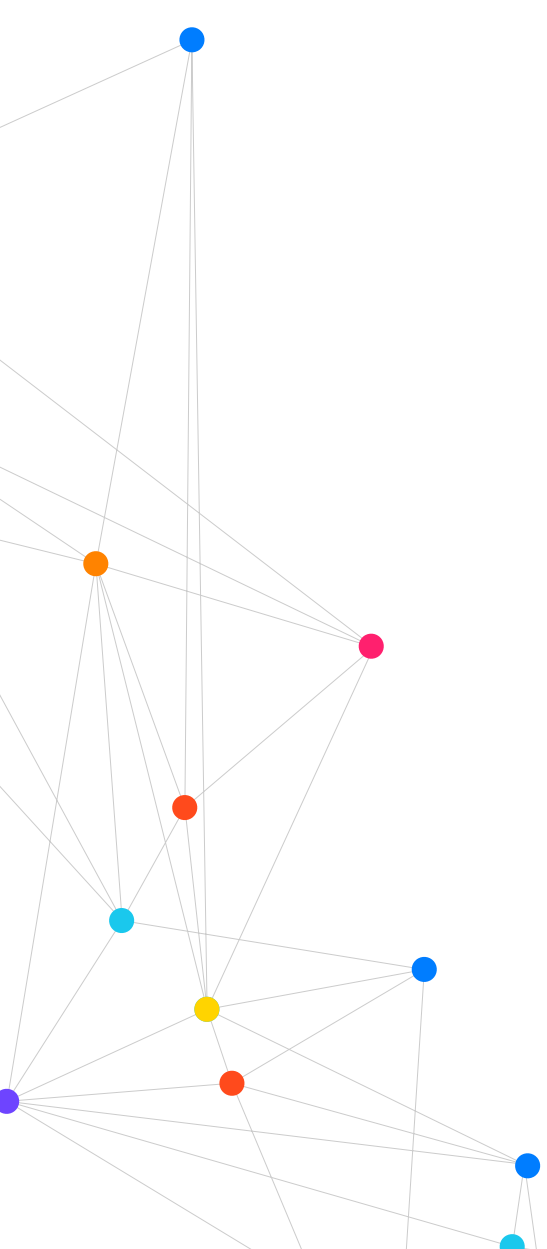
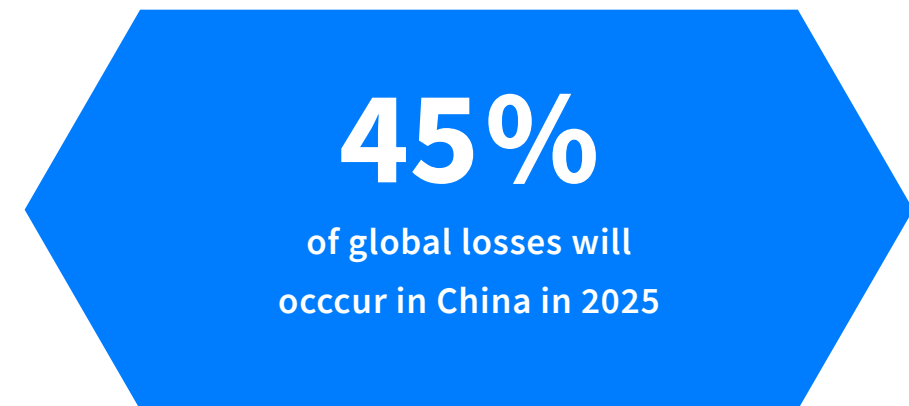
## Where Does Fraud Fit In?

Unfortunately, while consumers celebrated bargains and merchants raised a glass to record holiday sales, malicious fraudsters went to work. According to a TransUnion analysis published at the close of 2021, **17.46%** of all global ecommerce transactions between Thanksgiving and Cyber Monday were potentially fraudulent, those numbers higher still in the U.S., sitting pretty at **19.66%**.

Worse still, the number of suspected ecommerce fraud attempts made during last year's holiday shopping season was also a **25%** increase over attempts observed earlier in the year. Globally, the percentage of fraudulent transactions rose **4%** from November 25-November 29.

## How Does Fraud Affect Revenue and Profitability?

The impact of fraud on retailer profitability is huge. In fact, commerce losses to online payment fraud were estimated at 20 billion U.S. dollars globally in 2021; a growth of over **14%** compared to the 17.5 billion dollars recorded in the previous year. More of this online fraud will occur in China than anywhere else. According to Juniper Research, China will account for over **40%** of global losses in 2025, estimated to be over \$12 billion.





