JOURNAL OF ADVANCED ANALYTICS
IQ
3Q 2012

FRAUD PREVENTION

Learn how leading organizations and institutions prevent fraud in the digital age.

WHAT'S IN THIS ISSUE

Banks, insurance companies, health care organizations and government entities are all seeing an increase in the incidence and sophistication of fraud, waste and abuse activities, fueled in large measure by the financial turmoil gripping the world's economy. To fight fraud effectively, organizations must continually improve the monitoring of customer behavior across multiple accounts and systems. Combining technologies like business rules, anomaly detection, predictive and learning models, and social network analysis allows organizations to predict fraud with astounding accuracy and take steps to prevent fraud from occurring.

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 60,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW.®

JOURNAL OF ADVANCED ANALYTICS
IQ
3Q 2012

Editorial Director
Mikael Hagstrom
mikael.hagstrom@sas.com

Editor-in-Chief
Alison Bolen
alison.bolen@sas.com

Managing Editor
Anne-Lindsay Beall
anne-lindsay.beall@sas.com

Copy Editors
Amy Dyson
Chris Hoerter
Amy Madison
Trey Whittenton

Editorial Contributors
Michael Dowding
John Geurts
Amitava Ghosh
Eva Gustin
David Hartley
Graham Kemp
Eva (Hyun-min) Kim
Julie Malida
Marcie Montague
Mark Moorman
Ramesh Subrahmanyam
David Stewart
Amar Vohra
Katrina Wakefield

Art Direction
Brian Lloyd

Photography
John Fernez
Steve Muir

sas
THE POWER TO KNOW.

FRAUD IS EVERYONE'S PROBLEM

You can put a stop to it with predictive capabilities and a holistic framework for fraud

Mikael Hagstrom Executive Vice President, SAS

In March 2012, Nikolay Garifulin was sentenced to two years in prison for his part in the Zeus cybercrime spree that defrauded banks for hundreds of millions of dollars and infected more than 2,400 computers around the world. Garifulin himself was just one part of a franchise of fraudsters that used the Zeus malware, which allowed an imposter to capture personal information from the computers it infected. Garifulin was convicted of stealing more than $3 million.

As a point of comparison, Thomas Woodward was sentenced to 10 years in prison for robbing $4,267 from a bank in Massachusetts. While Garifulin's sentence was considerably lighter, the most interesting thing, frankly, is that he was sentenced at all. Most fraud and abuse activity goes untried. In many cases, it goes undetected. Typically, the cost of fraud is passed on to customers, constituents or owners in the form of higher fees, increased taxes or lower margins.

What the Zeus cyberattack and others like it teach us is that fraudsters are prevalent, active, coordinated and technically skilled. In our efforts to open our organizations to Web commerce, we have created new concerns for the protection of our funds, information and customer data. Cyberattacks will continue, and some believe there may even be a crippling attack in the near future, which could lead to a crisis with even more devastating impact than our current financial crisis.

It doesn't have to be this way. In fact, the digital age has more to offer the defenders than the offenders. With analytics, you can move frontline fraud management from detect-and-defend to prevent-and-eradicate. While many still engage in an arms race of rule-based detection to lock offenders out, this issue of the Intelligence Quarterly highlights those who analyze big data to neutralize organized crime and to prevent the opportunistic seeker from making the wrong choice.

OWN AND UNDERSTAND THE FRAUD PROCESS

Fraud is everyone's problem and cannot be ignored. Its cost is trickled down through the economy, putting pressure on those of us who are honest and forthright in our dealings. For many people in government and business today, it is difficult to think like a fraudster, but just one abusive person in 100 can make all the difference. These social vampires exist, and they are collaborating.

Too often, I see organizations with limited fraud prevention, such as a black box system – or worse, none at all, other than a firewall. As more and more doors open through growing online services, it is imperative that your organization's fraud prevention efforts keep up.

Fortunately, high-performance analytics, coupled with big data, is available to organizations susceptible to fraud and abuse, helping them manage and prevent these activities. Many organizations around the world are using data and analytics to build fraud prevention technologies that save money, protect corporate reputation and reduce process costs. It is important not to lock yourself into a black box fraud solution built on some historical perspective of fraud. Instead, success comes when you can own and understand the fraud process and respond to the ever-changing dynamics of fraudsters.

A HOLISTIC APPROACH TO FRAUD MANAGEMENT

Fraud has often been compared to a balloon, since pressing on one place in the balloon just forces the air into another. Like the air, fraud moves from one inefficient process to another within an organization.

