GROW CROSS-BORDER E-COMMERCE AND MITIGATE FRAUD

5 Key Challenges Retailers Can Overcome with Global Identity Verification Data
# Table of Contents

Introduction ........................................................................................................................................... 3

**Challenge #1:** Consumer Identity Data Varies by Region ......................................................... 4

**Challenge #2:** Fraud Tactics Constantly Evolve and Get More Sophisticated Over Time .................. 5

**Challenge #3:** Fraud Risk Varies by Region .................................................................................... 7

**Challenge #4:** Overly Conservative Risk Policy Hinders Revenue ..................................................... 8

**Challenge #5:** Multiple Identity Data Elements are Required to Make Good Decisions (And what tools do I need?) ........................................................................................................... 9

**Solution:** Using a Multi-layered Approach to Approve More Cross-border Transactions and Still Avoid Fraud ............................................................................................................................ 10

**Summary** ........................................................................................................................................... 12
Introduction

The worldwide e-commerce market is projected to **reach $4 trillion in 2020**. Although domestic and cross-border digital fraud rates have **slowly declined** for North American companies since 2012, these transactions are still riskier than domestic ones and rejections of legitimate online orders—often called false positives—have risen. One reason this metric is increasing is due to companies expanding their reach across borders, making it difficult to distinguish between fraudulent and genuine customers in new markets. In fact, **44% of retailers** claim to use different fraud strategies when expanding internationally because they recognize the need for local knowledge and regionalized best practices.

According to Javelin Strategy and Research, LLC, retailers with $1 million or more in annual sales spend **$14.6 million annually in fraud and fraud prevention**. A whopping 19% of the $14.6 million comes from “good orders” mistakenly rejected. Understanding how to address the challenges of international commerce while clearing legitimate transactions with less friction is therefore essential to successful cross-border commerce.

Did You Know?
The fraud rate for international orders is still **1.5 times higher** than for domestic.

Accurately verifying a user’s identity during an e-commerce transaction is vital to preserving real customer relationships, driving more revenue and eliminating fraud. The **2016 LexisNexis True Cost of Fraud Study** (p. 11) definitively shows that those retailers conducting business cross-border experience more fraud than those simply focused on the US.

In this eBook, we’ll cover the fraud prevention challenges organizations face when selling across borders.
Consumer Identity Data Varies by Region

Unfortunately, there is not yet a global standard for customer identity verification. Country-by-country variations in the availability, format, and reliability of individual identity data makes it hard for companies to adopt a consistent, comprehensive approach to verifying a customer’s identity. Email, because it’s ubiquitous, is often the primary data validation point or verification component for companies conducting international e-commerce. Email can reveal a lot about a transaction such as when it’s positively linked to the name of the customer and the length of time it has been in existence. However, email looked at alone is not enough.

Standardization of dwelling addresses in the UK, Canada, Mexico, and other regions make this data point valuable in verifying order authenticity. But in Saudi Arabia, for example, residential addresses are not uniform in format and are therefore less effective for verifying a shopper’s order.

In certain regions, such as Brazil and Mexico, certain mobile carriers can be indicative of risk. However, across every region in the world, non-fixed VoIP numbers, like Google Voice or Skype, prove much riskier than fixed VoIP, mobile phone or landlines.

Also in Brazil, an e-commerce market projected to reach $27 billion by 2018, shoppers possess a unique identity number called a CPF (essentially a taxpayer ID number). This piece of data can also be compromised, leading retailers to consider additional data elements, such as IP address and mobile number when verifying transactions.

CHALLENGE #1

What implications does a lack of an identity standard have on a retailer’s fraud strategy?

- Good customers are rejected
- Revenue is lost
- Risk signals are missed
- Manual review costs skyrocket
Cybercriminals are always testing new tactics to circumvent fraud management systems. They often share or sell key fraud information with other criminals, establishing powerful networks. Companies doing business across national boundaries need to be aware of and responsive to the changing dynamics of global fraud. Common online fraud tactics include:

**Chargeback**

When the credit card issuer sides with a consumer’s fraud claim and a merchant loses out on the product and the revenue.

**Friendly fraud**

This type of fraud also results in a chargeback and occurs when the cardholder or someone known by the cardholder (like a relative) commits the equivalent of digital shoplifting—claiming non-receipt or having never ordered a product that they did in fact order.

**Account takeover**

When criminals take over online banking accounts. Often times this is the result of phishing, malware or data harvested from a breach.