Meanwhile, according to LexisNexis® Risk Solutions, every \$1 of fraud now costs U.S. retail and ecommerce merchants \$3.60, which is **15%** higher than the pre-Covid study in 2019 which was at \$3.13. This also represents a **7.1%** rise since the 2020 survey which was conducted during the pandemic.

The obvious damage due to fraud is financial loss. Losses that include the cost of fraudulently ordered items along with the associated processing and shipping costs. The retailer is harmed financially when criminals use stolen credit cards and when consumers purchase online, then request the credit card provider to issue a chargeback after the items have been shipped. What's more, fulfilling fraudulent orders renders that inventory unavailable to legitimate customers, resulting in lost revenue.

Fraud is also costly in other ways. Fraudulent transactions add to already higher order volumes, possibly slowing down order processing and delaying shipments. Additionally, shipments to fraudsters further clog the delivery system.

The result? Customer frustration and dissatisfaction that results not only in lost customers but also in an increased load on customer service agents who are trying to make things right.

# What Are The Latest Fraud Trends?

Ecommerce fraud isn't just growing. It's evolving. Indeed, fraudsters are becoming more and more sophisticated. Their increasingly complex and crafty schemes make their illegitimate activities hard to distinguish from legitimate ones. Like legitimate businesses, some fraudsters invest their "profits" in leading-edge fraud technologies, including artificial intelligence, machine learning, automation, and bots.

Here are just three of the latest fraud trends to keep an eye out for...

## 1. PROMO ABUSE

Promotion fraud (AKA promo abuse) involves the fraudulent exploitation of promotional program incentives. **Here's an example:** *A single customer redeems a promotional coupon — let's say for 50% off — multiple times even though it was intended to be used only once per customer.*

Promotional campaign types that are most subject to fraud include signup incentives, referral bonuses, and loyalty discounts. These are often used by retailers, subscription-model businesses, and quick-service restaurants.

Merchants often underestimate the threat of promo abuse, but it can become an expensive issue and could very quickly damage your brand reputation.

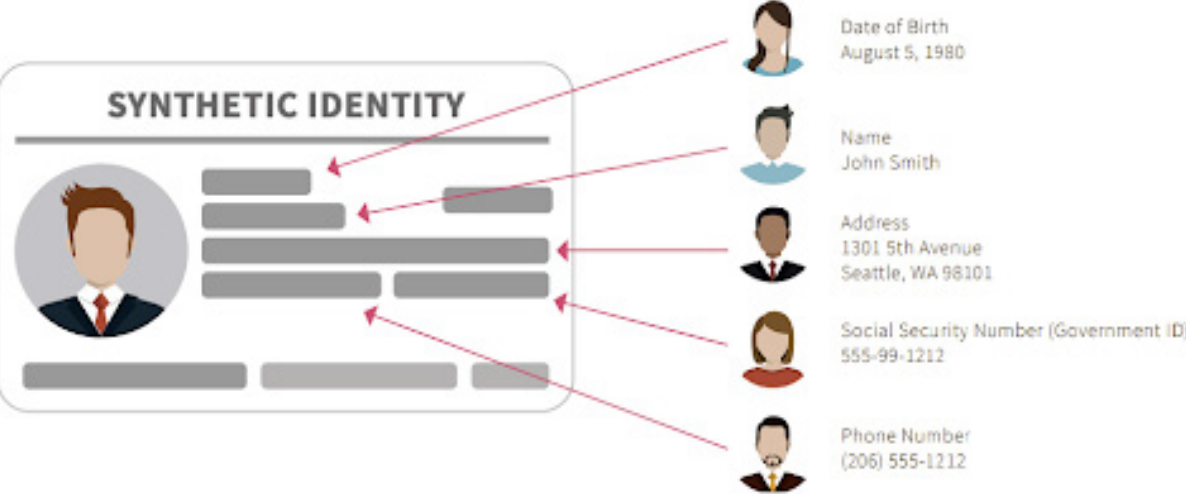
Read more about this type of fraud in our [Promo Abuse eBook](#).

## 2. SYNTHETIC ID THEFT

Growing more sophisticated by the day, synthetic identity theft is a crime perpetrated by bad actors who use real and fake personal information to craft an authentic-looking digital identity. Data breaches are not unique to the US — companies around the world face similar challenges. And, personal information exposed from data breaches often winds up for sale on dark web marketplaces, which is where fraudsters can buy the data they need to commit synthetic identity theft.