When we stop transactions or decline claims without prosecuting the person responsible and without fixing the inefficient processes to begin with, we are training fraudsters to just keep trying. This cycle teaches people who are bent on criminal behavior how to attack your system. Many times you need to follow the suspect, rather than just disconnecting, in order to convict and eradicate. Indeed, business changes can often have a big impact on your fraud exposure, making it essential to be active and elastic in fraud prevention – not just fraud detection – and to use technologies that will grow as your needs grow.

A fraud framework is a complete set of processes that access and integrate data, produce alerts, provide holistic reporting, control workflows and case management, and learn from past experience to become – and remain – effective.

Organizations from the public and private sectors alike are finding this fraud framework valuable. We introduce you to some of these organizations in this issue, including:

- The Swedish tax office, where fraud prediction has changed the entire tax collection process – and improved the public's perception of paying taxes (Page 20).

- LA County, where analysis of social networks, combined with other fraud predictive methods, has prevented millions of dollars from going to childcare fraud rings, money that would otherwise have been stolen from the defenseless with the greatest need (Page 7).

- Hyundai Marine & Fire, whose fraud prediction and prevention programs help protect the company's most valuable customers (Page 13).

Also in this issue is an explanation of how other tax revenue offices use a fraud framework to monitor value-added-taxes (VAT) for fraudulent activities, such as carouseling, by engaging in preventive services that help reduce errors in tax returns. Banks, health care providers and welfare organizations have all used this framework to protect themselves from fraudulent and abusive behavior.

Along with accurate detection, these organizations find value in a holistic approach to fraud management. Combining technologies such as business rules, anomaly detection, predictive and learning models, and social network analysis can predict fraud with astounding accuracy. Using analytic models like neural networks, these systems become learning systems that get better over time, and they become more dynamic by accounting for evolving fraud activities and by using anomaly and social network models.

Fraud continues to be a major concern and that concern continues to grow. Currently, there are more white collar workers unemployed than ever before – and fraud is a white collar crime. The "fraud triangle" describes three factors present in fraud: motive, rationalization and opportunity. With a highly skilled unemployed population, these causal factors make for a trained, motivated and potentially desperate group of people. Add to that the Internet access available to so many people today and you have a toxic mix.

Most governments and organizations around the world are beginning to take this growing threat seriously. Now is your chance for your organization to aggressively pursue fraud prevention processes. I hope this issue of *Intelligence Quarterly* will motivate you to take that first step toward a better future.

online

Read Mikael Hagstrom's blog:
blogs.sas.com/mikaelhagstrom

As head of an expanding global team of 4,500 professionals in 48 countries, Mikael Hagstrom is passionate about providing a culture where innovation can flourish, resulting in market leadership for the organization and its customers. He leads SAS' Europe, Middle East, Africa (EMEA) and Asia Pacific regions, which account for 54 percent of SAS' 2011 revenue, or $1.47 billion.

FRAUD DETECTION IS MORE THAN COOL

On financial crime, capable guardianship and behavioral analytics

John Geurts Chief Security Officer, the Commonwealth Bank Group

You can't deny the cool factor of fraud prediction. Today, at the Commonwealth Bank Group, for those products and channels we monitor, we can reliably predict the likelihood of fraud activity for any given transaction before it is authorized. Not only that, but we can do it up to 250 times per second, get answers within 40 milliseconds of the transaction being initiated, without transaction sampling, and across multiple channels and products.

However, it is worth understanding the principles that formed the basis of how we got here and also ask, "Can we do more?"

Fraud in the banking industry is not just another cost of doing business that needs to be priced. It has its roots in crime, and we must defend ourselves against crime and misadventure. This can be a challenge in a complex technological age where the range of products and services has evolved to meet the needs and demands of our customers.

ARE YOU AND I PARTLY ACCOUNTABLE FOR FRAUD?

To truly understand the challenge, we can draw inspiration from research that pre-dates consumer e-commerce. Criminologists Lawrence E. Cohen and Marcus Felson introduced the concept of capable guardianship, which identifies the role we all play to address the three precursors to crime: motive, means and opportunity.

They contend that crime is normal and that it depends on the opportunities available. If the target is not protected, crime will happen. If this is the case, then our job in financial services is more difficult because we are not just protecting ourselves from criminals or hardened offenders. We must also protect ourselves from people who take advantage of an opportunity that we created by failing to provide capable guardianship.

