Top 10 Takeaways on Leveraging Big Data for Fraud Mitigation

“Big Data” is demonstrating its value across many industries. Public and private organizations are processing torrents of data—from terabytes to multiple “petabytes” (one petabyte is a million gigabytes). Examples we’ve seen in the news include predicting weather and airline delays, identifying treatments for premature babies, increasing operating margins, and reducing crime. For instance, using billions of Google search terms and data from the Centers for Disease Control, scientists can now predict flu outbreaks a few weeks in advance according to researchers publishing in Scientific Reports.1

Getting a “Big Data” view of anything is just a means to an end. For fraud fighters at credit unions, a major goal is reducing fraud losses. To do so, credit unions invest heavily in data, analytics and technology. They rely on internal IT resources and external parties to convert massive amounts of data into business intelligence—the predictive insights they need for better fraud prevention decisions.

Now that everyone seems to have jumped on the Big Data bandwagon, what are the implications of this trend for credit union executives who are trying to control fraud losses? The hype on Big Data is almost as voluminous as the data—but at the risk of over-simplifying a complicated topic, let’s examine what the Big Data story means from a fraud control perspective.

To Help You Cut Through The Hype, Here Are Our Top 10 Takeaways On How To Leverage Big Data For Fraud Mitigation:

1 | Big Data isn’t new. The application of Big Data for fighting fraud is not a new story. Financial institutions have long employed a variety of data sources to determine fraud risk, verify identities, control online access to credit union accounts, and reveal suspicious activities.

When financial institution personnel or credit union systems use a score, a reason code, or a flag in the course of fraud detection and prevention processes, they are likely already leveraging Big Data that came from a huge database with billions of records.

What continues to evolve is the sophisticated techniques fraudsters deploy, and the need for financial institutions to access even more data sources to help identify suspicious activity.

2 | Don’t just give me data — tell me what to do with it. Offering financial services is complex enough as it is. Credit unions want to make an instantaneous decision on a potentially fraudulent request or application. The credit union doesn’t want terabytes of data. The credit union doesn’t care about all the monitoring, sifting, scrubbing, and modeling involved behind the scenes. The credit union just wants to get insights, in milliseconds, in a simple-to-use form. Born from Big Data, credit unions want the scores and attributes that embody the predictive knowledge for reducing fraud.

Andrew Smith
Senior Vice President
Enterprise Fraud

Gasan Awad
Vice President
Fraud and Identity Product Management

June 21, 2015
3 | **Internal resources aren’t enough to win.** Internal systems, by definition, focus on the credit union’s own member base, incident history, and products. Fraud prevention teams need both internal and external perspectives. External data sources are essential because they give a credit union visibility into fraud attempts everywhere.

Fraud teams need more than outside data assets; they frequently seek outside expertise, too. Credit unions of all sizes often ask their outside data partners to develop data attributes, customized models, or analytical research for their specific anti-fraud applications.

When a known fraud threat has been identified by external resources, the credit union needs to know before that threat comes knocking at the door.

---

**Equifax Fraud Management Experts Offer The Following Tips**

1. Focus significant prevention measures on the first line of defense: account opening processes. However, don’t neglect the increasing fraud happening with Account Takeover schemes. Using a multi-layered approach to detect fraud at both account opening and high-risk transactions. Combining alerts can be essential for real-time, multi-channel defenses to address a wide spectrum of fraud threats.

2. Use internal and external data and analytics to detect hidden patterns for new applications and within existing accounts. Tip-offs to fraud might include application anomalies, unusually high purchases of popular items, or multiple accounts being opened in a short period of time with data in common.

3. Leverage external consortium data with velocity and pattern detection to be alerted to suspicious behavior by an applicant at other organizations. With 3rd party velocity and pattern detection alerts, your organization will detect suspicious activity that would have otherwise been missed.

Equifax worked with a financial institution to help mitigate deposit account fraud. In this case, the existing false positive rate for the financial institution was 53:1. The Equifax fraud solution was used to isolate the most important attributes. The result was a reduction in the false positive rate from 53:1 to 15:1 or a 72% improvement. Based on industry averages and by including velocity and pattern detection alerts in their account opening processes, the financial institution is on track to save $700,000 dollars a year.