One of the common uses of synthetic identities is to commit account opening fraud. It is how fraudsters gain access to a slew of exploitable opportunities. In the world of ecommerce, this involves creating online accounts for fraudulent transactions.

Read more about this type of fraud in our [Synthetic Identity Theft eBook](#).



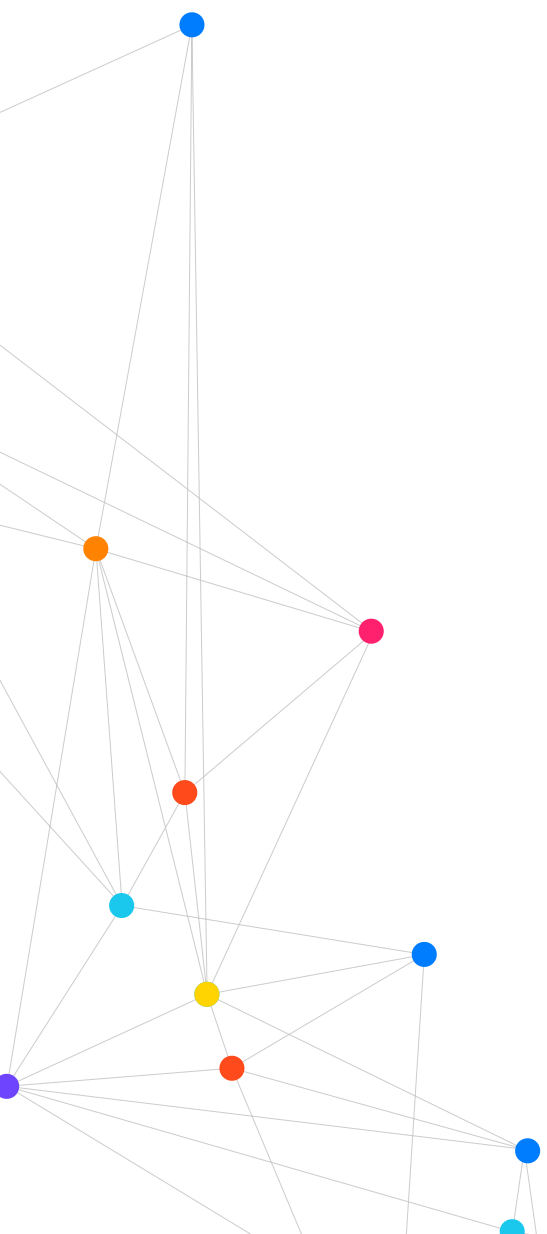


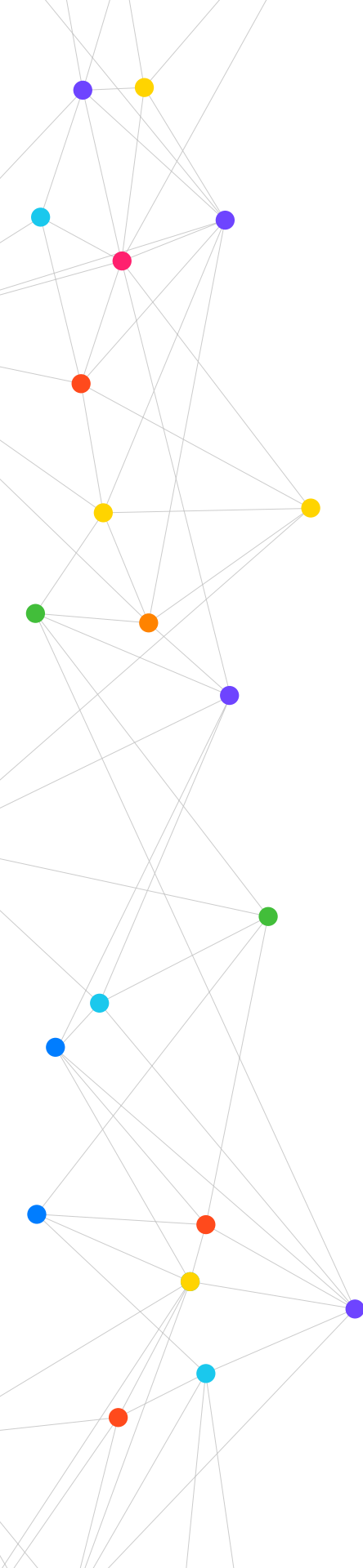
### 3. BOPIS FRAUD

Let's face it. When curbside was a small fraction of sales, retailers could generally manage the process easily. However, that all changed with the pandemic.