As a provider of services, we must take accountability for fraud and use the resources we have available to anticipate, prevent, detect and respond to fraud if it occurs. Capable guardianship implies that we, as a key component in the chain of criminal behavior in banking, must invest both intellectually and practically in guarding everything within our power to protect.

PREDICTING WHEN FRAUD WILL OCCUR

Of course, the opportunities to commit fraud have changed with the advent of

WHAT IS A MULTILAYERED APPROACH TO FRAUD?

In building their fraud detection methods and models, firms are using all of the following approaches:

- Business rules. Individual rules score or define alerts based on intuition and general experience.
- Anomaly detection. Alerts are defined based on events that represent statistical deviations from normal or expected behavior.
- Predictive models. Full-scale statistical models establish alerts based on a risk score derived from event characteristics that are indicators of prior fraud incidents.
- Social network analysis. Alerts are based on the level of association (through shared or similar attributes) between the current event and individuals or accounts that are known or suspected of fraudulent behavior.

The choice of which methods to use often depends on the details of the application and institution. In general, there is a trend away from using business rules as the sole method for defining alerts, and a broader trend toward using all methods as needed.

technology. As systems and processes become more automated, we have an increased opportunity to implement systems and controls at appropriate places in the cycle to prevent and detect fraud.

Our key principle in detecting fraud is, simply, to stop looking for fraudulent transactions. That sounds counterintuitive, but it actually works.

Instead, our approach is to predict whether or not an event or transaction has occurred that will give rise to fraudulent activity, money laundering or other proscribed activities. This approach does not mean the end of transaction fraud rules, but they do have their limitations.

Events to watch include customer and network activities, account transactions or activities surrounding entire classes of accounts. In essence, we are looking for behavioral indicators of fraud or other activity.

It is important that we choose "the right time" to interdict a transaction of interest. We should not be seduced by the need to do everything in "real time" unless we need to, because real time is expensive.

For the Commonwealth Bank, fraud detection needs to be real-time, as we have a real-time core in our retail and business banking platform, and we seek to determine whether or not a transaction is fraudulent before it is authorized. On the other hand, an overnight batch is more appropriate for anti-money laundering obligations. Likewise, when detecting payments to sanctioned countries and entities, we can delay that transaction to make a decision later that day.

FRAUDULENT BEHAVIOR IS INCONSISTENT WITH NORMAL BEHAVIOR

The real difference that has emerged in our thinking in the past six years is that we stopped just looking for fraud at a transaction level and started looking for changes in our customers' overall behavior.

Criminals do not segment themselves by product or service or geography. What they are actually doing when committing fraud or laundering money is taking advantage of a weakness, more often involving a customer or the customer's data. The fraudulent act is a behavior that can be recognizable through advanced modeling techniques because we can anticipate that the behavior is sufficiently inconsistent with known normal behavior.

This change in our thinking, coupled with a desire to streamline a number of siloed, product-specific fraud detection platforms, led to the use of SAS®.

SAS had a longstanding relationship with the Group through credit risk and customer marketing analytics solutions. In fact, much of our early success in fraud detection was due to two skilled analysts from our marketing department who joined our team and developed our early lending and transaction fraud models. Their approach was to identify the range of data sources that would be required to build a behavioral profile of the customer.

SYSTEM REQUIREMENTS FOR FRAUD DETECTION

Beyond the increased possibilities presented by the behavioral analytics approach, how does the approach work from a practical perspective?

Based on a customer-centric model, consider this example: A customer withdraws money with a chip-enabled debit card at an ATM in her home city, lends a friend $50 using her mobile banking device and uses Internet banking to transfer funds to a third party from an IP address located offshore. The Internet banking transaction

is most likely to be fraudulent, and we must be able to pass a message back through our system to deny the transaction within 40 milliseconds or so.

Without a customer-centric fraud detection system, we likely would not be able to identify the transaction as fraud in time to stop it, and we probably would not even know it occurred until the customer complained some weeks later.

Fundamentally, fraud systems for commonly used retail products and channels must be linked to customer behavior, and we must have a good idea what "normal banking activity" looks like; otherwise, the opportunities to detect and prevent fraud are lessened.

This is not a trivial task. The efforts required to detect fraud, money laundering and other proscribed activities demand a disciplined approach and robust systems. The Commonwealth Bank operates two SAS platforms to attend to the majority of real-time and batch requirements for both fraud and money laundering.

