id:analytics®

WHITEPAPER

Improving Insight into Identity Risk through Attributes

March 2013

Table of Contents

Introduction to Identity Attributes

Risk management strategies are often presented with two distinct challenges: assessing the risk associated with existing customers and evaluating new consumers. While organizations have a lot on the line with both challenges, the data they have at their disposal to manage these risks differs significantly.

Companies offering new products or services to existing customers can simply use historic performance data to make those decisions. All that is needed is to pull up the customer's record and evaluate the institution's experience with that customer. Is the customer behaving normally? Is the customer low or high risk? In some cases, an analyst will manually pull the customer's file and in others, a scorecard based on the customer's historic performance has been built to determine the customer's eligibility for additional products and services.

But, what can a company to do to manage risk when it wants to offer products or services to brand new customers? Many institutions ask for the prospective customer's personally identifiable information (PII) and will submit it to a third party for purposes of authenticating the person's identity or determining the risk for fraud. Risk management solution providers can return summarized credit or fraud scores which can be very useful at predicting the likelihood of default or risk for fraud based on the PII used in the application.

While scores and grades are typically very accurate, organizations are increasingly requiring more visibility into the specific risk factors summarized in these assessments. How can an institution gain detailed insight into identity risk to assess the risk of new customers? Identity attributes are an excellent complement (or alternative) to scores when an institution is looking for a third-party opinion about a prospective customer's legitimacy or risk for fraud. The intention of this document is to explain what identity attributes are, how to use them, and how a company might go about assessing their value.

Identity Attributes Defined

Identity attributes – sometimes referred to as identity data variables or elements – are calculated facts that describe an asserted identity in the context of an event during the consumer lifecycle (e.g., new-account application, account-management activity, collections processing). The most common reason for collecting identity attributes is for authentication purposes. For example, when a person wants to gain access to their records via a local government's website, the agency requires that the person input a set of identity elements (e.g., Social Security number, name, address, phone number, date-of-birth, or email address). Those identity elements are then compared to what is known about that person and attributes are generated (e.g., "Does the asserted address match the one on file: "yes" or "no"?).

Another common and successful use of identity attributes is fraud prevention. Identity attributes can provide very specific information about an identity asserted during an event which can be both informative and even predictive. Attributes have a wide range of sophistication, ranging from basic insights such as incident counts to more complex insights achieved by examining patterns and the interrelationships of identity information.

In a fraud scenario, a basic "count" attribute such as "number of times the asserted SSN has been used on an application" can provide important insights. It could indicate lower risk if that SSN's frequency falls within a normal range, however, it could be associated with elevated risk if the credit-application frequency is above normal or if that SSN has never been used on an application previously.

More complex attributes often measure the relationship between two or more identity-related elements, for example "Number of unique addresses associated with the identity, normalized by age group". Interestingly, an attribute's level of sophistication has little bearing on the predictive or informative value of an attribute. The most effective risk mitigation strategies often utilize both simple and complex attributes.

Whether an institution wants to authenticate an identity or prevent fraud, identity attributes are powerful tools that can reduce risk while facilitating safe commerce.

Types of Identity Attributes

There are multiple ways to categorize identity elements based on their use and the type of information available. The following is a high-level overview of some of those categories:

Attribute Category	Description	Sample Attributes
Confirmed negative behavior	Compares event information against confirmed, historic fraudulent events.	Number of times confirmed fraud was reported using a Social Security Number (SSN) within: • The last one, five, 15, or 30 days • The prior three or six months
Pattern	Examines anomalies in identity elements and general consumer behavior.	• Unusually high number of recent events using primary phone • "Address type" codes used to identify high-risk addresses
Validation	Assesses the validity of input. Invalid input can highlight discrepancies that require resolution.	• Name appears to be a business name • SSN likely frivolous (e.g., "123-45-6789") • Primary phone type (e.g., landline)
Velocity	Examines the frequency with which an input element has been asserted across a range of time periods. These attributes provide insights into behavior that is out of the norm; the presence of increased velocity is potentially indicative of risk.	• Number of events using address in the last 15 days • Number of events using SSN in the last year • Number of different industry segments in which the consumer has submitted an application in the last 30 days (e.g., wireless, mortgage)
Verification	Assesses the legitimacy of input information. Used as a potential filter to exclude illegitimate identities or to highlight discrepancies and inform resolution strategies.	• Last name and primary phone confirmed • SSN and name combination reported as deceased • Level of confidence that the asserted identity elements match those for a known identity

