The Secret Weapon in the Fight Against Fraud

June 2012

Instaknow.com, Inc.
1001 Durham Ave., Suite 201
South Plainfield, NJ 07080
908-650-9598 www.instaknow.com

TABLE OF CONTENTS

The Secret Weapon in the Fight Against Fraud

Introduction

The cost of fraud is staggering and is expected to increase dramatically in the coming years. As businesses and individuals continue to face tremendous financial pressures, more people are turning to fraud out of sheer desperation, costing businesses untold sums of money, with many victim organizations totally unable to recover.

Against this backdrop fraud investigators are working harder than ever to stop frauds in their tracks. Unfortunately, ever increasing case loads, a widening array of fraudulent crimes, and the constantly shifting technological landscape are making it harder to keep up. Each case that goes undetected can cost hundreds of thousands of dollars – if not millions – and there is an urgent need to add new weapons to the fraud investigator's arsenal.

Fraud examiners can be a diverse lot – from CPAs to forensic IT specialists – yet across the board, their greatest asset is their keen investigative eye. Therefore, the key to combating fraud is giving examiners the data they need to put that investigative eye to work in order to stop frauds and protect their clients.

Unfortunately, global economies are now forcing many organizations to cut back on, or cap the number of, investigative resources, and investigators are being challenged beyond their capabilities with mounting case loads and fewer resources. In addition, organizations are continually seeking ways to reduce costs and increase productivity. One well-known approach to achieving these goals is to automate repetitive processing and eliminate manual touch points. Elimination of unnecessary human intervention in the repetitive processes of fraud investigation can: reduce the need for hiring and training additional investigative staff as the workload grows, lower operational costs as productivity improves, and foster a more efficient and flexible investigative scenario.

Fraud on the Rise

Desperate times often bring about desperate measures, and, sadly, the enduring recession has pushed more and more individuals to turn to fraud out of sheer desperation. In May of 2008, Network, a U.S. firm that runs compliance and corporate-governance hotlines for about half the Fortune 500, reported that fraud-related calls amounted to 21% of all reports in the first quarter of the year, up from 14% in the same period in 2007. That represented a 50% increase in the number of cases reported – just months after the recession began.

While there was clearly an immediate jump in the level of fraud following the financial collapse, the increase in fraudulent activity, like the financial slump, has been enduring. In the ACFE's 2010 Report on Occupational Fraud, it was found that more than 55% of fraud examiners had

seen an increase in the number of cases over the previous year, and a staggering 88% expected to see an increase in the following year.

Sadly the current financial crisis creates a perfect storm to cultivate fraud. As all fraud experts know, breaking the fraud triangle of motive, opportunity and rationalization is the key to deterring fraud. With the current recession dragging into its fifth year, more individuals are finding their mounting money problems to be irresistible motives for committing fraud. At the same time, given the choice between defrauding an employer, insurance company or other "faceless" institution and losing the family home, many are finding all the rationale they need. Finally, the increasing financial pressure is forcing businesses to lay off employees and neglect important internal controls, providing opportunity to increasingly desperate fraudsters.

With the possible breakup of the Euro, an economic slowdown in China, and stubborn unemployment in the US, it looks as though the world has many years of financial hardship ahead. These hardships will undoubtedly be accompanied by an increasing case load for fraud examiners. This increasing case load, coupled with tightening resources and the constant need to produce more results, places even greater emphasis on the need to equip fraud examiners with a new set of tools to combat ever growing fraud.

The Cost of Fraud

It is difficult to understate the cost of fraud. The ACFE estimates that the typical organization loses 5% of its revenue to occupational fraud alone, adding up to $3.5 trillion lost globally each year. In terms of Gross Domestic Product (GDP), that would make occupational fraud the 5th largest country on the planet, just behind Germany and well ahead of France, Brazil and the United Kingdom.

Health care fraud also accounts for massive losses in the US. The National Health Care Anti-Fraud Association estimates that fraud accounts for between 3% and 10% of overall health care spending, or between $51 billion and $110 billion annually. Credit card fraud takes a massive toll as well. It is estimated that 7 cents of every $100 in credit card transactions are lost to fraud, accounting for nearly $1 billion each year.

While the cumulative cost of fraud is massive, the cost of individual fraud cases is significant as well. The average fraud case costs businesses $140,000, with 20% of cases costing more than $1 million. The cost combined with the fact that small businesses are disproportionately the targets of fraud mean that nearly half of all victim organizations never recover from the loss, having to shut their doors forever.

Although there are no exact figures on the number of jobs lost due to fraud, given the massive scale of fraud it seems reasonable to assume that tens of thousands of jobs, if not hundreds of thousands, are lost each year due to fraud. The human toll taken by fraudsters makes the job of

the fraud examiner all the more important, and the need to equip them better all the more pressing.