4 | **Four variables drive your Big Data view.** The “four V’s” of Big Data will determine the effectiveness of a data asset for fraud control:

- **Volume**—how much data is involved.
- **Variety**—the types of structured and unstructured data used by the application, such as credit files, utility records, or even Facebook posts.
- **Velocity**—how fast and frequently the data will be processed by an application. You can’t waste time massaging or cleansing data that’s needed for time-sensitive, real-time processes.
- **Veracity**—the data’s accuracy. Can it be verified? Do you trust the data as an effective, predictive element of your fraud decisions?

The more experience a solutions’ provider has with the four V’s, the more you can trust the predictive power of their Big Data.

5 | **Data is a raw material, not a finished product.** Ask probing questions about a Big Data provider’s volume, variety, velocity, and veracity.

- Find out what types of data are available and match them to your strategic objectives. Look for an extensive depth and breadth of services based on public and private databases, such as utility payments, credit files, income and employment verification, cell phone numbers, addresses, social security numbers, IP address, device location, and much more.
Leveraging Big Data

- Determine what applications need real-time decisions, and which data sources can meet these high-velocity requirements.
- Ask if the data is structured or unstructured. Unstructured data, such as text, images, and video extracted from social media, can deliver unique insights—but only if the data can be efficiently mined for relevant information and then converted into a form for predictive analysis.
- What is the Big Data provider’s track record in building data attributes, developing models, and delivering measurable results for other financial institutions.

6 | **Consortiums are the gold standard of Big Data.** Some industries, including financial institutions, contribute valuable information to central repositories. Hosts of the repositories capture petabytes of data from consortium members and make the information available to authorized parties. As the host for several industry-leading consortiums, Equifax is in a privileged position to access deep, rich consortium data to help combat fraud.

7 | **New pattern detection tools add heavy firepower to the fraud fighter’s arsenal.** Certain patterns of activity are indicative of fraud—and the patterns are hard for fraudsters to hide. For most credit unions, the ability to spot fraud patterns has been limited to what they can detect within their organizations. External velocity and behavioral pattern detection tools, which are getting much more sophisticated, can alert fraud teams to suspicious schemes that are in progress elsewhere.

8 | **Discreet measures avoid friction with good consumers.** According to researchers, fraud managers spend more than half of their budgets on costly manual reviews of false positives. Used in conjunction with pattern detection tools, passive techniques can pull through good applications quickly with minimal false positives and revenue loss. Passive checks operate in the background, without negatively impacting the member experience. A best practice is to waterfall between multiple passive checks before actively engaging with the consumer to verify if they are indeed who they say they are.
Fraud keeps changing—and so do the countermeasures. Financial institutions need to constantly upgrade the tools they use to stop fraud without interfering with the flow of “good” account applications and transactions. Data providers are responding with new tools and techniques that combine Big Data concepts and mammoth computing power to fight fraud. Here are several examples:

- **Proprietary keying technology** is now being used to link and consolidate records from hundreds of millions of consumers. Unique identifiers or “keys” to every consumer help discern their true identity despite variations in the data. These solutions can dramatically reduce false positives.

- **Voiceprints** and other forms of biometrics are gaining traction as anti-fraud measures.

- **Device identity tools** that track phone settings, model information and location, and even history on previous possible fraud, serve as good proxies for personal identifiers.

Big Data can do double-duty for financial institutions. Tough regulatory requirements require lenders to perform many checks before issuing credit to any individual. These verification processes typically reside in account opening and other front-line sales systems. Consequently, credit unions have an opportunity to get “extra mileage” as they upgrade their regulatory processes to also improve their fraud prevention measures. A holistic view of the consumer helps improve regulatory compliance, reduce fraud and improve member satisfaction.

Summary
Fraudsters are continually developing new techniques to rob financial institutions of billions of dollars. Keeping up with criminals is a vast undertaking that puts Big Data concepts in the forefront of next-generation fraud management. When contemplating leveraging Big Data for fraud mitigation, be sure to look for a solutions’ provider that offers:

- Comprehensive data coverage from thousands of consortium members supplying millions of records daily

- The ability to add meaningful context to vast amounts of data through sophisticated recordkeying technology, analytics, scoring and attribute reporting

- The ability to deliver scores and attributes based on real-time data, reported timely by consortium members

RESOURCES