The crash of BOPIS orders has made traditional manual review cycles and billing/shipping address matching nearly impossible. And, curbside orders don't come with a delivery address, which is usually a key signal in fraud protection. It is therefore easy for a fraudster with a stolen credit card to supply a legitimate billing address at curbside and avoid suspicion all together. Meanwhile, orders need to be filled fast, which leaves little to no time for manual review or to consider the legitimacy of the order. The result? Fraudsters get away, fast – from the curb, and from suspicion.

Unless retailers adopt effective fraud prevention strategies and implement appropriate processes and technologies, and quickly, fraudsters will continue to get away with it. For retailers, this is especially true during seasonal peaks such as Black Friday, Christmas, Lunar New Year, and Singles' Day.





# Fighting Festive Fraud – The 2021 Battle

Last year, traditional approaches for distinguishing between good customers and fraudsters were inadequate to contend with the skills and cleverness of criminal organizations. The identity verification approaches that retailers used in 2021 fall into two categories based on retailer size.

## LARGER MERCHANTS

Some larger merchants leveraged fraud prevention platforms, many of which don't have access to sufficient data sources to reliably identify good customers. Since larger merchants also have higher transaction volumes, this problem is multiplied. For many transactions, the lack of customer data may result in secondary friction, manual review, or both.

In addition, these platforms frequently created false positives, thereby denying transactions to good customers. The false positive declines went undetected because customer validation processes weren't robust enough to recognize good customers and fast-track their orders. What's more, the sheer volume of transactions exceeded the capacity of some platforms' capabilities, delaying processing time and sometimes even crashing.

Without the ability to continually challenge primary and secondary details at any point in the workflow, platforms sometimes allowed customer account takeover (ATO) by fraudsters. The fraudsters would then manipulate the customer account for their gain and the retailer's loss. According to a report by LexisNexis Risk solutions, automated bots are one of the factors contributing to the rise in ATO activity.

## SMALLER MERCHANTS

Smaller merchants often found fraud platforms unaffordable. Instead, they relied on manual review for customer identity verification and transaction processing. According to a [2022 Ravelin study](#), over two-thirds of merchants spend 20-60% of their time on manual review. Review teams quickly became overloaded during the holidays, resulting in lengthy review times. This drove up abandonment by new customers and frustrated return customers who wondered why they were encountering this level of scrutiny.

*“Over two-thirds of merchants spend 20-60% of their time on manual review.”*

– RAVELIN, ONLINE MERCHANT FRAUD & PAYMENTS SURVEY 2022

## IN GENERAL

Fraudsters kept ahead of the merchants by evolving new methods for not only establishing seemingly legitimate accounts, but also returning to the accounts to increase the value of their transactions.

Some merchants developed in-house fraud management systems using their own collected data, but those typically came up short because they didn't provide the robust data required to develop the accurate risk scores necessary for making informed risk decisions.