**Synthetic identity fraud**

A falsified identity based on a combination of real and fake information. But others are even more complex and nefarious.

**EXAMPLE #1**

**MMO fraud**

Massive multiplayer online (MMO) games, a market that approached $20B in 2016, is driven largely by in-game purchases. In some countries, cybercriminals organize “gold farms” where huge numbers of fulltime players, often using false or stolen identities, acquire in-game currency, which is then sold for real money. But when MMO operators shut down the original false accounts, purchasers lose their money.
EXAMPLE #2

Retail crime groups

Some highly organized retail crime groups prey on retailers’ weaknesses during their checkout processes. They detect vulnerabilities, such as site code loopholes or promotion/coupon abuse to see what they can get away with. For example, if the criminals learn the company’s review threshold for purchase amounts is above $500, they buy below that amount since there is a greater chance of going undetected. Additionally, they place as many orders as possible without triggering velocity rules.

These criminals are experts at reverse engineering retailers’ risk models.

EXAMPLE #3

Failure to coordinate

Failure to coordinate across corporate divisions can set a retailer up for the worst possible fraud scenario. For example, fraud teams need to be given advance warning when new products in high demand are released. New phones, sneakers, and limited issue toys can cause a sudden influx of orders, overloading a fraud team’s operational threshold. Similarly, flash sales and discount codes can increase order rates and cause issues for fraud rules. Preparing for these planned events as well as new alternative payment methods (i.e. installment payments in Latin America) may require updating fraud policies, team expansion, and more.

Did You Know?

The fraud attack rate increased by 8.9% in 2016, led by massive increases in fraud in the apparel (69.9%) vertical.
Fraud Risk Varies by Region

Some regions of the world are simply less risky for cross-border e-commerce. Lower levels of risk can be associated with a combination of factors, including availability of consumer identity data, security of payment methods and population density. Denmark, Finland, New Zealand, Norway, and Switzerland are among the least fraudulent countries.

Where are the world’s fraud hotspots?

Indonesia  Venezuela  Romania  Brazil  South Africa

It’s estimated that more than a third of all online transactions from Indonesia are fraudulent. But with a 250 million and growing population, retailers have begun to focus on how to sell successfully to this country. This is good news for the millions of upstanding shoppers who are largely ignored by leading online retailers.

During the 2016 Olympics, Rio de Janeiro retailers saw a surge of fraud when hackers installed malware on electronic credit card readers in advance of the arrival of athletes, sponsors, and fans. Credit card cloning and Radio Frequency Interception (RFI) of credit data at restaurants and other public areas has reached epidemic proportions. Amplifying the problem are insufficient laws and weak enforcement.

Did You Know?
The world’s largest e-commerce markets are China, U.S., U.K., Japan, and France.
Unfortunately, a merchant's fear of fraud can often limit the shopping experience for legitimate customers. In extreme cases, entire countries can be “blacklisted” upon experiencing uncontrollable fraudulent activity. Countries on this short list include Nigeria, Romania, and Vietnam. However, overly cautious fraud prevention strategies are more common and result in customer insult. In both scenarios revenue is lost.

Nearly three-fourths of organizations that track false positives believe that up to 10% of the orders they reject on suspicion of fraud are actually from legitimate buyers. Merchants that reject a sale to a legitimate buyer lose not only immediate revenue, but also the opportunity to build a long-term customer relationship as rejected buyers take their business elsewhere.

In a recent survey (P. 22, figure 21) international e-commerce merchants have a higher rate of false positives than domestic merchants. This means that 35% of declines would have been successful transactions by legitimate consumers.

**How to prevent overcompensating for risk:**

- **Track an accurate tally** of false positives and review multiple period analyses of false positives
- **Coordinate with your Chief Revenue Officer** to thoroughly understand the global expansion roadmap to prepare well in advance for unique risk factors in new markets
- **Utilize identity data** in conjunction with fraud scoring to confidently auto approve orders to save time and speed good orders without using costly manual review
Multiple Identity Data Elements are Required to Make Good Decisions (And what tools do I need?)

Reducing online fraud while preserving a good customer experience requires companies to verify identities quickly and accurately. Unfortunately, with today’s savvy cybercriminals hijacking identities and data, merchants can’t just look at individual identity elements. They need to be reviewed in tandem to establish links between individual identity elements. Sourcing this much data for effective identity verification is daunting. The good news is that there is a source for reputable global identity verification solutions.

