



# The 2023 holiday season fraud prevention eBook

**REJECT BAD ACTORS, IDENTIFY GOOD  
CUSTOMERS – IN 2023 AND BEYOND**



# Table of contents

<b>01</b>	Introduction	<b>07</b>	Coming out on top in 2023
<b>02</b>	2022 global overview	<b>08</b>	Enter the ring with Ekata <ul style="list-style-type: none"><li>• Ekata Identity Engine</li><li>• Ekata Account Opening Solution</li><li>• Ekata Pro Insight</li></ul>
<b>03</b>	Where does fraud fit in?	<b>09</b>	Success with Ekata
<b>04</b>	How does fraud affect revenue and profitability?		
<b>05</b>	What are the latest fraud trends?		
<b>06</b>	Fighting festive fraud – the 2022 battle		

# 1. Introduction

The holiday season is approaching fast, especially for merchants looking to get ahead of the holiday rush. Thankfully, there's still time to prepare.

During the holidays, while consumers are busy filling their online shopping carts, fraudsters are getting to work. Yet, to stop this fraud from damaging customer satisfaction or your bottom line, retailers must ready their fraud infrastructures starting now.

With the right strategies, actions, and layered technologies, you can keep bad actors out, let more good customers in and make 2023 your most successful holiday season to date.



## 2. 2022 global overview

To prepare for the onslaught, let's take a quick overview of what we saw during 2022 and address the best ways merchants can refine their process for assessing consumer behavior and, in turn, fraud.

### Let's begin, shall we?

It's official. The head of the World Health Organization (WHO) has declared an end to the global health emergency COVID-19. And yet, we are hesitant to run to the streets to celebrate. Indeed, our global economy is still under immense pressure, between inflation and the war in Ukraine, not to mention supply chains still disrupted around the globe due to the pandemic.

Still, it's vital we celebrate the wins. And a true win is this: In the United States in 2022, holiday season retail sales grew by 4.8% YoY, following two years of surging retail and ecommerce growth. Better still, a similar gain of 4.5% is expected this year.

Unfortunately, globally, online sales were flat, reaching \$1.14 trillion. According to Salesforce, global sales were reduced by weak performances across Europe, where economic turmoil contributed to an 8% decline in growth. Meanwhile, in Australia and New Zealand, amid a "digital rebalancing," sales fell 7%.

Furthermore, Latin America ecommerce sales grew by 24.7% in 2022, but sales growth is expected to drop 13.4% in 2023 due to the economic uncertainty in the region.

**\$1.14 trillion**

Global online sales were flat at \$1.14 trillion

**+4.8%**

U.S. holiday season retail sales grew by 4.8% YoY

### Increased pricing over increased demand

One global finding is that all online sales growth over the holiday period was driven by an increase in prices rather than an increase in actual shopper demand. In fact, worldwide, prices were up 5.3% from 2021, thanks to inflation.

### Big drive for big discounts

Despite the above increase in prices across the board, big discounts hit record highs across multiple ecommerce categories, peaking at 34% off listed price versus 19% in 2021. Furthermore, Salesforce data shows the average discount for the three weeks after 2022 Cyber Week was higher than the previous year, when high demand reigned and inventory scarcity haunted retailers. In fact, merchants' discounts in this study peaked during Cyber Week at 27% globally and 30% in the U.S.



Naturally, these discounts reaped multiple benefits; drawing in price-savvy (and cautious) consumers who sought holiday bargains, while providing an answer to retailers challenged with oversupply issues, particularly in categories such as electronics, apparel and toys.

### Online shopping surges (via mobile and social media)

Interestingly, according to Mastercard Spending Pulse, U.S. shoppers returned to in-store shopping in 2022, with sales growing by 6.8% over 2021. Still, ecommerce was the name of the game, increasing by 10.6% and comprising 21.6% of total retail sales for the entire holiday season.