Preventing and Investigating Fraud

While detecting fraud once it occurs is an essential to any business, it is obviously best to prevent it before it happens. There are numerous new ways to prevent fraud before it happens, and there are a number of tried and true methods that are still essential for preventing fraud. But in the new world of digital and social media, even these tried and true methods can be executed in new and innovative ways.

Vet Employees

The first – and perhaps most important – step to preventing occupational fraud is to know who you hire. While it may seem obvious, a failure to properly vet your employees can have disastrous consequences. In May of 2012, it was discovered that newly appointed Yahoo CEO, Scott Thompson, had lied on his resume about college degrees he had never actually received. The ensuing fallout forced Thompson from his office, and was a huge embarrassment to the already embattled company. Just imagine the number of HR managers who must have failed to vet Thompson's resume throughout his career before he was able to make it to the coveted C suite.

In addition to an education and employment review of any new employees, criminal background checks and financial review should be performed for any employees who will be in control of significant assets. Also, there are now companies that can vet employees' social media profiles for potential red flags. While there has been quite a bit of controversy regarding employers' use of social media searches to vet potential job candidates, it is increasingly understood that what people put on the Web is fair game for prospective employers.

One pitfall of relying on background checks to prevent fraud is that the vast majority of occupational fraudsters have no previous record of fraud in their criminal or employment history. According to the ACFE, 87% of occupational fraudsters had never been convicted of a fraud related crime, and 84% had no record of fraud related punishment or termination in their employment history.

Use Tips to Prevent and Catch Frauds

Tips have long been an extremely effective way to both prevent and detect fraud once it occurs. Tips are the most common way that occupational fraud is prevented and detected, and the ACFE reports that companies with robust anti-fraud training programs detect frauds faster and experience smaller losses due to fraud.

Tips can be used to prevent and detect all kinds of fraud as well. The Coalition Against Insurance Fraud, an organization that brings together insurance companies, consumer groups and government agencies, has launched a public service campaign aimed at deterring fraud and encouraging citizens to report fraudsters. The Coalition's public service announcements and website make citizens aware of the cost of fraud both in terms of dollars and cents, and possible jail time. Many of their ads encourage consumers to call in with tips if they become aware of a potential fraud, lest they get swept into the scheme themselves and end up in a jail cell.

Use Technology to Prevent, Detect, and Investigate Fraud

There are now a number of companies deploying technology that can detect suspicious activity and flag it, helping to stop a fraud before it can come to fruition. These technologies are particularly useful for companies that have a large number of transactions being processed on a daily basis. The technologies monitor numerous transactions and metrics throughout an enterprise in order to detect suspicious activity and bring it to the attention of fraud prevention teams. Fraud detection software can be useful for detecting multiple kinds of fraud, however, the various software packages are often expensive and can be difficult to implement.

Automation Technologies: SOA and BPA

Two standard technology solutions in use today are Service Oriented Architecture (SOA) and Business Process Automation (BPA). There are many drawbacks to these solutions in automating the process of fraud investigation and simultaneously achieving system integration. Some of these drawbacks include:

1. Re-engineering individuals systems in such a way that they will “talk” or interact with each other can be challenging. Usually this involves invasive techniques, such as re-programming, adding a connecting application, or involving a “middleware” solution to enable translation and information exchange. Considering the cost of additional applications plus programming, these methods can become expensive fairly quickly.

2. Hard-coded solutions are inflexible and require significant time, cost and effort to keep them in synch with evolving business requirements.

3. Perhaps the biggest drawback is the limited nature of SOA and BPA solutions. They are not extensible to many sources of information routinely used by the investigative staff, including: external Web sites, e-mails, attachments, Excel, Word, PDFs, Legacy mainframes, AS400 systems etc. These are simply NOT amenable to the SOA approach because their content and data formats cannot be standardized. Much of the work of investigators involves compiling Web related information in combination with data from internal and external systems and databases; therefore, highly-structured and static integration solutions just don’t work well for automating the process.

4. Any disruption to existing systems is highly undesirable, especially with the need to achieve respective divisional or departmental goals. In many organizations, the business operations staff are fully trained and well versed in the existing systems.

Artificial Intelligence

Artificial Intelligence (AI) technology can be the answer without the drawbacks of SOA and BPA. How great would it be if automation could be accomplished by "teaching" an AI e-robot to do what the investigators do with regard to data access, matching and retrieval, and by instructing the e-robot to return the results to the investigator? It would be a great saver of time, effort and costs. The e-robot could help to detect fraud early on – being much faster and more accurate than a human – and to prevent payouts on the fraudulent claims that were detected early. It could help to eliminate investigator burn-out and free up the investigator to do the important "other" stuff that can be performed only by the investigator, including the analysis and conclusion.

