CHERRYDALE APPLICATIONS

White Paper

An Inside Job

Data Analytics in the Battle Against Small Business Employee Fraud

It's the silent scourge of small business. Trusted employees with their proverbial hands in the till, lining their pockets while the rest of the company wonders where the profits went. The schemes can run for years before being discovered, if they're discovered at all, and companies are seldom able to recoup all of their losses.

Known as occupational fraud to auditors and law enforcement agencies, frauds committed by a company's own employees can be exceptionally difficult to detect. The fraudsters are often in a position of authority with responsibility for the very security processes that they are circumventing. Small businesses, with fewer resources for prevention, are particularly vulnerable to these types of attack.

Fortunately, modern data analytics techniques are bringing business owners new tools in the fight against occupational fraud. Advances in machine learning are enabling the development of software that flags fraud indicators earlier and more reliably than ever before. In the right hands, these tools can be implemented very affordably, giving small businesses access to the same fraud-fighting methodologies in use by the world's largest banks and insurance companies.

The Value of Proactive Analytics

The great majority of frauds are discovered by passive or backward-looking means. According to the Association of Certified Fraud Examiners (ACFE), a full 40% of frauds are revealed by whistleblowers, with internal audit and management review accounting for 15% and 13% of detections respectively. Meanwhile, only one-third of businesses even have proactive anti-fraud data analytics programs in use.

The potential benefits of proactive measures are huge. The longer a fraud scheme goes undetected the costlier it will be. The simple passage of time enables the perpetrator to divert more funds. Even more significant is the fact that schemes grow larger over time as employees become emboldened and more sophisticated in their exploitation of vulnerabilities. Frauds detected within 6 months have an average loss of $30,000 while frauds that go undetected for 5 years will see an average loss of $715,000.

Pro-active measures are strongly associated with a substantial reduction in the severity of fraud, primarily because they detect the fraud more quickly. Frauds discovered by IT controls and surveillance have average durations of less than 6 months, compared to frauds discovered by tips which have an average duration of 18 months.

Overall, proactive data monitoring and analysis are associated with a 37% reduction in fraudulent activities, with a 52% reduction in loss and 58% reduction in duration when frauds do occur.

Types of Fraud

Wherever money and other assets move through the organization, the possibility for fraud exists.

Check and payment tampering schemes are among the costliest frauds faced by companies. In these frauds an employee either creates a new payment to themselves or an outside co-conspirator, or alters an existing payment. The ubiquitous nature of

electronic transfers in modern systems has created an explosion of new opportunities for asset misappropriation.

Vendor billing fraud occurs when an employee establishes a fake vendor in the system and then proceeds to invoice the company for products or services that were never received. The payments, of course, eventually land in the accounts of the fraudster. In related schemes, a genuine vendor is a co-conspirator, participating in overcharging and fraudulent billing while sharing the spoils with the corrupt employee.

Payroll fraud takes many forms. Employees with access to the payroll system can increase their salary or hourly wage. Other types of payroll fraud do not require access to the system. Hourly employees can report hours that were not actually worked, and commissioned employees might report sales that did not occur. While individual incidents of these types of fraud tend not to be as costly as in some other categories, they are quite common and therefore impact the bottom line in aggregate.

Profile of a Fraudster

Bad actors can be found across the entire workforce, from entry-level clerks to the executive suite. In fact, opportunity would appear to be the most significant factor in the role of fraudsters in an organization. The staff of accounting and operations departments are some of the most likely to be engaged in fraud, followed closely by company executives and the sales team.

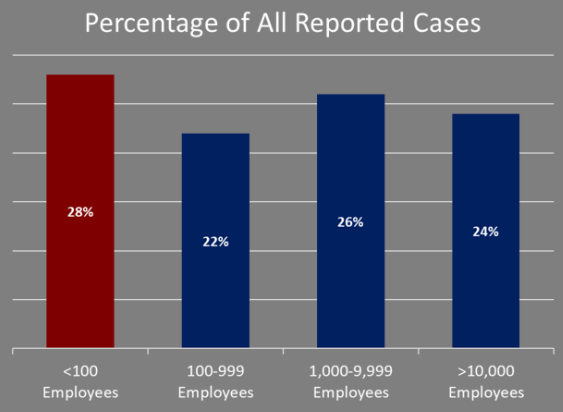
Although almost half of fraud cases involve non-managerial staff, the dollar losses in cases involving employees in positions of authority eclipse those of the work-a-day staff. There are many explanations for the greater loss experienced when managers and executives perpetrate fraud, most of which are reasonably obvious. Those in positions of authority frequently operate with less oversight, especially in smaller companies which rely more on trust. Authority figures have easier access to greater assets and many times are in positions which enable them to override existing fraud controls.