The batch platform, which we call the Financial Crimes Platform, was developed in 2006 for transaction and origination fraud before it was extended successfully to money-laundering detection. The real-time platform was launched in 2011 for the Group's extensive debit card portfolio, with the migration of other channels and products from legacy systems progressing. In order to understand the scale of the systems, consider the following facts.

The Financial Crimes Platform (used to detect fraud and money laundering) includes:

- 31 source systems.
- 11 million customers.
- 15 million transactions loaded each day.
- Analyses of up to 420 million transactions every night, looking for fraud and money laundering activity.

The Real-Time Transaction Monitoring system (to prevent fraudulent transactions in real time) includes:

- 11 million account profiles.
- 6 million customers.
- A current average of 80-85 transactions per second with a mean response time of 40 milliseconds.
- Tested peak volume of 250 transactions per second.

Combining a customer-centric view of fraud with advanced analytics and computing capabilities presents many opportunities.

From a traditional fraud perspective, our systems can help us:

- Identify fraud where the customer is the victim or the perpetrator.
- Identify activity that gives rise to the Group submitting a suspicious activity report pursuant to our statutory anti-money laundering obligations.
- Provide an opportunity (in the case of a false positive) to learn more about our customer banking behavior.

CAN WE DO MORE?

We have demonstrated the trust we place in our systems to reliably defend us and our customers from criminal activity.

What we are yet to demonstrate, but intuitively believe is probable, is that the fourth opportunity to be gained from a customer-centric approach to analytics is marketing.

Declining non-fraud transactions for valued customers provides a suboptimal service experience. However, we mitigate that risk by understanding all transactions and building a detailed view of what is considered normal. The factors we use to determine what is normal should also be applicable when we consider how to generate just-in-time marketing leads without swamping our consumers with too many leads.

We can do more – I have no doubt of that. While our primary role is to ensure the fraud detection systems are optimized and applicable to the threats we face, we should take every opportunity to leverage our investment in advanced systems to improve our return on investment. IQ

online

Read more from John Geurts:
sas.com/success/CBA.html

John Geurts is the Executive General Manager for Group Security and Chief Security Officer for the Commonwealth Bank Group in Australia, and has had the pleasure of leading Group Security for almost 12 years. Group Security provides global security leadership for the bank, including its international subsidiaries and majority joint ventures.

LA COUNTY CLOSES IN ON FRAUD RINGS

Identifying child care fraud sooner saves millions per year

Los Angeles (LA) County has the largest population of any county in the United States, with approximately 27 percent of California's residents. If it were a country, LA County would be among the top 20 in the world as measured by GDP. The county's budget is approximately $23 billion, which goes toward providing social, health-related and law enforcement services.

Recently, LA County has been challenged by an increase in fraud related to child care services. The county estimates that fraud has grown by about 40 percent and, in many cases, is perpetrated by highly organized fraud rings. To stem the growing tide of financial crimes and losses, the Chief Executive Office of LA County and the Department of Public Social Services conducted a proof of concept (POC) to assess the feasibility of using the SAS® Fraud Framework and SAS® Social Network Analysis to get a better handle on the problem.

The Chief Executive Office is responsible for establishing and administering the budget for the county's services and programs, which includes monitoring and measuring them for efficiency and cost-effectiveness.

"Using the results of the POC we did projections and cost-savings analysis and concluded that the county could expect to see a return on investment of somewhere between $7 million to $30 million annually," says Manuel Moreno, Director of Research, Chief Executive Office. "The POC showed a number of advantages in using the technology, not only related to costs, but how we prioritize investigations.

"The county [expects] to see a return on investment of somewhere between $7 million to $30 million annually."

Manuel Moreno, PhD, Director of Research

With social network analysis and predictive analytics, we can identify benefit recipients and service providers and predict those most likely to engage in fraud and where there might be a potentially large loss of funds."

Moreno says common fraud cases are characterized by criminals filing false claims of employment, which usually include declaring employees who don't exist. In some cases, businesses are set up by the heads of fraud rings. These individuals are in collusion with recipients, who falsely declare that their children are attending nonexistent child care programs. Sometimes, criminals declare work schedules that are either false or shorter than the amount of time claimed.

The POC demonstrated that by using predictive models and peer group analysis to detect behavioral anomalies in the utilization of child care services, fraud risk scores could be developed to help decrease the number of false positive cases assigned to investigators. The POC also allowed the team to map potential fraud rings.

