Five Tips to Detect and Deter Fraud During Customer Acquisition

The Application Hustle

Daniel Jean
Assistant Vice President
Identity & Fraud Product Development

Vanessa Giuliani
Fraud Solutions Consultant

July, 2015

According to research by the Aite Group, the cost of fraudulent applications is expected to rise to $28.6 billion by 2016.

Fraud is flourishing — and fraud management, risk management and marketing teams need all the help they can get to combat what is an elusive, expensive problem. Because fraudsters look for weak points, account opening poses an obvious target.

The problem is universal and affects all industries. Finding a workable solution can be difficult because it requires balancing the competing priorities of optimizing the customer experience, minimizing operating expense, meeting regulatory requirements and mitigating loss.

In today's market, one of these priorities — optimizing the customer experience — gets lots of airplay, and for good reason. As the economy has improved, companies in all industries have pushed for customer acquisition.

But this wealth of potential customers has created an issue for fraud and security teams: More applications in the queue means an increased number of application challenges — questions and requests for additional verification, for example — which may create unnecessary friction with the prospective customer, compromising his or her experience and leading to lost sales and business.

WHAT BEST PRACTICES ARE POSSIBLE?

We suggest five tips to detect and prevent fraud at account opening:

1 | **Start with frictionless tools.** Many fraud detection tools work silently in the background, reducing friction between you and your prospective customer. These tools include scores, models and rules systems that detect suspicious identities early in the application process. For example, a scoring system might link a social security number with an address or phone number. If these pieces of identity "go" together, the tool would generate a score reflecting a certain amount of confidence that the applicant's identity is valid. A rules system might identify addresses or phone numbers associated with prior fraudulent activity.

Using these passive tools, only the identities that seem suspicious get passed on to more interactive, friction-causing screening. These passive tools help reduce abandonment rates and strengthen the foundation of a good customer experience.

2 | **Use analytics and big data.** Sophisticated, predictive analytics take passive tools into more advanced territory by leveraging vast amounts of data to discern patterns. These types of analytics include regression analysis, machine learning and neural networks, and would typically flag behavior patterns and connections that veer from "normal" relative to the likelihood of fraud.

The objective is to get as much relevant data as possible from a variety of sources. The better your data, the better the mathematics and connections, and the better the predictive capability of the model.

3 | **Reinvigorate your own data.** Companies often overlook the richness of their own data or don't update their tools to take advantage of the most current applications. A sophisticated rules engine can go a long way on both fronts. First, a rules engine lets you set up and waterfall through the passive fraud tools mentioned above. If necessary, it will then prompt the next level of verification, which might involve slightly more intrusive tools. At this point in the process, you've already let most applicants through the fraud screen and you're down to the small percentage of applications that truly seem suspicious.

Now the rules engine can examine your data to verify identity elements against past identity history using matching, inconsistency and validation techniques. In terms of matching, for example, the rules engine can see whether a Caller ID number or email address been used before in an application to your company (or a division of your company if you share data). The engine can "match" an applicant against a list of suspicious people you've already identified.

Know the Enemy

Who are the people defrauding your company, and how do they work?

Fraudsters talk.
There's an entire network — hundreds of thousands — of sophisticated fraudsters who share their knowledge and techniques, and work together to defraud companies. There are marketplaces where criminals buy stolen identities.

Fraudsters want ROI.
Once they've gone to all the trouble of buying or building a fictitious identity, fraudsters will use it to the fullest to leverage their investment.

Fraudsters like silos.
Many companies don't share information between channels, products, geographies or divisions. Fraudsters thrive on lack of information sharing.

Fraudsters are sometimes insiders.
It's disappointing but true: fraudsters exist within sales, customer service and other internal departments where information is accessible. And one insider can do a lot of damage.

Our research with customer data tells us that matching rules capture about 55 percent of fraud overall.* In terms of inconsistency, the rules engine might ask if a certain name and address is consistent with the associated social security number given. Or does a certain address come up again and again, but with different people living at it in the past year? Lack of consistency would raise an alert. Internal studies suggest that these types of rules catch about 25 percent of fraud.*

Finally, validation or filtering rules typically isolate high-risk variables and combinations of variables. For example, in a premise based check, if an applicant lives in an dwelling where multiple charge-offs have occurred in the previous 6 months, that is a suspicious situation. Our data tells us that validation rules capture about 20 percent of fraud.*

4 | **Use the power of exchanges.** Naturally, data from only one company or division will have blind spots, so it's a good practice to use the power of a network of similar companies to share fraud-detection information. Consider the efficacy of using a rules engine across not only your own data but the data of your peer companies. For example, has this applicant's social security number "matched" another fabricated identity at other companies, too?

If you're sharing data with your peers, you're more likely to stop criminals before they get to you.

Also, fraudsters often use the same fraudulent identity again and again for as long as it works. When it stops working at one company the fraudsters often move on to the next one — which may be yours. If you're sharing data with your peers, you're more likely to stop criminals before they get to you.

Another benefit of exchanges is that they help give you a window into what's new in fraud techniques, tactics and patterns. This preventative and detective system gives you time to react and tweak your rules engine to catch what's coming next.

Insist on a solution that facilitates changes with advanced reporting.

5 | **Embrace flexibility.** Fraudsters move fast, and you need to be ready for quick changes to shut down the latest scam. This can involve both changing your business rules and monitoring your fraud detection tool's effectiveness. With this in mind, you should insist on a solution that facilitates changes with advanced reporting.

For example, how many fraudsters are being caught? How many false positives are you generating? And if these numbers are not within your acceptable range, your tools should be flexible enough to adjust in real time. This way, you can react to new trends and ever-changing tactics, follow fraud patterns, identify fraud patterns earlier, and control false positives.

So, where is your company on the path to better application fraud detection and deterrence?

Are you onboard with these five tips?

Are your current procedures effective?

It's likely that there's more you can do — and help is available. There are excellent tools available to help you close the gaps in your process and help you lower fraud losses, cut operational costs and, perhaps most important, improve the customer experience.

** Internal studies are based on individual customer data. Each organization's fraud situation and results from fraud prevention tools will vary.*

❯ **CONTACT US TODAY**

For more information:
equifax.com/business/prevent-fraud
877-262-5261

EFX®