EKATA

PRODUCT BUYERS GUIDE FOR MARKETPLACES

TABLE OF CONTENTS

PRODUCT BUYERS GUIDE FOR MARKETPLACES

Marketplaces face many challenges when it comes to platform growth and risk mitigation. First and foremost, marketplaces must provide a positive experience to customers throughout their journey in order to create repeat business and grow the network. At the same time, marketplaces must prevent fraudsters from entering the platform and strengthen platform reputation by preventing account and content abuse. Also, marketplaces must ensure that there is an easy way to transact while simultaneously reducing the number of fraudulent transactions. And when fraudsters gain access to a marketplace (and some will), they must be detected before the payment authorization.

PLATFORM INTEGRITY IS INTERTWINED AT EVERY STAGE

When thinking about user experience and fraud prevention, a marketplace must use a holistic approach. After all, platform integrity is intertwined throughout every stage of a marketplace; from account opening and buyer/seller transactions to checkout, payment authorization, and shipment. For example, if a marketplace validates identities at account opening, the transactional risk can be decreased by weeding out bad users such as bots and spammers.

In addition to validating identities at account opening, using a solution to mitigate risk at the point of transaction, marketplaces can further decrease the number of fraud attempts, chargebacks, and additional fees paid to major card brands. With a higher population of good users to work with, marketplaces companies can reduce manual investigation and leverage it for only the riskiest subset of accounts and transactions. Marketplaces that monitor the lifecycle and interactions of every account create a positive customer experience because there is visibility into "typical" user behavior across the board. Understanding legitimate user behavior allows marketplaces to pick up patterns of bad user activity quickly such as account takeover (ATO). Understanding and developing the product with ideal user behavior in mind and knowing patterns of the riskiest users allows platforms to innovate and scale with less risk.

One major goal of a marketplace is to connect the demand of buyers to the supply of sellers with a simple-to-use, reliable user experience (UX). The buyer-seller ratio must be proportionate for users to have a positive experience on a marketplace. For example, if a rideshare marketplace has no drivers nearby for a rider causing a 30-minute wait time, the rider will leave and go to a competing service. And the buyer sellerratio means nothing if users are not legitimate.

To ensure trust and safety across your entire platform focus on two key areas to ensure platform integrity: identity validation at account opening and identity verification for each transaction.

Account Opening - A Critical Piece of a Marketplace

Account opening is a crucial piece of a marketplace— there is no marketplace without sellers and buyers joining the platform. Most marketplaces have a unique onboarding experience for buyers versus sellers. And the onboarding experience varies depending on the size of the marketplace. The supply side of a marketplace requires a different type of

scrutiny regarding risk because the types of fraud are far more costly. For example, a fake storefront could rack up hundreds of thousands of dollars before disappearing.

When it comes to the demand side of the marketplace, the risk stems from allowing just any user on the platform. If your role is user acquisition, your number one priority is increasing the number of users on the platform. So, you want to ensure that the sign-up process is optimized and with the least amount of friction possible. On the other hand, if your role is fraud prevention or trust and safety, your number one priority is preventing bad actors from getting onto the platform. And preventing fraudsters from creating or taking over accounts is the best way to achieve that goal. Finding balance and communication between teams is critical to best support these goals.

Fraudsters Employ Sophisticated Techniques to Create Fake Accounts

Fraudsters use synthetic or stolen identities to create fake accounts on marketplaces; synthetic identities are especially tricky to detect. If a fraudster uses information from three different identities, such as an email bought on the dark web, a random stolen name, and a phone number from a data breach, they look like a valid identity when pieced together.

Identity validation at account creation is a critical first step as the first line of defense against fraudsters. Whether the sign-up form is completed by a legitimate consumer, a fraudster, a basic script, or a bot, marketplaces request the same basic information when verifying identities: name, email address, phone number, and physical address. All marketplaces require, at a minimum, a name and email address to create an account.

Solutions Marketplaces Employ at Account Opening

Most marketplaces employ a combination of solutions at account opening to prevent bad actors from gaining access to the platform.

Identity Validation

Many marketplaces use an identity validation solution at account opening which enables real people to create marketplace accounts quickly and easily while also adding a light layer of fraud prevention behind the scenes.