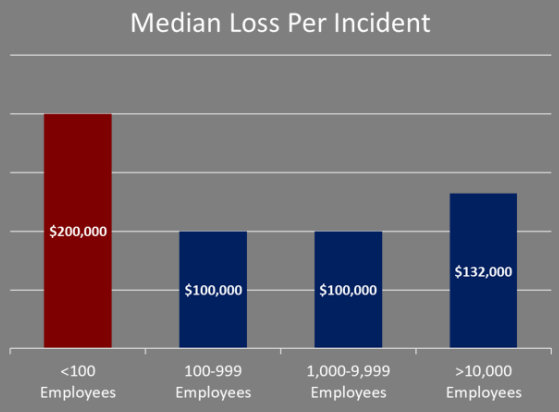
While there are no demographic indicators of fraud, there are nonetheless warning signs. ACFE has identified six red flags of fraud. In 85% of fraud cases reported, the perpetrator exhibited at least one red flag:

- Living beyond their means
- Facing financial difficulties
- Unusually close association with a vendor or customer

Small Business Impact

Small businesses are hit particularly hard by fraud. Businesses with fewer than 100 employees typically have fewer resources to prevent fraud and fewer resources to go after fraudsters once the crime is discovered. The result is fraud schemes that last longer and cost more than any other business segment.





- Control issues and unwillingness to share duties
- Divorce and other family problems
- "Wheeler-dealer" attitude

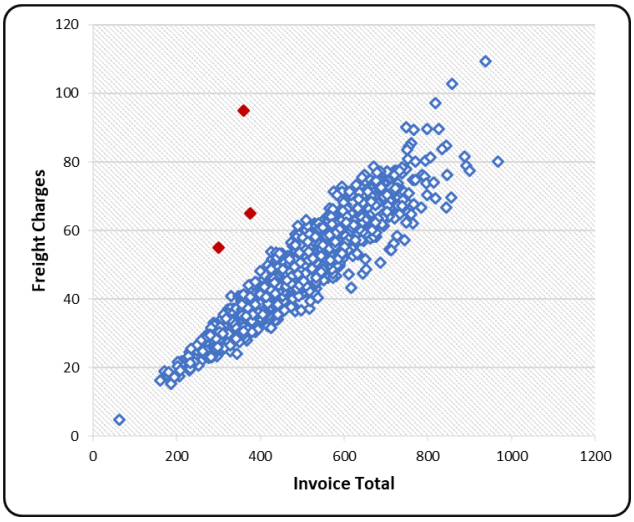
Analytic Approaches to Fraud Prevention and Detection

Modern data science provides a wide range of techniques to be applied as part of a comprehensive anti-fraud program. Analytic approaches are generally broken out into three major categories according to the underlying analytics as well as the nature of the data being scrutinized.

Rule-based algorithms take known patterns of fraudulent behavior and implement flags in the workflow based on those patterns. An example of such a rule would be to flag an invoice with an amount greater than $10,000 within one-month of a vendor address change.

Rule-based systems are an important first line of defense and can be very effective against the identified patterns. However, these systems also have weaknesses. By their nature, the suspect behaviors must already be known; rule-based systems do not independently identify new patterns. Rule-based systems also must be evaluated periodically, and the rules manually updated based on newly identified patterns and changes in the business environment. Finally, once fraudsters know the rules, the rules can be defeated.

Anomaly detection, also known as outlier detection, uses standard statistical methodologies to find transactions and other data that fall outside the normal range. For example, if most supply orders are between $300 and $500, an anomaly detection system would be expected to flag a $3,000 supply order. In contrast with rule-based systems, it is not necessary to know in advance which patterns are suspect. Anomaly detection systems are straightforward to implement and can be very effective.