Today’s API and web-based services can conduct multiple searches at once and link together real-time identity data to ensure order authentication. One common example is to verify that a customer’s name, addresses, phone numbers, email, and IP match from an order or transaction. Some tools go so far as two different data input fields for physical addresses (i.e. separate billing and shipping information) within a single query. When retailers see the full picture of a customer’s identity, they can fulfill orders faster, reduce customer insult rates, and quickly identify truly risky transactions or new accounts.

Going one step further than verifying individual data elements—identifying linkages between multiple data elements—is exponentially more powerful. Knowing that a phone number ties back to a name, that an address ties to the same name, and that the IP address is within a few miles of the address as listed on the order are very strong positive signals for a savvy merchant using a vendor with identity data linkages.

Did You Know?

Under the current regulations, merchants and credit card issuers don’t communicate with each other to verify identity. This can create bad consumer experiences that impact the vendor or card issuer brand.
Using a Multi-layered Approach to Approve More Cross-border Transactions and Still Avoid Fraud

Automated fraud screening offers an efficient means for detecting and controlling fraud. But, successfully catching fraud requires utilizing global consumer identity data as part of a layered process. Many organizations have adopted Gartner’s research on the 4-step process to identity verification:

STEP #1

**Endpoint**

The endpoint screening process starts by identifying the device location or fingerprint (or other endpoint data like location, device point, device behavior, phone, mobile ID, etc.)

STEP #2

**User navigation**

This focuses on a user’s behavior in-session, determining if the behavior looks legitimate or malicious (i.e. web session navigation behavior, in-app behavior, gesture analytics, etc.)

STEP #3

**User data**

This focuses on pulling data such as credit card information (like external personal identifiable information, social network info, internal records, etc.)

STEP #4

**Linkages and metadata**

Linkages and metadata: this focuses on making connections between dynamic identity data (like person, business, phone, email, address, etc.)

As discussed earlier, finding data linkages are key to validating a consumer’s identity. At the same time, fraud patterns can be recognized in real-time, flagged, and incorporated into fraud rules. Knowing your business’ risk signals is key to reducing cross-border e-commerce fraud.
Some of the **risk signals** when looking at customer data include:

• With very few exceptions, non-fixed VoIP numbers are riskier than mobile or land lines. Certain carriers are known to have higher levels of fraudulent accounts associated with them.

• Email address is less than 90 days old.

• Phone, email or address is invalid.

• There are proxy IP addresses.

• The IP address is more than 100 miles from the physical address or phone locations.

• The email, phone or address linked to the transaction does not match customer’s name.

Some of the **positive signals** when looking at customer data include:

• The email address has been in use for more than 720 days.

• The IP address is located within 10 miles of the physical address or phone location.

• The phone number matches the customer’s address.

• The registered owner of the email matches the name on the transaction.

• The phone subscriber’s name matches the name on the order.

• The address resident’s name is a match to the customer’s name.
Summary

As the global economy moves online, it's becoming more difficult to quickly and accurately confirm consumer identities. Even historically useful authenticators like Social Security Numbers are no longer enough. National IDs can't address the worldwide marketplace and many have been compromised by data breaches. The demands of global commerce and risk management have given rise to a multi-layered approach to verifying identities—one that looks to correlate common customer identity data such as phones and emails, behavioral analytics, device identification, and existing profile information.

**Ekata Identity Check** is a 5-in-1 global identity data solution that helps companies identify fraud and speed good transactions to clear. In a single API query, Identity Check returns match statuses and risk signals around the five key consumer data attributes of name, address, email, phone, and IP address. It leverages the Ekata Identity Graph™, which houses over 5 billion global contact records and curates 1 million linkages per day to connect these consumer data attributes. The Identity Graph ingests data from over 100 global data sources, to provide accurate, rich, and complete global identity data to businesses worldwide.

Ekata is deployed by global merchants for speed and scale with our enterprise-grade API or web application. The company’s global consumer identity data is available in all leading fraud management platforms.

“Some fraud attempts can be detected early on, and others aren’t revealed until much later in the checkout process. By layering together multi-modal fraud tools, retailers can protect against a greater variety of fraud tactics. This is critical for retailers selling cross-borders where fraud may be less predictable.”

Robert Capps
VP of Business Development
NuData Security Inc.

Schedule a meeting with one of our Global Identity Data Experts

**SCHEDULE NOW**

Or call us at +1 877.767.8052