How to Use Identity Attributes

It is difficult to assign a single value-proposition to the adoption and use of identity attributes because the insights they provide can be applied in so many different ways. In a broad sense, they represent a very large identity toolkit. Successful companies are finding unique ways to apply these tools to address numerous problems and to support decision optimization.

For instance, identity attributes can be applied to new account onboarding processes as previously discussed, or used to improve existing account management processes such as online profile change requests. They can be used for complex segmentation analysis or as simple, minimal-threshold-eligibility criteria. They can be applied to "All" applications or only to selective, high-risk or marginal-condition subsets of applicants. They can be used in conjunction with scores to drive more complex decision-logic processes or used instead of scores or used as inputs to custom analytics. They can be used in automated decision-engines or to improve manual processes. Because attributes can be employed for any or all of these use cases, it's ultimately incumbent on the organization to determine how to best translate their unique insights into improved risk management decisions.

Also, because identity attributes return known values (yes/no, counts, True/False, field codes etc.) it's relatively easy to periodically "fine tune" the use of attributes to adjust decision criteria to achieve more optimal outcomes and quickly respond to changing market conditions.

Finally, most attribute vendors support real-time, on-demand delivery of attributes as well as batch file processes so clients can match adoption of attributes with existing IT processing models and update cycles.

The following scenarios outline some of the most common use case categories for identity attributes...

Manual Review Use Case

An intuitive and straight-forward way to utilize identity attributes is as an investigative tool for manual reviews and screenings. In this case, attributes are employed as a way to verify the legitimacy of an asserted identity where concerns have arisen. The insight provided by each attribute can be viewed as individual clues that are efficiently made available to the reviewer. When these insights are examined in the context of an investigation, they can deliver the missing or critical piece of information needed to reach an accurate determination of the identity's fraud and verification risk.

For example, an investigator reviewing an application for potential fraud risk might zero-in on attributes which focus on confirmed negative behavior, like "Number of reported frauds at address in last 12 months" and "Email address associated with confirmed fraud in past 3 years" to help determine whether the application should be approved.

Rules-Based Strategy Use Case

In a typical rules-based approach, a series of business rules and corresponding gating criteria are applied in succession to an application or event. Treatment is assigned based on the flow-outcome of those rules which is determined by the information associated with that event or application.

By adding identity attributes to the information set for each event/application, organizations can significantly deepen their non-judgmental insights, create more sophisticated rule-sets and ultimately improve the precision of deterministic outcomes.

For example, an organization might use attributes which focus on verification, like "Full Name and SSN Confirmed = NO" or "Number of times same SSN/Name/Phone/Address have been previously used together ≥ 1" to determine whether additional steps are required to verify an identity.

Custom Model Use Case

For organizations choosing to base their risk management strategy on scorecards or other customized analytics, attributes can be extremely useful providing critical new information to help tailor models to the precise needs of their business. Whether layered on top of a purchased vendor score or serving as the foundation for a custom score built from the ground up, identity attributes provide efficient and reliable access to new data assets that can drive greater proven predictiveness.

For example, an e-Commerce retailer might use attributes which focus on unusual velocity, like "Unusual number of events using address" or "Number of events in past 90 days where this full name is associated with a completely different address" as variable inputs into their custom fraud model to insert greater sensitivity around a shipping address.

Comparing Scores and Attributes

For organizations looking to utilize a score-based approach to risk mitigation, the most significant decision to be made is often whether to buy a vendor score or to build a custom score using an attributes set.