"One of the things we showed is the system's ability to utilize social networks to detect if individuals are likely to commit fraud, based on their fraud risk score," explains Moreno. "We established a network, for example, consisting of participant and provider nodes and illustrated their relationships. We looked at whether this small network fit into the larger scheme of networks, in which participants are in collusion with other child care providers. With the technology, we identified strong central nodes. In one case, we had a child care provider servicing many nodes of participants engaging in collusion activities.

"We needed a unified approach to get a handle on the fraud problem," Moreno continues. "We wanted a solution that provided data integration, as well as a powerful analytical tool workbench. To perform sophisticated predictive modeling we needed historical data, and for that we had to integrate many external and internal data sources, such as the state of California's Employment Development Department data and business license data from Los Angeles County."

Based on metrics from the POC, Moreno and his team concluded that data integration, predictive capabilities, data mining tools and the insight by the SAS solution can be used effectively to detect fraud before it occurs.

"We calculated that the accuracy rate of fraud rings identified by the social network analysis solution to be, with reliability, 85 percent." IQ

online

Learn more about SAS Social Network Analysis: **sas.com/solutions/fraud/social-network**

WHAT IF YOU COULD…

- Improve information credibility. What if you could easily eliminate duplicate names, addresses and other identifying information from your data to reduce erroneous payments and duplicate billing?
- Enhance audit effectiveness. What if you could predict the likelihood that a transaction would be fraudulent and flag suspicious activity for further investigation so you could not only uncover fraud, but prevent fraudulent payments?
- Deliver fact-based insight. What if you could not only access reports that measure your efforts toward reducing fraudulent payments, but also drill down for details at the department level?
- Achieve financial accountability. What if your financial system could track program purchases, payments and costs to ensure that they are necessary and justified?
- Manage performance. What if everyone in your organization worked together collectively and collaboratively, sharing knowledge and best practices, to achieve common goals for preventing or correcting improper payments?

You can with the SAS Fraud Framework: sas.com/solutions/fraud/index.html

PREVENTING FRAUD FOR THE GOOD OF SOCIETY

We can no longer afford to let fraud and error burn a hole in our pockets

Graham Kemp Public Sector Head, SAS UK

Tackling fraud is seen not only as a moral issue nowadays, but also as the most obvious, and possibly the least painful, way to reduce deficits. In April, the UK's National Fraud Authority released the results of its Annual Fraud Indicator, which found that fraud against the public sector has been revised down from US$33.2 billion to US$31.8 billion per annum, influenced to a large extent by reduced fraud against the tax system.

While the figures are clearly a step in the right direction and show that measures the government is putting in place are beginning to take shape, the government cannot afford to rest on its laurels. If the public sector is to build on the momentum of the announcement, it will need to ensure that civil servants have the proper training and procedures in place to continue to prevent, detect and punish fraudulent activity effectively.

Fraud has long been associated with lack of effective monitoring of financial information and transactions. In the private sector, the insurance industry is already implementing best practices that collect, analyze and share information between otherwise competing partners **(see Page 15)**.

COLLECT, ANALYZE AND SHARE

To combat fraud, the public sector needs to improve efficiency by using an intelligent approach to data analytics to detect abnormal patterns, link multiple parties, automatically route suspicious cases for further investigation, and use predictive modeling to uncover new fraudulent activity. Government departments must also accelerate cross-government working and adopt a data-sharing policy where appropriate.

Public sector organizations must recognize that dealing with fraud in its various forms, whilst balancing increased pressure for savings, can only be achieved by treating information as an asset that should be collected and analyzed in smarter ways.

As is often the case, you do not know whether you have the right information until you act upon it. It is also true that different public sector stakeholders have different views on what information could be collected, shared and analyzed. The information accessible to public sector organizations includes both structured and unstructured data – such as text, video, audio and social networking

information. To better manage this, comprehensive frameworks that support integration of the different types of information need to be developed.

DEVELOP BEST PRACTICE GUIDELINES

As it stands, fraud and error represent a huge black hole in the government's balance book. If the government wishes to realize its vision of an all-pervasive, sustained, zero-tolerance culture to fraud and error across the public sector, civil servants will first need to better understand exactly how their departments are already tackling fraud and error, and have the right training and incentives to ensure that they can build on this.

