



News

Who's Really Calling Your Contact Center?

ID Analytics' new authentication solution looks to break high-cost boundaries.

by Christopher Musico
Thursday, July 3, 2008

Security is always a concern for all contact centers, beginning with the first introductory phone call. With vicious scammers and plots to phish vital data from both companies and customers, authentication tools are essential. Also, a happy balance needs to be struck with legitimate customers who don't want to jump through the hoops of myriad questions just to get to a representative. San Diego, Calif.-based ID Analytics, an on-demand identity intelligence provider, believes it has shored up the weakest link in the consumer authentication process -- identity proofing -- with its newest solution, ID Analytics for Authentication.

Todd Higginson, director of product marketing for ID Analytics, says that most technology focuses on authenticating credentials such as passwords granting access to your banking information. Not enough is done, he says, to verify the identity associated with that credential: It's often only authenticated once during the initial proofing process, and more needs to be done. "The weakest link is strengthening the process prior to credential issuance," he explains. "With our approach, based on advanced analytics we can determine the risk of this individual for identity fraud with more sophisticated questions."

Avivah Litan, distinguished analyst for Gartner, agrees. "Companies need a better identity-proofing system," she states. "If you can keep costs down and offer [the] promise of a fraud score combined with beefed-up knowledge-based identity, then I think they'll have a real winner because that's one of the biggest issues, not just with financial institutions,

but any companies with new accounts. How do you know who you're dealing with on the other end of the line?"

ID Analytics for Authentication is a network-based solution that uses advanced analytics and the company's ID Network, which has a proprietary repository of information used to generate questions that can't be answered by quickly glancing over public records or credit reports. The information, Higginson says, is gathered on a voluntary, opt-in basis. "ID Analytics customers share identity information with the ID Network knowing that they will receive the identity intelligence that comes from the analysis of not only their own information, but also the information of the many other organizations contributing information," he says. "And they receive the benefit of this cross-industry analysis without the sharing or selling of raw data between organizations that would raise privacy concerns among consumers."

Litan says that customers are sufficiently motivated to share the data based on what they get in return: "Companies who use [ID Analytics] pass their application data -- e.g. application for a credit card account -- to ID Analytics for fraud scoring. In return, the companies get a better fraud score because ID Analytics' score is based on all the applications from all the companies [ID Analytics does] business with."

Higginson calls ID Network the country's "only real-time, cross-industry compilation of identity information to intelligently authenticate individuals." Each individual's identity

comprises various information patterns -- the new offering enables companies to differentiate between high- and low-risk patterns, while getting rid of unnecessary questions for legitimate customers. "This solution can throttle the sophistication of those questions," Higginson explains. "Somebody with a high risk of identity theft may have to get 100 percent of the questions right, while someone with moderate risk may [be able to get away with] an 85 to 90 percent pass rate. In some cases, people may not know some answers, and this solution allows that flexibility."

Litan explains that a key differentiator for ID Analytics' offering is that the identity questions are "based on harder-to-steal information" than public records and credit reports. "This is much closer to the chest than a lot of the public data being used in other authentication systems," she says, adding that some companies using public data include Acxiom, ChoicePoint, and LexisNexis. Higginson gives the example of asking someone the birth date of an individual who used to share an address with him. "There is no public data source to have a question like that answered," Higginson says, arguing that it would take multiple documents to try and piece together exactly who the other individual is, where she lives now, verify that she did at one time share

an address with the caller -- and then still have to verify her birth date.

ID Analytics argues that it can deliver a unique view of individual identity risk and can generate strong authentication questions that will cost half as much as existing question-based authentication products. Higginson says that the company does not buy, sell, or trade the data in its ID Network, and consequently does not need to pass any such cost along to clients. "This way, we can offer a much more cost-effective price," he maintains.

The issue of cost has been a problem, according to Gartner's Litan: "While the vast majority of consumers support the use of authentication questions when protecting personal information, [our] research highlights the fact that cost has been a hindrance to broad adoption of this technology within call center and online environments," she wrote in a statement released by ID Analytics. Discussing the new product in a subsequent interview with destinationCRM, however, Litan says she believes that ID Analytics for Authentication has the potential to break down that cost -- and adoption -- barrier. "It's a very promising offering to increase both security and customer convenience," she says.