Vendor scores and custom scores have different pros and cons. Vendor-provided scores offer a solution based on a generic strategy that is designed to perform stably across a number of different clients, typically customized at the industry level. These scores require less analytical sophistication to utilize and are quicker to implement, as they're already built. Alternatively, custom scores combine internal data with an attribute set, and allow companies to build a model more tailored to its specific needs, resulting in a solution that can sometimes exceed the performance of a generic score.

It is not necessary to choose one or the other as an organization may decide to use both solutions. A company may use a vendor score to rank-order the risk of identity-related events, and then focus the use of attributes on those medium-risk events that merit additional scrutiny, creating a customized solution. Deciding which combination of solutions to use typically comes from experimentation and testing. Ultimately, the decision on whether to adopt a vendor score, utilize attributes to build a custom score or both comes down to the amount of insight and control an organization desires, the availability of expert skillsets required, and the amount of time and effort they're willing to spend.

In summary, the following is a comparison of how vendor scores and attributes used in custom models diverge in how they are used and how value is driven:

	Vendor Scores	Attributes in Custom Models
Performance	Accurate risk assessments tuned to provide value across a variety of market segments and use cases	Highly accurate risk assessments tailored to an organization's business and market segments
Control of Model	Vendor managed, providing less insight into and control over the model	Managed by the constructing organization, providing full insight into and control over the model
Cost	Less expensive, as fewer internal resources are required	More expensive, as both the attributes and analytical resources must be purchased
Ease of Adoption	Quicker to production, as models are already constructed	Slower to production, as the model must be constructed

How to Evaluate Identity Attributes

For organizations that choose to apply attributes to their risk-management challenges, the fraud and verification market offers no shortage of attribute options from a wide array of providers. Against this backdrop, how does an organization determine the most effective attribute sets for its specific business challenges? For many, the process begins with a thorough attribute evaluation.

The first step in attribute evaluation involves a clear articulation of an organization's risk management goals and the insights required to meet them, followed by an internal analysis to identify gaps in existing internal data. Only after identifying the crucial, missing insights an organization requires to meet their challenges can a search begin for reputable attribute vendors.

Since attributes ultimately represent a way to digest predictive data, the principal determining factor of attribute quality is the accuracy of the data source. In determining whether the quality of a vendor's data source and derived coverage and the ability to provide distinct insights.

Key questions include:

- What are the sources of data used to generate attributes?
  - The most fundamental question in any attribute evaluation, and the first step in understanding attribute quality.
- How often are the data sources updated?
  - Effective identity attributes provide a current perspective on risk, making the recency of data sources an important factor. Attributes derived from public records or White Page data, which are only periodically updated, often present an outdated picture of identity risk.
- Do the attributes provide consistent geographic coverage?
  - Whether a company is operating regionally or nationally, it's important for an attribute provider to provide consistent geographic coverage everywhere the organization does business. For example, an attribute provider that focuses on the southern United States would not be an ideal source for a national company.
- Are the attributes diverse and derived from a wide variety of experiential sources, such as Credit, Payments, Transactions, and Telecom categories?
  - Effective attribute sets are derived from large, representative data sources capable of telling an organization what they don't already know.
- Do the attributes capture and represent consumer behaviors that are relevant, meaningful and important to the decisions being made?

The quantity of attributes made available isn't nearly as important as their relevance. Having visibility into "known fraud" attributes in association with occurrence, location and consumer identity, for instance, would be critically important for fraud decision-making whereas lots of attributes about public license record data or employment history may not be. By carefully evaluating internal risk management goals and data needs, then assessing attribute vendor data quality and relevance, organizations can produce a trimmed list of candidate providers suitable for further evaluation.

Picking the Right Provider

Conducting a performance test to assess the best attributes for an organization's needs is a crucial undertaking regardless of how a list of candidate vendors is produced. If an organization is constrained by time or resources, it may consider moving directly to a live pilot of the solution, or to segment a relatively small portion of its transaction volume for "champion versus challenger" testing. However, a retrospective test conducted across a variety of vendors is the ideal way to assess value if that company has the time and the staff to manage the process.