Two-factor Authentication

Some marketplaces employ two-factor authentication (2FA) in addition to an identity validation solution. When a new customer signs up for an account, an authorization code is sent to the customer's phone or a confirmation link is sent to their email address. 2FA can be an effective means of identity verification- it checks to see if the device logging

into the platform is from the actual owner of the account. 2FA is not foolproof though. Fraudsters use techniques such as phishing and password reset to bypass 2FA.

Device Fingerprinting

Others add another layer to account opening security measures by implementing device fingerprinting. A device fingerprint uses identifiers such as IP address, device ID, and browser version to verify the identity of users as they sign up for and login into accounts. Most multilayered fraud prevention products feature device fingerprinting capabilities.

Enhanced Identity Verification

Sophisticated marketplaces use enhanced identity verification tactics by linking digital and traditional identity attributes. This can be supplemented with expensive and cumbersome document uploads and background reports as an additional check-point if needed. For example, a ridesharing marketplace typically requires drivers to upload copies of their driver licenses. For some marketplaces, compliance/KYC is important as it helps to make sure the platform is adhering to required financial and legal compliance requirements for online transactions of money, goods, and services.

Many marketplaces use a behind the scenes, digital process for identity verification that involves the linking of identity attributes together through progressive sign-up flows. This process allows onboarded users to build profiles with more information about themselves. And because the process is behind the scenes, identities are verified without users feeling the friction behind the process.

By the time users get to a transaction, the marketplace should have a better indication of the risk level users pose. The stage of a marketplace might change how the risk level is assessed- mature marketplaces may use progressive information collection and user segmentation based on information provided. Less sophisticated shops often use single point data validation methodologies.

Account Opening Solutions

	Validation solutions	Two-Factor Authorization	Device Fingerprinting	KYC/AML Document Upload	Background checks
Functionality	Validate user identity	Time-based, one-time OTPs	Capture Fingerprint of a device	Verify driver's license, etc.	Full verification of legal records - Requires PII
Vendor example	Ekata	Twilio	Sift	Jumio	Checkr
Product Name	Phone Validation Reverse Email	Authy	Device Fingerprinting API	Netverify ID Verification	Screenings

Transactional Risk – A Significant Point of Contention for Marketplaces

Transactional risk is a significant point of contention for marketplaces because transactions are the height of user engagement- transactions are where real dollars and goods are exchanged. Most marketplaces support multiple payment options to allow flexibility and ease of use for their customers. Marketplaces that enable payments must deal with fraud attempts before the payment authorization takes place. The types of fraud marketplaces must catch before payment authorization include credit card fraud, card testing, and cross-border fraud. Marketplaces must also prevent payment fraud as it is difficult for merchants to reverse a payment authorization once it is completed. If the payment is fraudulent, it can take days for refund settlements to be processed. And like merchants, marketplaces must not exceed the 2% maximum fraud rate allowed by the card brands.

Solutions Marketplaces Employ to Mitigate Transactional Risk

Marketplaces must implement an effective solution to mitigate transactional risk and prevent payment fraud. There is a small window of time to decide if the customer is good or bad during a payment transaction.

Internal Data and IP Intelligence

When it comes to transactional risk, many companies use internal data such as account age. Internal data is used to discover unusual patterns based on historical account activity. A marketplace might use internal data to build an internal blacklist. However, additional data is usually needed for the marketplace to make a better and more informed decision as to which users should be placed on a blacklist. An IP intelligence solution is a tool that marketplaces can use to build blacklists that filter out potentially bad users. Although, most IP intelligence solutions only look at IP addresses. Transaction Risk API provides the benefit of full identity verification at the top of the funnel.

Automated Solution That Leverages Machine Learning

For most marketplaces, preventing fraudulent transactions requires an automated solution that leverages machine learning (ML). An automated solution is required due to a high volume of transactions, to protect against the use of bots and botnets in high-speed, high-scale fraud attacks.

Adding identity verification to an ML solution can improve the performance of fraud/risk models to help marketplaces weed out bad actors as they go through checkout. Leveraging machine learning and automation aids in platform optimization as it reduces the number of manual reviews required to spot check performance. Leaving the manual review team to only investigate the riskiest subset of marketplace users.

Transaction Risk API

Transaction Risk API provides global identity verification in under 100 ms to improve model performance at scale. Marketplaces can easily integrate the API into existing models to fight payment fraud and improve the efficiency of authorizations.Leveraging identity verification earlier in the transaction flow optimizes the model to reduce false positives and find previously undetected fraud.