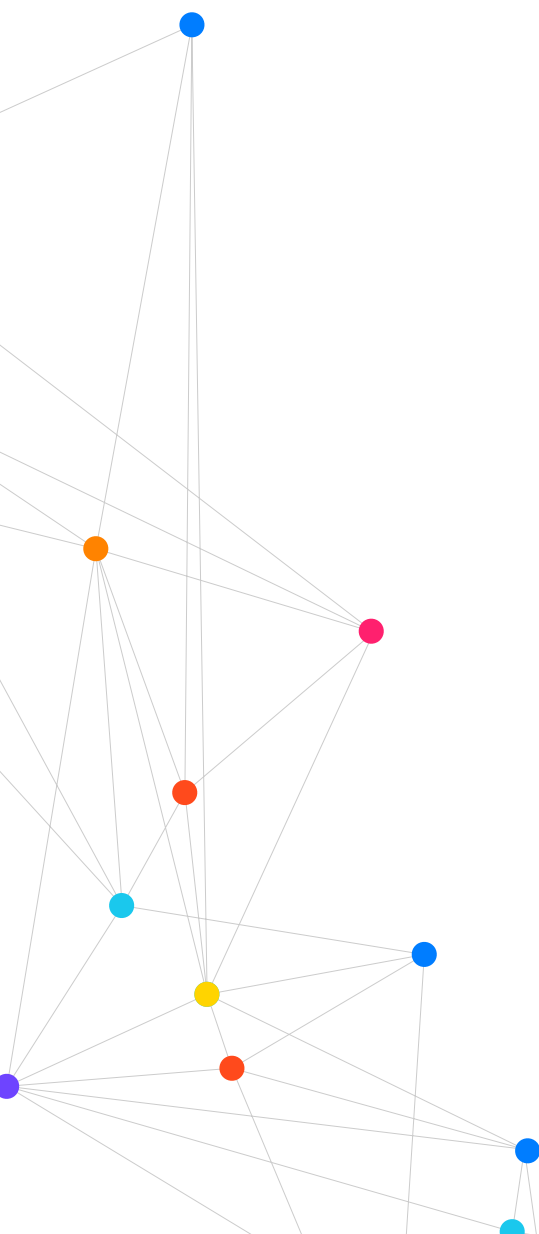
## Coming Out On Top In 2022

To address the dynamic 2022 market and its anticipated holiday surge, you need a fraud management strategy and supporting technology to address the shortcomings of the approaches used in 2021. That combination must enable you to:

- Immediately and accurately identify good customers
- Reject fraudsters
- Subject only questionable customers to in-depth reviews

The best approach is a layered one that employs a customizable, automated customer identification validation solution that bases analysis on a robust foundation of customer identification data gathered from authoritative sources. Before any transaction is authorized, your validation process must reliably assess the legitimacy of the user attempting to make the transaction. Based on this assessment, the process then advances the user through the appropriate validation workflow.

This approach lets you identify good customers upfront, routing them through fast approval of the current transaction and subsequent ones. The approach also immediately identifies fraud and rejects the transaction before it's executed. If warranted, the workflow routes the user through additional assessment that may involve manual review. A good customer identification validation solution should support the review team with actionable risk assessment information.



# Enter The Ring With Ekata

The **Ekata Identity Engine** is a customer identity verification solution that meets retailers' requirements for quickly distinguishing between good customers and fraudsters. The engine includes two datasets.

## IDENTITY GRAPH

- Validates identity element relationships
- Includes data from 100+ authoritative data sources
- Contains 8+ billion elements with 100+ billion unique identities

## IDENTITY NETWORK

- Includes 1st-party data gathered by 400+ million monthly anonymous customer queries
- Includes international data from 238 countries and territories
- Unmatched by other probabilistic assessment solutions

The **Ekata Identity Engine** applies sophisticated data science and machine learning to generate a probabilistic assessment of the validity of the identity information. The methodology analyzes linkages and activity patterns, such as how long a customer's identity elements have been in use and how they have been used in combination. The analysis derives signals that indicate:

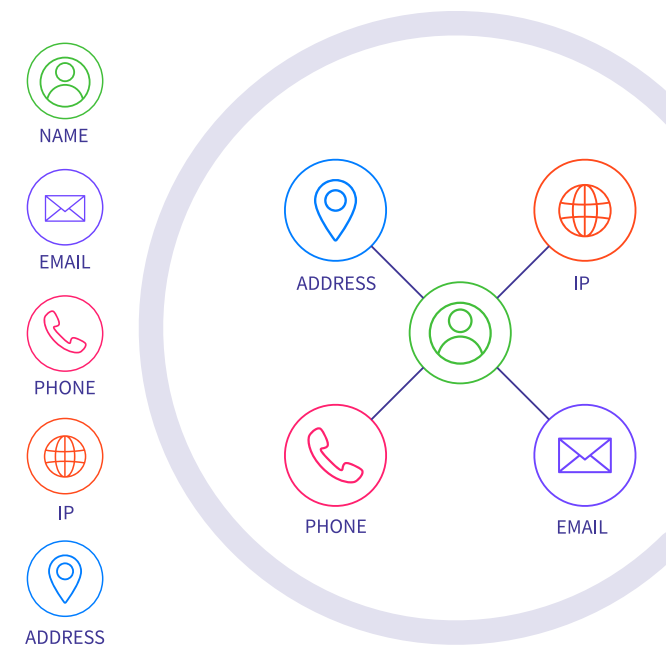
- Whether or not the identity elements supplied are consistent with a real person conducting a transaction
- That the consumer is who he or she claims to be

The engine also calculates an overall risk score based on the signals. The analysis happens quickly so as not to add friction to the business operations or to the customer experience.

