How to Detect Online Fraud in 2020

The first thing to know about online fraud is that it's very profitable. It is a multi-billion dollar business, growing and evolving.

It's easy for fraudsters to obtain basic personally-identifiable information. Merchants should always presume that the names, addresses, and social security numbers of most U.S. consumers are compromised.

A fraudster could then combine that info with anonymized services such as disposable "burner" mobile phones, temporary email addresses, and proxy (hidden) IPs to construct a fake identity.

The good news, however, is that fraud prevention is increasingly sophisticated, too, especially via machine learning, which is self-teaching and improves over time.

Machine learning can analyze a vast number of worldwide data points and run complicated logic to improve detection and reduce the need for rules and manual reviews.

Data Attributes

The rise of the internet has created massive amounts of data. All companies — ecommerce included — have access to internal and external data that can differentiate good customers from fraudsters.

Start with internal account data, such as order history and purchase patterns. Is it a first-time customer? Is the transaction time-of-day typical for the customer? Has there been a change in the account, such as a new physical address, email address, or phone number?

Protection for Merchants

Ekata is a global identity verification company to protect merchants from fraudulent orders while minimizing false declines. We work with thousands of international merchants and payment providers, including Amazon, Expedia, Alipay, Stripe, and American Express.

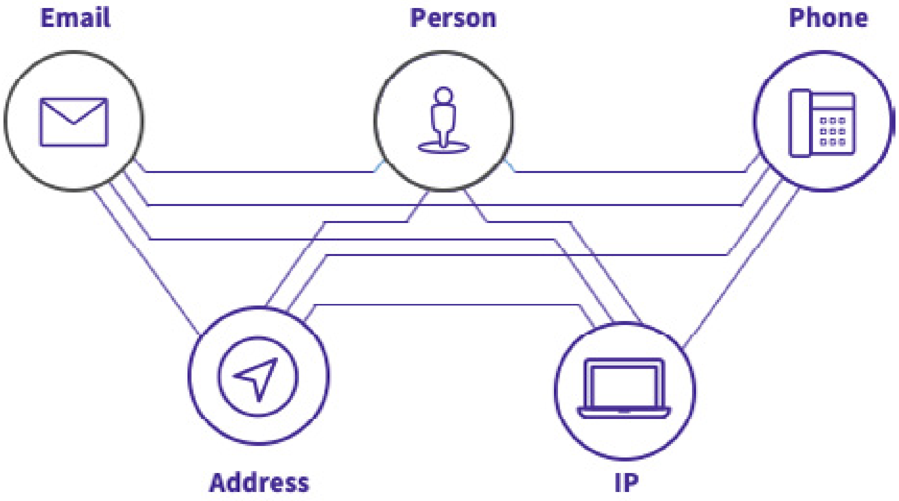
Our fraud-prevention tools easily integrate into any ecommerce workflow (proprietary, hosted, licensed) with a single endpoint to automate and optimize your decision rules.

Ekata is 100-percent cloud-based and always available. Ekata accesses roughly 2 billion identity records per month with return speeds of less than 250 milliseconds — the fastest available.

Ekata's global coverage extends to more than 170 countries with unparalleled data quality, coverage, and accuracy. Customer service is a top priority — retention rates are roughly 100 percent.

Evaluate the contact data. Is the buyer's phone number real or from a burner phone? Is the email address legitimate or temporary? Does the physical address exist?

Is the buyer associated with the phone, email, and physical address? The name, address, and phone number may look good. The email and IP address may be real. But if none of them are linked, or if the IP address is far away from physical components, it's a high risk.



IP proxy detection is critical. A buyer using an IP proxy (a third-party intermediary) is always a higher risk.

The product itself can indicate fraud. What is the buyer trying to purchase? Certain items, such as new tech products, are intrinsically high-risk. Consider, too, the purchase amount. It the transaction high-dollar and unusual for the customer?

The combination of account, contact, and product data is a powerful way to identify fraud. But it doesn't help with account takeovers (where a fraudster "takes over" a legitimate existing account) or with so-called synthetic identities via anonymized services. Both require more sophisticated tools to detect.

External data can also help detect fraud. An example is devices. Is the buyer's device recognizable? Does the IP address match the shipping destination? Has the buyer used, say, this iPad previously? If a customer has always transacted on a particular laptop and now it's a smartphone, you likely should investigate.

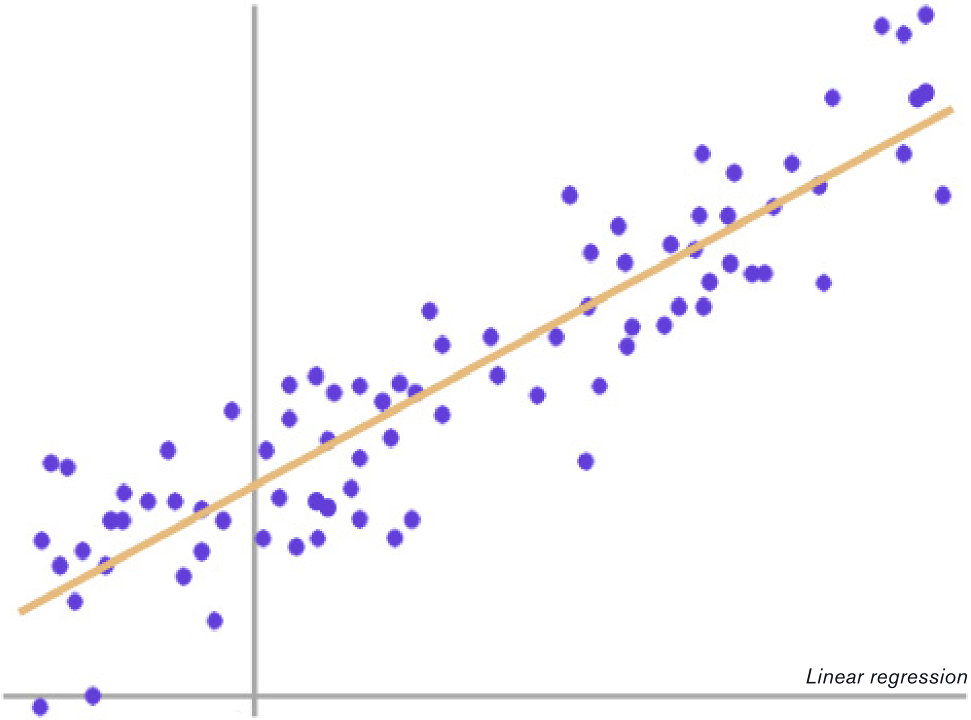
Geography matters in fraud detection. Fraud is typically much higher in certain countries, those with lax law enforcement or legal structures.