According to Adobe, 47% of online sales were transacted via smartphones during the 2022 holiday season, up 4% from 2021. Furthermore, spending on Christmas Day set a new mobile record, comprising 61% of online sales — up a whopping 58% from the year before. Similarly, during Cyber Week, 51% of sales came through smartphones, which is 5% more than the same period in 2021. And, according to the Annual ACI Holiday Spending Report, 36% of Black Friday ecommerce traffic came via mobile devices. Still, desktop shopping had a better conversion rate than mobile and desktop purchases had more items per order. Meanwhile, in Europe, traffic referrals hit an all-time high

over the holiday season, which drove 12% of all mobile traffic, up 23% from 2021. Specifically, Belgium and Italy are home to the most social media-minded shoppers (outside of the U.S).



In fact, similar to trends seen in 2021, much of the European continent moved online over the holiday season. As Ekata's very own Director of Partner Management EMEA, Anthony Mannino, stated last year, some 45-50% of E.U. residents are more comfortable with online shopping and 71% of U.K. shoppers said prior to the 2021 holiday season that they planned to shop online. [More recent stats show](#) that ecommerce in the E.U. was boosted by demand from shoppers aged 25-34 years of age, with 87% of individuals in this age group buying goods and ordering services online throughout 2022. Specifically, [the highest share of online shoppers lives](#) in the Netherlands (92%), followed by Denmark (90%) and Ireland (89%).

Meanwhile, across the Asia Pacific (APAC) region, thanks to increasing access to smartphones and growing internet penetration, ecommerce witnessed robust growth in 2022 and is forecast to continue growing. In fact, the ecommerce market is expected to grow by 7.46% this year, reaching US\$3,758.4 billion and US\$4,815.5 billion in 2027.

**87%**

Of EU shoppers aged 25-34 bought goods and services online throughout 2022.

**6.4 million**

Internet users in Australia will purchase a product through social media in 2024.

**34%**

Of surveyed Latin Americans use their mobile devices for holiday shopping.

As for social commerce in the region, it is expected in [2024](#) that [a total of 6.4 million internet users](#) in Australia will purchase a product through social media. Meanwhile, social commerce is expected to grow three times faster than traditional ecommerce in South East Asia, [generating \\$1.2 trillion by 2025](#).

The Latin America region is no exception to this trend with the social commerce industry projected to reach US\$8347.9 million by the end of this year. Additionally, according to Meta, 34% of surveyed Latin Americans, and in particular, 43% of shoppers in Brazil, said they use their mobile devices for holiday shopping because it was more convenient than going to a store.

### BNPL and BOPIS boom

2022 saw the continual evolution of consumers embracing the new ways to pay and receive their goods, driven by the need to be adaptable during a pandemic and merchant modernization. The Buy Now Pay Later (BNPL) phenomenon shows no signs of slowing down; with Adobe data showing a 68% rise during the week of Black Friday compared to the previous week. Furthermore, ACI Worldwide data shows BNPL transaction values increased by 87% during Black Friday compared to 2021.

Interestingly, an embrace of the Buy Online, Pick Up In-Store (BOPIS) movement continued into 2022 despite lockdowns being truly over. More consumers opted for Click and Collect, saving on delivery costs, with transaction volumes increasing 25% in Q4 of 2022 versus 2021.

68%



a 68% rise during the week of Black Friday on delivery costs, with transaction volumes increasing 25% in Q4 of 2022 versus 2021.

87%



BNPL transaction values increased by 87% during Black Friday compared to 2021



### 3. Where does fraud fit in?

Unfortunately, while consumers celebrated bargains and merchants raised a glass to holiday sales, malicious fraudsters went to work. According to a TransUnion analysis published at the close of 2022, the average number of suspected digital fraud attempts during Thanksgiving and Cyber Monday (Thursday, Nov. 24 and Monday, Nov. 28) was 82% higher globally than during the rest of 2022 and a whopping 127% greater than during the rest of the year for transactions outside of the U.S.

In fact, according to TransUnion's Consumer Holiday Shopping Survey, conducted in August 2022, some 54% of American consumers were recorded as concerned with being victimized by online fraudsters over the holiday period – an increase of 17% from the previous year.



## 4. How does fraud affect revenue and profitability?

The impact of fraud on retailer profitability is huge. In fact, during the 2022 holiday season alone, merchants turned away a shocking US\$24 billion in good transactions out of fear of fraud. Specific losses related to actual fraud are even greater, with merchants expected to lose up to US\$ 206 billion on fraud between 2021 and 2025. The leading cause of online payment fraud was physical good purchases, which accounted for 47% of all fraud losses last year.