The government is already using software solutions and predictive analytics as a key enabler to combat fraud, but skills and training are still a serious issue. SAS recently polled civil servants on this issue and found that 73 percent of those questioned claimed to have received no training in tackling fraud and error over the last 12 months. It is imperative that the government addresses this if it wishes to root out fraud across the board.

The findings from our research suggest that, despite the billions of pounds lost to fraud and error every year, the level of awareness about how public sector departments were addressing the issue is low. Nearly half of those questioned were unsure whether their department had carried out an investigation into fraud over the last 12 months, and this was only slightly lower among the senior-grade sample. For investigations into error, the results were slightly better, but 44 percent of respondents still lacked awareness of their agency's or department's approach to the issue.

THE TIME TO ACT IS NOW

The UK public sector needs to be innovative in order to protect the citizen from the effects of fraud, both individually and also to ensure that taxpayers' money is not used to pay fraudulent claims. Otherwise, confidence in the public sector will be eroded and money will be taken from the pockets of the most needy. The fraudsters aren't going to give up anytime soon, so the onus remains on the government to take the fight to them. IQ

online

Learn how to combine traditional fraud detection methods with modern methods like social network analysis:
sas.com/fraud-hybrid

Fraud tips webcast:
sas.com/fraud-webcast

IRISH REVENUE COMMISSION USES SAS® TO TARGET EFFECTIVE INTERVENTIONS

The Irish Revenue Commissioners (IRC) worked with SAS to develop predictive models that moved from identifying risks of non-compliance or liquidation, to predicting the likelihood of a case yielding in the event of an intervention, such as an audit. The models also assess the value of a potential yield to the IRC, so that interventions can be prioritized and tailored accordingly. Early results have been positive, with a strong relationship between cases predicted to yield and actual average yield. See Page 25 to learn more about how IRC uses analytics to prevent fraud.

Graham Kemp has more than 10 years of experience advising public sector organizations on how to select and deploy effective technology solutions to meet their unique needs. He participated in the Government's Information Age Partnership. He is also a former chair of the Department for Education ICT Industry Club, Infrastructure Group and a member of the Government's Distance and Education Learning Group advisory board.

IS YOUR HEALTH CARE FRAUD DETECTION SOLUTION IGNORING VALUABLE SOURCES OF DATA?

Julie M. Malida Principal for Health Care Fraud, Enterprise Financial Crimes Practice, SAS

In the health care industry, professional fraud often involves multiple parties that are in collusion, premeditated schemes, identity theft and organized crime. Frequently, the money evaporates in a matter of days. Consequently, it is now more important than ever to be timely in fraud detection (preferably before monies are paid out), employ multiple analytical methods of detection, and use a variety of data sources beyond just claims data.

Let's take a closer look at the most common methods of fraud detection and the frequently ignored data sources that can help improve detection.

MULTIPLE METHODS OF ANALYSIS

Fraud is a spectrum of activity that ranges from opportunistic deception to truly premeditated, organized schemes. Each different type of analytics attacks a different issue or type of activity.

Basic rules on prior known schemes have their place and cast a wide net for detecting suspicious activity. An example would be, "Show me all claims where the patient is traveling more than 200 miles for routine care." But rules are very linear in the way they are written, and investigators end up chasing many false positives to weed out the cases that may be explainable. Fraud rules are also very easily gamed, once the fraudster figures out how the rule is written.

Anomaly detection, which casts the net a bit wider and looks for oddities you didn't know enough about to write a specific rule around. However, such oddities show up as outliers in behaviors that don't look normal. Fraudsters can also game anomaly detection, for example, by working with multiple providers to make their schemes harder to detect through this method.

Predictive modeling applies statistical methods like decision trees and neural networks to data from prior cases of known fraud, and looks for statistical similarities. A good example is a chiropractor who treated everyone in the same family for the same low back pain twice per week until all family members' health plan benefits were exhausted. You can build a model that can look for similar characteristics to detect similar fraud schemes before they are paid. Predictive models will vastly reduce the false positives and make analysts laser-like in the claims they pursue for full investigation.

Social network analysis (also called link analysis) builds mathematical models that show the connectedness of different entities and score their statistical significance for fraud, either by looking at their activities or by looking at their personal relationships. Physicians who always send patients to a certain lab or two physicians who attended the same schoolwould be linked entities, for example. Once entities are linked, it becomes interesting to see which grouped entities violate a rule or model from one of the other methods previously described. This method allows analysts to spot organized crime and collusive behavior.