A retrospective test requires that vendors have the ability to "turn back the clock" to pull attributes on historical transactions based on the original date. For example, a company might provide to vendors a file that contains six months of new-account application information that has sufficiently aged to determine the outcomes of those applications. Because historical applications are used, the outcome (e.g., fraud / not fraud) is known to the organization, allowing for an accurate assessment of the attribute's value. This type of test can determine which vendor's attributes will enhance the organization's ability to assess fraud and verification risk.

An effective retrospective test design process can involve the following steps:

1. Representative Sample of Applications: The application data set must paint a representative and statistically significant portrait of an organization's business. Large application volumes over the widest possible time frame produce more reliable results.
2. Sufficiently Aged Transactions: During a retrospective test, it is impossible to determine whether a vendor's attributes would have prevented a negative outcome (e.g., fraud) if that test file does not contain records that have sufficiently aged. Outcomes ("tags") are typically available within 90 days for most events, but in the credit world, records require a full 12 months to age. Depending on the use case, the test file should contain records with the appropriate aging.
3. Clean Tags: An organization must possess all performance tags required to clearly understand the potential impact to its own business before providing a data set to attribute vendors. Being able to clearly differentiate fraudulent accounts from bad credit accounts can determine the success of the test.

After assembly, the file is typically scrubbed of performance tags and provided to all participating vendors. Vendors then append their attributes, generated as of the original application date, and return the file to the purchasing organization. The organization can conduct a final analysis to identify the best performing solution once all vendors return their identity attributes and the performance tags are re-appended to the analysis file. A prospective buyer should consider the following performance categories when evaluating vendor attribute performance:

- Firing Rate: How many times did the attribute "fire" (e.g., "deliver a non-zero response")?
- Fraud Rate or Confirmation Rate: For fraud analyses, how often did an attribute indicate fraud? For verification analyses, how often was an attribute able to deliver a "confirmation" response?
- Predictive Lift: This can be measured in multiple ways depending on the use case, but the end goal is to understand whether the attributes are providing the crucial, missing insights the organization is seeking. For custom models and rule-based strategies, this metric is often improvement to fraud-detection rate, the percent of total frauds captured within a given percent of overall accounts.
- Financial Analysis: All retrospective analysis will ultimately be won or lost with a return-on-investment or cost/benefit analysis. While the predictive lift analysis should determine the top performing attribute provider, solution and implementation costs must be factored in before determining the best vendor.

Performing a retrospective test can provide companies with a clearer understanding of how attributes will perform in specific use cases on their own data. Factoring in attribute performance, solution integration, and projected financial impact, an organization can make a much better decision about the value of using a third-party attribute vendor.

Better Data Yields Stronger Results

Attributes are only as good as the data sources and analytics used to create them. High-value attributes are derived from data which is relevant, accurate, timely, broadly-sourced and predictive. Attributes generated from high-quality data provide quantitatively better performance results which can be demonstrated in structured tests and comparative analysis as discussed. High-performing attributes, in turn, will drive improvements in business results which can be measured in acquisition rates, departmental efficiencies, fraud rates, customer retention, compliance metrics and ultimately, dollars and cents.

ID Analytics®, a leader in consumer risk management, is now making their proprietary ID Network® Attributes available to provide leading organizations with flexible access to the ID Network, the only real-time cross-industry network of U.S. consumer behavior. Comprised of over 2 billion consumer events, the ID Network offers a comprehensive view of consumer behavior and is currently used by numerous Fortune 500 companies across a range of industries. ID Network Attributes are able to provide on-demand access to granular fraud and verification insights needed to stay ahead of evolving identity-risk threats. These same attributes are used by ID Analytics in their industry-leading fraud and identity verification scores and services.

Available in Fraud and Compliance & Verification bundles, ID Network Attributes can easily be implemented across all points of consumer contact including online, call centers, mail, and in-store. For more information on ID Network Attributes and how they can be incorporated into a retrospective test, contact marketinginfo@idanalytics.com, call 858-312-6200, or visit www.idanalytics.com to learn more.

id:analytics®

www.idanalytics.com