“To prevent fraud and identify good customers early in the transaction flow, businesses have historically relied on their internal data and signals. But as they move more commerce and services online, these businesses face both an order of magnitude increase in transactions and a compressed time window to make decisions. Transaction Risk API addresses these needs by leveraging technical innovation and machine learning to deliver a suite of our most predictive attributes,” said Ekata Senior Director of Product Management, Ajay Andrews.

Transactional Risk Solutions

	Identity Verification	IP Intelligence	Manual Review
Function	For pre-auth modeling	Look at geo-location and/or IPs for building a blacklist	Manual investigation of risk
Vendor	Ekata	MaxMind	Ekata
Product Name	Transaction Risk API	GeoIP2	Pro Insight

Platform Integrity – An Ongoing Effort

Marketplaces lose revenue and reputation when platform integrity is compromised. And for marketplaces, platform integrity is an ongoing effort that happens throughout the lifecycle of an account. Platform integrity is not something to be considered at a single point in time or a specific stage or maturity level of the marketplace. No matter the size of a marketplace, platform integrity is crucial to the overall trust and safety of the platform.

Fraudsters find numerous ways to exploit marketplaces which can alter the perceived validity and overall trust of the platform. For example, many fraudsters create accounts to post fake product listings. If a product listing has thousands of unwarranted five-star reviews, buyers will be angry when they receive an inferior product. If a buyer pays for an item that never ships, they will be angry that they were scammed out of money. And the marketplace will take the reputational hit for allowing fraudulent suppliers to leverage their platform.

There are three sides to this story: buyer perception, seller perception, and marketplace perception. Buyers must perceive that sellers on the marketplace are legitimate, selling real products, and have genuine reviews. Sellers and buyers must perceive that the marketplace is not inundated with bad actors and bots. Marketplaces must also make sure

bad users are unable to take over the accounts of legitimate users of the platform.

Solutions Marketplaces Employ to Ensure Platform integrity

A variety of solutions are available today that help marketplaces prevent fraud and ensure the overall integrity of the platform.

Data Validation and Identity Verification

Marketplaces start with data validation during onboarding and account opening to ensure platform integrity. The next step involves using collected information at each point of a transaction to determine the legitimacy of users. An additional step that helps at both account opening and point of transaction is leveraging internal data to understand user behavior and patterns of interactions.

User and Behavioral Analytics

Transactions and user behavior must be monitored to detect unusual patterns and fraud. Behavioral analytics and fraud prevention platforms allow marketplaces to monitor user activity and detect unusual and abusive behavior on the platform.

Ekata Products

Ekata products ensure platform integrity by verifying the identity of users throughout the lifecycle of an account. The product suite can validate identities at account creation, boost the performance of ML models, and provide insights and deep dives for manual investigation to best understand your users.

Platform integrity Solutions

	Identity Verification	Device ID	Behavioral Analytics	Manual Investigation	Internal Data
Function	For post-auth modeling	Check velocities of device IDs	Platform and Account integrity	Investigate transactions	Leverage Known patterns of your own user base
Vendor	Ekata	Iovation	Sift	Ekata	N/A
Product Name	Identity Check API	FraudForce	Account Defense	Ekata	

TAKE A MULTI-LAYERED APPROACH TO IDENTITY VERIFICATION

As the global sharing economy grows online, it's more difficult to quickly and accurately confirm identities. Historically useful authenticators like Social Security Numbers are no longer enough, and National IDs don't address the worldwide marketplace with much of this data being compromised in breaches. The demands of global commerce and risk management have given rise to a more sophisticated multi-layered approach to verifying identities—one that looks to correlate common key customer identity data such as emails, phones and physical addresses, with behavioral analytics, device identification, and existing user profile information.

This is especially true for marketplace companies who have diverse user base of buyers and sellers. Taking a holistic approach to identity verification, utilizing multiple fraud protection and risk mitigation tools to increase customer transactions while decreasing the amount of fraud, helps keep the platform trusted and safe. This multilayered approach is critical to grow a marketplace, with a strategy more sophisticatedthan the fraudsters who attempt to break in.

Ekata is deployed by global merchants for speed and scale with our enterprise-grade APIs and SaaS tool. We apply pattern recognition, predictive analytics, and machine learning to the five core consumer attributes of email, phone, name (person or business), physical address, and IP to deliver unparalleled coverage and accuracy, Powered by the Ekata dentity Graph™, and our Identity Network, we provide real-time insights from the millions of daily online transactions of our risk management conglomerate.

"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.