The fraud investigator typically follows routine or semi-routine processes throughout the investigations. These routines are usually documented as Standard Operating Procedures (SOPs) or may simply be informal "best practices" adopted by the team. For example, the analysis of insurance claims may include matching a given claim to internal and external databases, applying filters to weed out false positives, on a "match" emailing adjusters with relevant details, populating an internal database with the details, and executing a review process with higher level management. This is an example of a repetitive, but easily documented claims investigation process with little variation, requiring access to various data sources and systems, and requiring manual scan and data entry. This entire process can be automated using an application of Artificial Intelligence.

A New Tool for the Fraud Investigator

Even though there are countless ways to enhance fraud prevention and detection, the role of the fraud investigator will always be essential to any business. With fraud on the rise, it will be increasingly important for investigators to do their jobs more effectively, efficiently and with greater accuracy. In order to do this they will need new tools that can handle the volume and complexity of today's fraud.

For most fraud investigators much – if not the majority – of their time is spent gathering data. And while the advent of electronic databases has provided a wealth of data that was previously unavailable, it also means there are now dozens of data sources to identify, compile and organize before the real work of analyzing and investigating can begin. This investigator-intensive process is exacerbated by an increasing case load. As examiners have more and more data to gather and process, the tedious manual work is leading to burnout and decreased productivity.

What if all that intensive, repetitive manual work could be eliminated? What if fraud investigators could spend all their time using their expertise as investigators as opposed to spending countless hours compiling reams of data? Enter Human Intelligence Automation®, a powerful Artificial Intelligence platform.

A New Approach: Human Intelligence Automation®

Human Intelligence Automation® (HIA) is a real-time process automation platform developed by Instaknow.com, Inc., a leader in application of Artificial Intelligence. HIA overlays new integrated business processing on top of current systems and data sources WITHOUT changing them. This approach to deploying the benefits of process automation is far more cost-effective and time-saving than SOA and BPA.

Powered by patented Artificial Intelligence, the HIA platform watches and remembers business case examples shown by an authorized user. All system/data interactions used in the examples are automatically saved for future automated execution of similar business transactions.

Just like a trained user, the platform can interact in real-time with any number of hard-to-integrate data sources, including Web sites, portals, documents, e-mails and attachments – *without* needing a formal programmatic interface such as XML/SOA. Using friendly "point-and-click" graphical interfaces, any level of business intelligence rules and decisions can be added across the self-learned multi-system reads/updates to intelligently execute the automation based on run-time conditions. The platform automatically detects, reports on and handles all processing exceptions according to desired rules.

Working like an automated, expert user, HIA can process thousands of complex business transactions in minutes, rather than in the number of days that humans would take, while following every rule and policy you ask it to follow. Built-in "fuzzy matching" capabilities allow for correlation of non-exact information across systems in a highly reliable manner. Audit trails are kept as desired and existing security policies of all systems are honored automatically, including digital certificates, passwords, and LDAP based roles. The processing can happen as desired: triggered by users, invoked by other authorized systems on demand, according to schedules or in a continuous mode until stopped by an authorized user.

The technology performs the "human-like" processing using existing application front ends, thereby overcoming a major flaw in "stateless" or "single-request, single-response" protocols that include XML, SOA and EDI, which have no memory of any prior interaction with any system. By automating interaction with an application screen, the technology can enter partial data in several application windows just like a human user, based on application messages returned (e.g. "Please provide data for highlighted fields"), look up that additional data from

other sources or applications and then complete the screen data entry in all systems. Such electronic "swivel chairing" across multiple data sources is required for many complex business transactions and is impossible using conventional technologies.

Uniqueness

Combining all capabilities of a programming language AND those of a well-trained, expert user, the "overlay" process automation approach is distinctive because it:

1. Does not require programming: It programs itself automatically from the external system interactions you choose to show, adapting to each system's unique data content, format and navigation. You can also add cross-system business decisions (business rules) via a point-and-click graphical interface to make the automation as intelligent as your most expert business users.

2. Easily links with normal data sources – Databases, SOA, EDI, APIs, etc. – as well as with hard-to-integrate sources that no other technology can link – Web sites, portals, SaaS, Excel, Word, PDF, e-mails, attachments, mainframes, AS400 and other legacy systems.

3. Executes electronic "swivel chairing" across multiple and diverse applications with user-like intelligence for real-time reads and updates, including multi-parameter "fuzzy matching" intelligence to find the same or similar information with the reliability of a trained user.

4. "No Change to Existing Systems" process automation approach results in avoidance of a huge amount of technical analysis, design, coding, testing efforts and costs inherent in SOA and BPA. This type of automation frees up technology staff and budgets to deliver other new, strategically valuable business systems.

5. Built-in parallel processing and multi-server-fail-over allows for mission critical, high-volume operations.

Business Benefits of a Hyper-Connected Solution

- Faster business processing at reduced operating costs.