**\$24 trillion**

how much merchants turned away in good transactions out of fear of fraud during the 2022 holiday season alone.

**\$206 billion**

The amount merchants are expected to lose due to fraud between 2021 and 2025.

Meanwhile, according to LexisNexis, every \$1 of fraud now costs U.S. retail and ecommerce merchants \$3.75, which is 19.8% higher than the pre-Covid study in 2019 which was at \$3.13. This also represents a 11.6% rise since the 2020 survey conducted during the pandemic.

The obvious damage due to fraud is economic loss. Losses include the cost of fraudulently ordered items and the associated processing and shipping costs. The retailer is harmed financially when criminals use stolen credit cards or 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, slowing down order processing and delaying shipments. Additionally, shipments to fraudsters further clog the delivery system.

The result? Customer frustration and dissatisfaction leads to not only customer loss but also increases the workload of customer service agents who are trying to make things right.



## 5. What are the latest fraud trends?

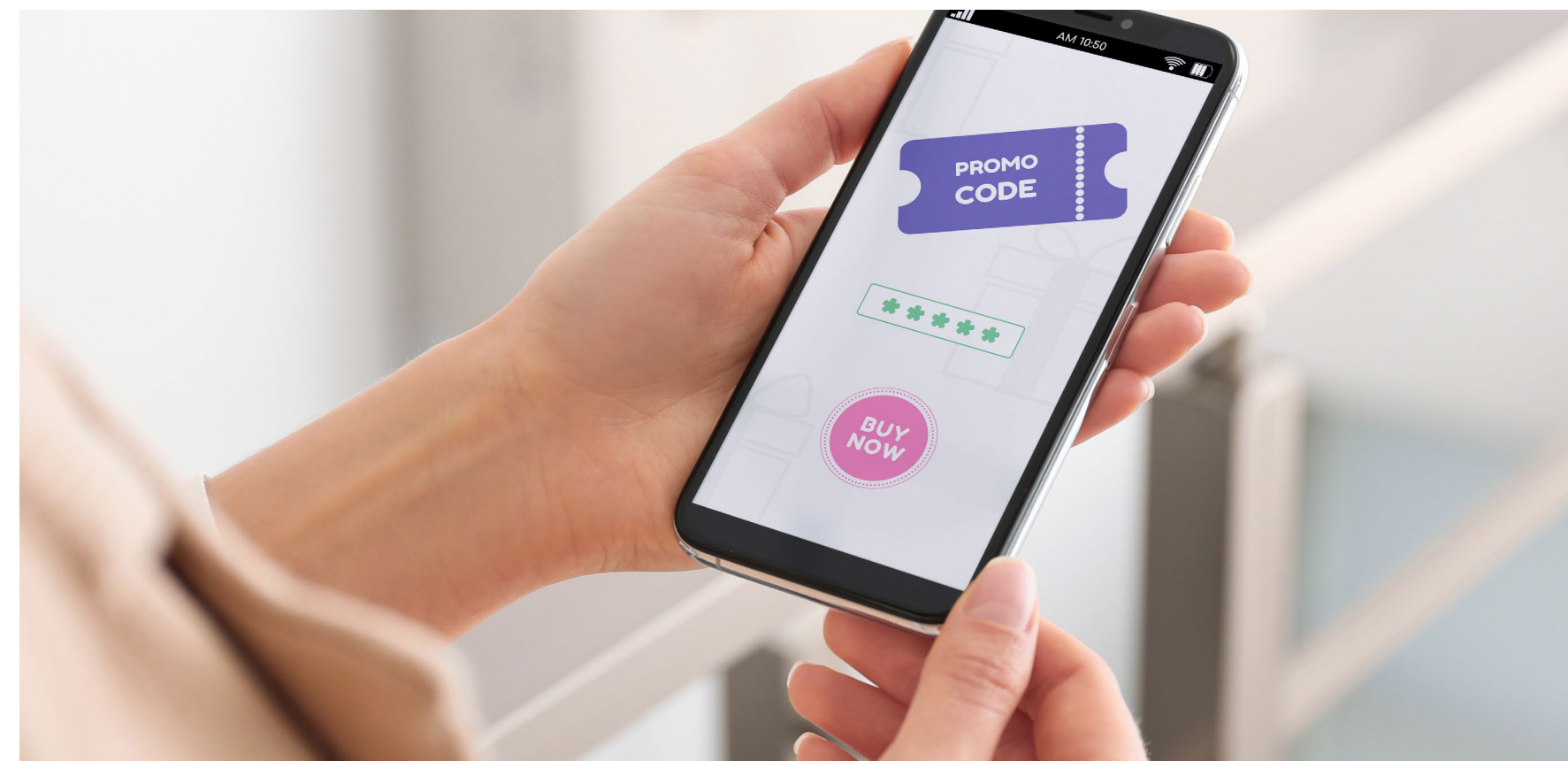
Ecommerce fraud isn't just growing – it's evolving. Indeed, fraudsters are becoming increasingly sophisticated. Their complex and crafty schemes make their illegitimate activities hard to distinguish from legitimate ones. Like legitimate businesses, some fraudsters invest their "profits" in leading-edge 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.

