

California

Reprinted with permission of BankNews Publications. Contents of *California Banker* are, and remain, the property of the California Bankers Association.

BANKER

R-U-U?

Don't wish to apply in person? Apply online! Sparse credit history? Just click here!

But, before we go any further:

are you YOU?

by David Nussenbaum and Melanie Turgeon Zimmerman

U.S. regulators now require banks to develop red flag fraud management programs that include documented procedures for detecting, preventing and mitigating identity theft. The Federal Financial Institutions Examination Council also recommended that financial institutions that do business online adopt multi-factor authentication. Fortunately, a sophisticated crop of new identity verification and authentication technologies has emerged to support such efforts. But all of these new tools also beg questions:

- How successfully are companies implementing these sophisticated identification tools?
- Are these tools effective in shutting the door on imposters?
- Are these tools a nuisance to legitimate consumers?

The match game

One of the more logical approaches to identity management is comparing submitted personal information to data on file. Provided a financial institution has access to a rich set of data to match against the information, determining if the applicant is legitimate is fairly straightforward. The challenge, however, is ensuring that the businesses' files contain the most current information and eliminating issues with confusing an applicant with a person on file with the same name. Therefore, data must be updated, scrubbed and cleaned constantly to ensure the most current information also is the most accurate.

Popping the question

Some financial institutions authenticate their applicants by asking them to share a few somewhat obscure things about themselves. Such questions may scare off the assailant. Unfortunately, these questions also have the potential to scare off good customers, who might take their business to a competitor.

Keeping score

Today, analytic models recognize a fraudulent application in ways far more sophisticated than mere data matching. Indeed, this approach has proven quite effective, efficient and holds great promise. Risk scores are often high or low. The challenge is with those identities that receive ambiguously middle-of-the-road scores. In these situations, companies need to plan next steps for processing customers.

What's the point?

Determining what solutions to implement, as well as the procedural questions to ask to most effectively stop fraud can be a daunting task. For example, should your process for validating new applicants be different than the one used for existing customers? More often than not, the answer is yes. As a result, financial institutions, credit grantors and lenders must establish an implementation strategy that conforms to all of their business needs.

Financial institutions often use a stand alone point solution that addresses a single business need or problem. This

About the authors: David Nussenbaum and Melanie Turgeon Zimmerman are members of TransUnion's fraud and identity management team and can be reached at dnussen@transunion.com and mtergeo@transunion.com.

strategy is valid and provides quick relief for a specific point-of-pain. The downside is that enterprise-wide solutions might produce better results over the long term.

The key, then, is to strike a balance between point and enterprise solutions.

Bigger is better?

When it comes to fraud tools and solutions, bigger isn't always better. For many existing identity management solutions, the old adage, "information overload" is apt. There are just too many messages, flags, alerts and options. It also is one of the prime reasons for the number of false positives and manual review cases organizations experience and the reason why many organizations are wary of implementing a customer verification solution.

To be effective, a fraud application must provide its users with clear guidance on what information to act on. Although a rules engine is a core component of any good fraud solution, it must provide solid, actionable information to empower the organization to quickly and easily

make the right changes, especially considering fraudsters are able to quickly adapt and find new ways to exploit. The goal of the identity manager must not be to find the biggest tool with the most options, but instead to find the right tool.

Tuning up

The process for properly configuring an identity engine for high performance begins with an understanding of your business. This includes answering such base questions as:

- What products are being offered?
- What markets are served?
- What are the channels being used?
- What prior cases of fraud have been documented and analyzed?

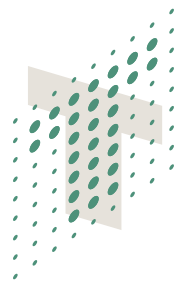
The second step involves an initial qualitative observation of normal business practice, as well as an assessment of primary threats and vulnerabilities. This should be supplemented by a more quantitative analysis of application and performance data to clearly isolate the data characteristics consistently associated with cases of fraud.

The third step is to conduct a technical validation to understand how

well the tool performs and optimize the configuration accordingly. For example a score cutoff may need to be changed for certain products or market segments. Or perhaps the authentication engine is repeatedly failing good applicants because a certain type of question is legitimately difficult for them to answer. Maybe a detail of matching logic needs to be changed, eliminating some pesky false-positives. Such parameters can be easily modified, once the symptom is accurately diagnosed.

Staying in tune

Sophisticated identity managers must dynamically adjust rules, cutoff scores and strategies as the business evolves, and as fraudsters conjure up new modes of attack. Like any sophisticated technological solution though, only half of the value-add is in the technology itself; the other half is the required skill to apply that technology toward your unique and complex business needs. **CB**



TransUnion®