- Ability to leverage value of, and investment made in, existing systems without costly technical changes.

- Seamless integration of vital information and functions among internal and external partners, customers and suppliers.

- Reduced manual data lookups, research, data entry, errors, corrections, re-do – and customer complaints – resulting in higher quality and performance. Frees up staff for higher-value tasks.

- Drastically reduced: system integration/development costs and traditional delivery times.
- Enhanced product/service offerings brought to market faster than before.
- Solutions to business problems previously considered too costly, time prohibitive, unrealistic or impossible to achieve.

Typical Scenarios Where the HIA Platform Provides Rapid Payback

- High transaction volumes spanning fragmented systems with heavy manual intervention in business flow.
- Market demanding faster response, and the current manual business process is too slow.
- Needing new, innovative business solutions to market to gain competitive distinction and market share.

e-Assistant for Fraud Investigation

Based on the HIA platform, the e-Assistant for Fraud Investigation (e-AFI) is a fraud investigator's best friend. This automated technology eliminates the tedious work of searching for and compiling investigative data, allowing investigators to spend their time on the essential work of analyzing the data and taking action.

e-AFI works by learning from investigators as they go through their usual process of gathering and compiling information. Similar to a new investigator in training, e-AFI learns by "observing" how to extract and compile data from a virtually unlimited number of sources – the very same ones the experienced investigator uses – and eventually takes on all the tedious manual work of data collection. Once trained, it can deliver all the requisite data straight to an investigator, allowing the investigator to do the essential work of reviewing data and closing cases.

e-AFI's patented fuzzy matching capability uncovers fuzzy correlations among a variety of categories, including, but not limited to: people, vehicles, addresses, claims, convictions, warrants, educational background and career specialization.

It can search an unlimited number of databases quickly and accurately without the burn-out factor associated with human fatigue. It learns to discover, correlate, update and publish real time data across enterprise systems, websites, search engines, portals, blogs, mainframes, emails, Excel, Word, PDFs, databases – and more.

The many benefits include:

- Substantial savings through reduction in fraudulent payouts.
- Ability to process additional cases without having to hire additional staff.

- Improved investigative accuracy and throughput.
- Interface with enterprise systems, including Case Processing and Case Management.
- Real-time capabilities that support informed and timely decision-making.
- Automatic request/review of ISO reports, background checks, and financial information.
- Auto-refreshment of old data throughout the case lifecycle.
- Reduced learning curve for newly hired investigators.
- Automatic preparation of standard case reports, audit trails and correspondence.
- Fast deployment and immediate return.

Capabilities

Imagine if an investigator could increase the number of claims they process and close by 200% - 500%, and more! e-AFI does just that. It gives investigators the advantage of new, powerful, cutting edge enhancements to research capabilities along with the best of those currently available.

In identifying suspicious claims, it scrutinizes the claims against a predefined list of red flags that have been found to point to possible fraud. Claims that fail this initial test will be set aside for further investigation. In addition, it can easily interface with statistical analysis and business intelligence systems, which may be used to analyze claims for other factors that suggest fraud. The suspicious claims identified statistically would be added to the list set aside for further investigation.

Once a claim is identified as suspect, the technology can automatically interface with Claims Processing and Case Management Systems, and undertake the next steps normally handled by human investigators, including:

- Requesting / reviewing ISO Reports, vehicle histories, real estate property histories, background checks, and financial information, and compiling relevant reports.
- Composing / sending emails requesting additional information from other insurance companies with regard to claims identified in the ISO Reports.
- Composing emails and / or letters requesting medical information from doctors for claims involving injuries.
- Automatically processing replies to emails according to Case Management Procedures.

The Artificial Intelligence-based e-AFI drastically reduces turnaround time through its ability to automatically and immediately start the lengthy process of acquiring additional data. Investigators need no longer suffer through tedious research; instead, they will be provided with information automatically collected, categorized, and ready to be reviewed.

Artificial Intelligence gives investigators the ability to train an electronic assistant that will free them from tedious, error-prone data gathering and give them the ability to focus on those functions that only a human investigator can perform, including the final decision with regard to potential fraud. The Artificial Intelligence used to support e-AFI has earned four (4) US patents for the "intelligent" capabilities that serve investigators well.

About Instaknow.com, Inc.

The information presented in this white paper with regard to Human Intelligence Automation® and the e-Assistant for Fraud Investigation reflect the proprietary, Artificial Intelligence based technology of Instaknow.com, Inc. Instaknow's multi-patented HIA platform replicates and improves on human knowledge work. U.S. patents include: 6732102, 7073126, 7437342 and 7979377.

Instaknow is a leading edge visionary of Information Technology (IT) software and services based on Artificial Intelligence. Founded in 1999, Instaknow serves major clients worldwide, including financial institutions, manufacturers, governments, military organizations, service companies, and more.