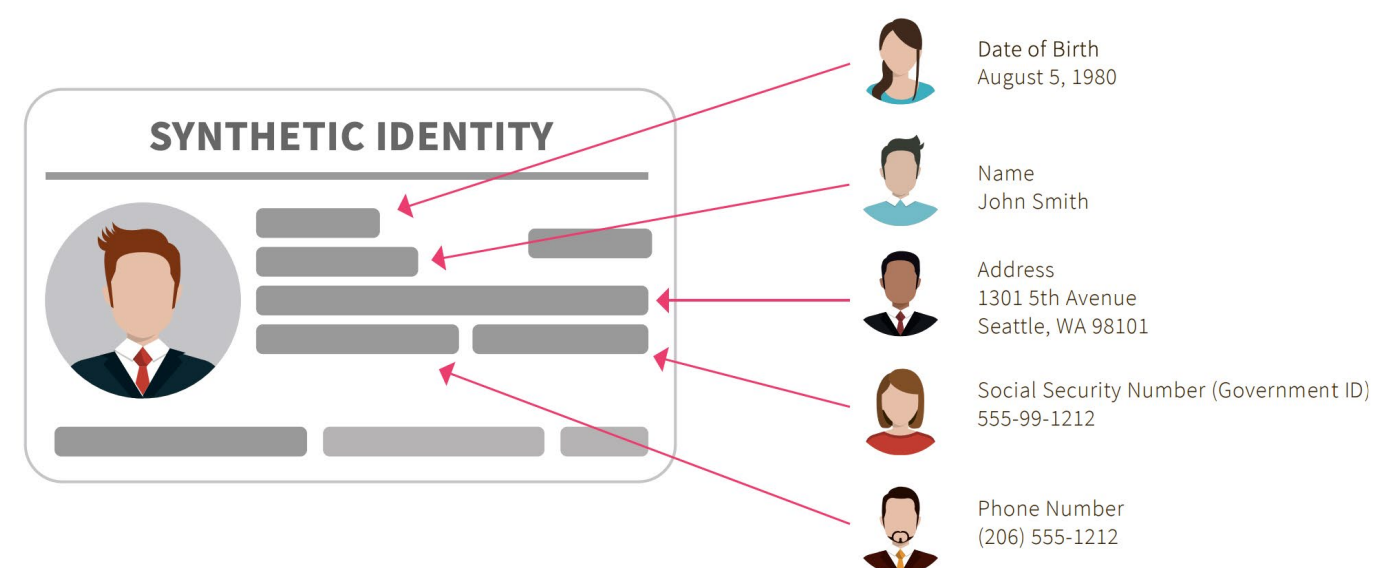


Merchants often underestimate the threat of promo abuse, but it can become an expensive issue and could very quickly damage your brand reputation.

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 U.S. — companies around the world face similar challenges. And personal information exposed from data breaches often winds up for sale on dark web marketplaces, 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 manage the process easily. However, that has all changed since the pandemic.

The crash of BOPIS orders has made traditional manual review cycles and billing/shipping address matching near 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 out 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 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.