## THE EKATA IDENTITY ENGINE

### Identity Graph

Licensed, authoritative sourced data points



**7B+**

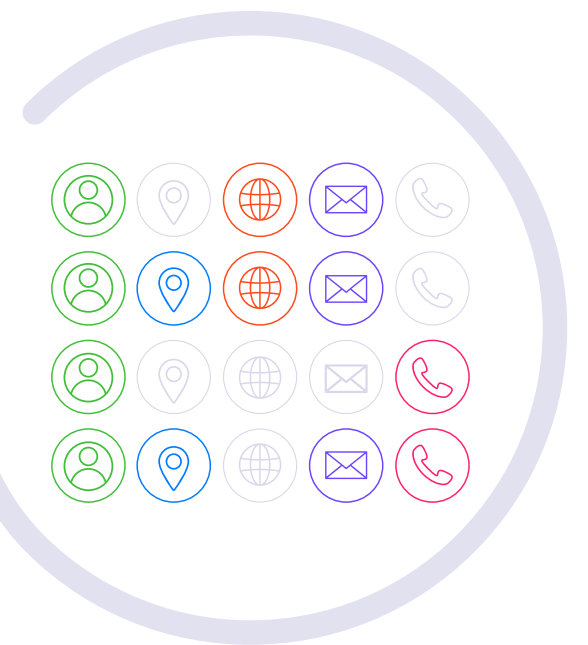
Identity Elements

**2B+**

Identities Worldwide

### Identity Network

Global, behavioral, pattern-based



**5B+**

Digital Interactions

**50M+**

Identity Elements Added per Day

## EKATA ACCOUNT OPENING SOLUTIONS

Merchants benefit from assessing fraud risk before their customer even gets to the checkout stage. This is where the Account Opening solutions come in; a tool that enables the quick and confident sorting of customers into low-risk and high-risk buckets, allowing you to tailor their experience accordingly (adding friction only when appropriate). This process not only keeps sign-up flows simple, it can help stop promo fraud in its tracks; ensuring all incentives on offer are only provided to the people who will grow your business.

## EKATA PRO INSIGHT

This software-as-a-service manual review tool empowers fraud managers to quickly approve or deny transactions quickly and confidently. Its visual dashboard displays a top-line score along with metadata flags that explain the top data indicators that contributed to the score. An interactive map enables reviewers to view distances between inputs such as IP and shipping and/or billing addresses.

Reviewers also have access to detailed reports on usage, users, and coverage. As a result, reviewers have the data and critical insights to accurately determine the risk level of any transaction.





## MAKE YOUR CASE – AND CELEBRATE!

Getting senior management to buy-in to your company’s need for a robust risk management solution is as simple as showing them the data; as ecommerce sales surge, especially during the holiday season, so too does fraud. Traditional customer identity verification solutions do not adequately protect against fraud. Nor do they scale to support the unprecedented increases in online sales volumes.

The key to success in this dynamic market is implementing processes and technologies that streamline transaction authorization for good customers, while denying transactions for bad actors.

Ekata’s global identity verification data is the answer. It gives you access to robust global data that makes smart decision-making possible at every point in a transaction authorization process – even at the busiest times of the year. The results speak for themselves.

## EKATA SUCCESSES

- A global fashion merchant slashed fraud by **50%** and saved \$360,000/month with the Ekata Identity Engine.
- A Global Buy-Now-Pay Later provider increased automatic approvals by **60%**
- A Global Payment Service Provider in China increased approvals by **18.6%** and reduced chargebacks by **17.3%** using Ekata.

**Contact Ekata today** to learn how we can help you clear good customers faster and stop fraudsters in their tracks—during the holiday season and beyond. The result: higher revenue and profitability throughout the entire year.

## ABOUT EKATA

Ekata provides global identity verification solutions via enterprise-grade APIs for automated decisioning, and Pro Insight, a SaaS solution for manual review for cross-border businesses to grow revenue by maximizing their predictability of good transactions. Our product suite is powered by the Ekata Identity Engine (EIE), the first and only cross-border identity verification engine of its kind. It uses complex machine learning algorithms across the five core consumer attributes of email, phone, name (person or business), physical address, and IP, to derive unique data links and features from billions of real-time transactions within our proprietary network and the data we license from a broad spectrum of global providers. Businesses around the world including checkout.com, Microsoft, Klarna, and Airbnb leverage our product suite to increase approvals of more good transactions, reduce customer friction at account opening, and find fraud.

**Contact us to learn more**  
**[ekata.com](https://ekata.com)**