All of these data points (and thousands more) can identify good or bad customers. But the analysis requires advanced tools and models.

Analysis

Real-time, machine-learning fraud-detection accesses vast amounts of data and makes instant decisions based on historical experiences. For example, past usage may show that a purchase transaction that's 300-percent higher than average from an unrecognizable IP location is 90-percent likely to be fraudulent.

There are two standard models for such an analysis: regression and tree-based.



Regression is the simplest. It's a linear combination of variables, such as the purchase amount and IP location.

Tree-based models are more complicated but far more effective in detecting fraud. A tree-based model can accommodate all kinds of variables with minimal effort. An example is helping a merchant decide whether to extend credit to a customer based on age, education, income, and home ownership.

Ekata by the Numbers

$17.4 BILLION.
Amount saved by companies after Ekata identified $162.5 million in fraudulent transactions.

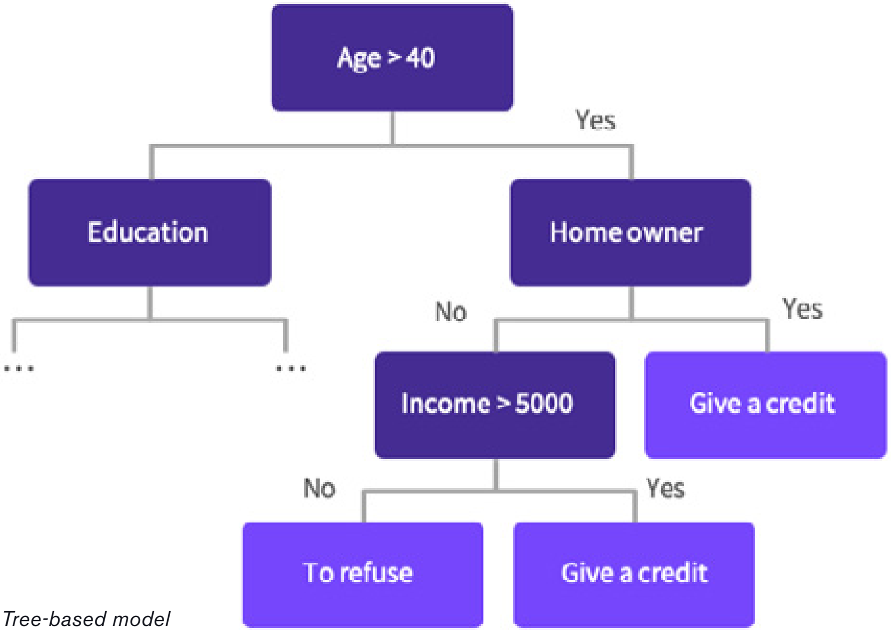
$56 BILLION.
Additional revenue approved when Ekata identified over 520 million good transactions.

$140.6 BILLION.
Total commerce touched by 1.38 billion transactions monitored by Ekata for its customers.

Tree-based models are also much better at identifying complex relationships or interactions, such as comparing a phone line type and the country. Or a product category and IP address.

Beyond modeling, a rare data point could indicate a higher or lower risk, depending on the scenario. Tracking or calculating the frequency of this data point may be secondary.

Also, be wary of data that is inconsistent or subject to change. Machine learning assumes that fraud patterns shift over time.



Tree-based model

Lastly, there's always room to improve the model. Certainly it's a good idea to have a success benchmark in mind or to identify a point of returns wherein it's better to move on and do other things, such as creating a separate model to predict a particular nuance. But there's always more to do. A fraud-prevention specialist should never say, "I'm done. I've totally optimized our model!"

In short, while online fraud is growing and evolving, modern detection tools are exceedingly robust and sophisticated. The availability of worldwide, real-time data combined with tree-based, machine-learning models enables near-instant approval of orders from good customers and rejection of those from fraudsters.

About Ekata

Ekata facilitates worldwide ecommerce by providing global identity verification solutions via enterprise-grade APIs for automated decisions, and via Pro Insight, a SaaS solution for manual review for businesses to grow revenue by maximizing the predictability of good transactions.

Ekata's product suite is powered by the Ekata Identity Engine, the first and only cross-border identity verification engine of its kind. Businesses around the world — including Alipay, Microsoft, Stripe, and Airbnb — leverage Ekata's tools to increase approvals of more good transactions, reduce customer friction at account opening, and find fraud. For more, please go to Ekata.com or call 877-767-8052.