## 6. Fighting festive fraud – the 2022 battle

Last year, traditional approaches for distinguishing between good customers and fraudsters were inadequate to contend with the skills and cleverness of criminal organizations.

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.

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.

# 7. Coming out on top in 2023

To address the dynamic 2023 market and its anticipated holiday surge, you need a fraud management strategy and supporting technology to address the shortcomings of your 2022 approach. That combination must allow 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 identity 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 identity validation solution should support the review team with actionable risk assessment information.





## 8. Enter the ring with Ekata, a Mastercard company

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 7+ billion elements with 2+ billion unique identities

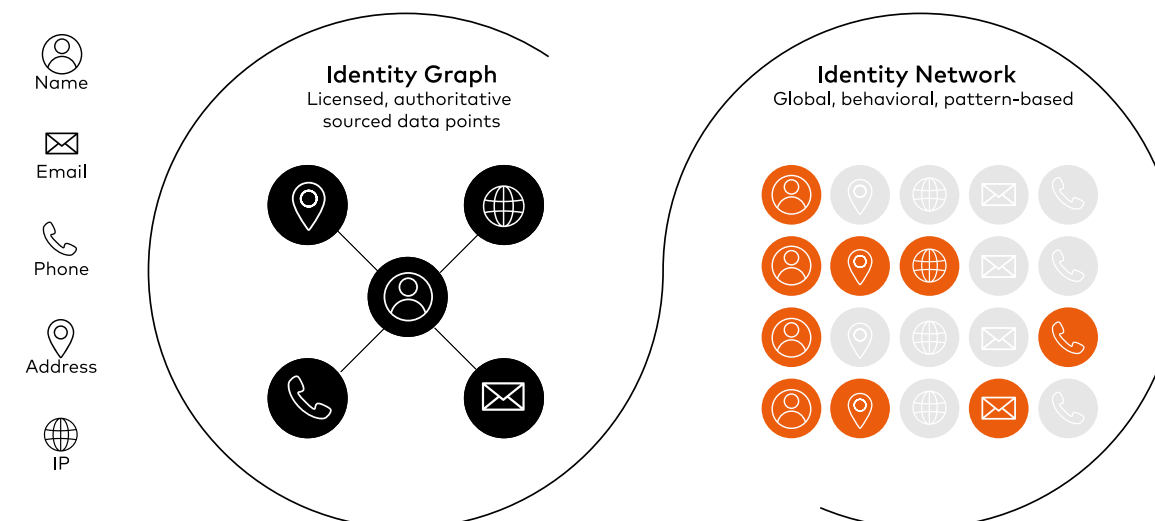
### Identity network

- 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 they claim to be

### Ekata Identity Engine



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.

### **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, but it can also 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 results page displays a top-line identity risk and network risk score along with metadata flags that explain the top data indicators contributing to the score. Network Pair Signals provide insight into how certain identity attributes (name, phone, email, addresses, and IP) have interacted with each other over time, with pattern categorizations including how frequently an attribute is paired with an unrelated data point and how many transactions the attribute has been in recently. 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.

## 9. 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 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.

### Success with Ekata, a Mastercard company

**-50%**

A global fashion merchant slashed fraud by 50% and saved \$360,000/month with the Ekata Identity Engine.

**+60%**

A Global Buy-Now-Pay Later provider increased automatic approvals by 60%.

**+18.6%**

A Global Payment Service Provider in China increased approvals by 18.6% and reduced chargebacks by 17.3%.

Contact us 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 Inc., a Mastercard company, empowers businesses to enable frictionless experiences and combat fraud worldwide. Our identity verification solutions are powered by the Ekata Identity Engine, which combines sophisticated data science and machine learning to help businesses make quick and accurate risk decisions about their customers. Using Ekata's solutions, businesses can validate customers' identities and assess risk seamlessly and securely while preserving privacy. Our solutions empower more than 2,000 businesses and partners to combat cyber fraud and enable an inclusive, frictionless experience for customers in over 230 countries and territories.

**Contact us to learn more.**

**[www.ekata.com](http://www.ekata.com)**

©2023 Mastercard. Proprietary and Confidential

ekata