Anomaly detection algorithms sift through thousands of data points to find outliers for further investigation.

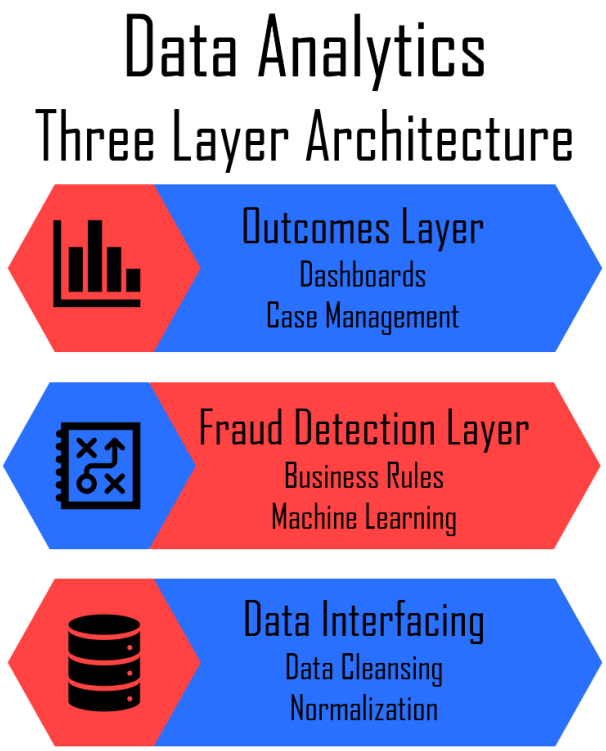
Predictive analytics uses advanced machine learning algorithms to identify the attributes of fraudulent behavior. Fraud models are trained by comparing data associated with fraudulent activity against data associated with normal activity. Predictive analytics can identify subtle, complex patterns across data sets that would be difficult or impossible for human auditors to stop. The fraud models produced by this process have the added benefit that they can evolve over time as fraudulent patterns of behavior change.

Implementing and Integrating Data Centric Fraud Detection

There is no plug-and-play solution for fraud detection and prevention. An effective system must be tailored for an organization and integrated with the existing IT architecture. The need for tailoring and fine tuning is especially pronounced for smaller businesses.

In smaller businesses existing data management systems tend to be less mature, often including key data housed in spreadsheets and other ad hoc solutions. Smaller businesses also tend to have fewer data sources and more sparse data.

A fraud detection and data analytics system is a three-layered architecture: the data handling layer, the detection layer and the outcomes layer. Each layer has its own implications for implementation.



Preparing an organization's data for analysis is almost always the most challenging aspect of the implementation. The first step is to inventory the data to determine what is available and where it is housed. Many algorithms rely on real time, or near real time, data, and custom scripts are required to normalize data and bring the data into the analytics system.

Once the data has been identified and normalized, and a plan made to interface with the various data sources, the fraud detection layers are implemented. In the best, most effective systems, data scientists work closely with business process experts to develop rule-based algorithms and lay the foundations for machine learning predictive models. It is important to develop as many models as possible. Machine learning algorithms perform better when many smaller models using different strategies are created.

The outcomes layer includes alerts and stops that are integrated with the existing IT workflow, along with custom dashboards and reporting. Again, success here depends on a close working relationship between the system architects and the business process owners. Critical, informed decisions must be made regarding anomaly thresholds and how the infrastructure will respond to a perceived threat. Likewise, dashboards and other reporting tools must reflect the needs and culture of the organization in order to be effective.

Cherrydale Applications

In business for more than 15 years, Cherrydale Applications is the ideal vendor to help your small business implement state-of-the-art solutions for fraud detection and prevention. Our staff is made up of experienced systems engineers, developers and analysts. Our clients include numerous government agencies, non-profits and businesses just like yours. More importantly, we are data science experts. Our leadership is passionate about implementing machine learning techniques to help our clients make sense of our data driven modern world. We manage an ambitious continuous education agenda; our entire staff routinely participates in training and education activities with some of the world's finest academic institutions to ensure we can keep you and your team on the cutting edge.

CHERRYDALE APPLICATIONS

11295 Glen Falls Parkway
Suite 300
Arlington, Virginia 20009
703-201-3131
contact@cdapps.com