VALUABLE DATA SOURCES OFTEN IGNORED

Medical claims data is the first and strongest data source for fraud investigations, but you can improve fraud detection efforts by including some of these additional data sources:

- Member eligibility data to compare benefit coverage dates, falsification of service dates, or falsification of supply purchases. Past medical provider history, including previous sanctions against providers, their presence on state and federal "watch" lists, and any underlying motives for deception.

- Ancillary claims like pharmacy billings, lab data and hospital records with revenue can detect whether all the care provided naturally seems to fit together as compared with accepted medical practice.

- Structured and unstructured text data, including nurses' notes, claim processor notes in claim records, electronic medical records and call center logs, provide a valuable and rich source of investigative data that may be locked in a payer's underlying systems.

PROVEN VALUE OF UNSTRUCTURED TEXT DATA

To understand the value of text analytics in detecting fraud, consider the text in call center logs. Wouldn't it be interesting to know if the same chiropractor's office called the health plan five times in one week to determine remaining benefit levels on every family member covered under the plan? By mining text data in the call center logs, this could be flagged as an outlier.

And the nurses' notes? Wouldn't it be meaningful if the notes documented a physician saying this patient needed a five-day hospital stay rather than two days due to multiple comorbidities that are not documented in the claim? The physician is either omitting information in one source or fabricating "facts" in another.

Finally, what might an audit of electronic medical records reveal? Perhaps there are far too many patients who all have the same documented height, weight and symptoms to be a normal occurrence. It could alert the investigator that someone is copying and pasting information, instead of filling out medical records accurately.

THE PUNCH LINE

Using multiple analytical methods and all the varied data sources available allows organizations to conduct more efficient investigations, know about fraud and abuse cases sooner, and find out pertinent information quickly. The investigator can also prepare a better bank of evidence if the case ever does proceed to law enforcement or prosecution.

It is becoming a recognized necessity for health plans to find fraud before the money goes out the door. The window of opportunity is shorter than ever due to timely payment guidelines and expectations from regulators and the marketplace.

Investigators and analysts that use anomaly detection, predictive modeling and social network analysis–combined with access to all sources of relevant data–will have the best chance of moving swiftly and accurately to detect fraud, waste and abuse before the loss occurs. IQ

online

Read the SAS text mining blog:
blogs.sas.com/text-mining

Julie Malida is the Principal for Health Care Fraud in the Enterprise Financial Crimes Global Practice at SAS. She has devoted 29 years to the health care industry, focusing on managed care, fraud and cost containment in medical claims. Malida is also a Fellow of the Society of Actuaries and a member of the American Academy of Actuaries.

13

HYUNDAI MARINE & FIRE INSURANCE PREVENTS FRAUDULENT AUTO CLAIMS

Avoiding losses saves costs for insurer and innocent policyholders

Korea's automobile insurers are getting slammed with fraudulent claims. The country's Financial Supervisory Service reports a one-year increase of 30 percent. Unfortunately, most insurers do not respond effectively – either because they lack enough claims investigators or because they base their predictive models on existing industry statistics.

But not Hyundai Marine & Fire Insurance. Using SAS for fraud detection and prevention, Korea's largest non-life insurer has built a system that prevents claims fraud and improves premium payment processing, thereby protecting its most profitable customers.

"Fraud costs not only the insurance companies, but also the innocent policyholders," explains Chul-Woo Lee, Manager of Hyundai M&F's Investigation Team. "For an insurance company, enforcing the existing fraud prevention system is no less important than creating new profit."

Hyundai M&F's fraud detection system combines business rules based on the experience and knowledge of its investigators with model rules generated from data extracted from various IT systems. The models are applied to insurance claims, delivering results to claims investigators in real time.

The system also monitors the performance of these rules, enabling the company to quickly modify existing rules or generate new ones. The predictive models enhance the process of fraud detection so Hyundai M&F can detect fraudulent claims before they ever get paid.

"It was inconvenient and ill-timed for us to have to investigate every individual accident history and assess the risk information by going on the network data every time," Lee says. "Our fraud detection system helped us to increase the detection rate by technically securing twice the amount of data than before. And as a result we were able to secure competitiveness in statistical service."

Hyundai M&F's system relies on a three-pronged approach. A fraud pre-detection system helps investigatorsjudge the possibility of fraudulent activities using statistics-based model and business rules, allowing a loss assessment in advance for the filed claim. A post-detection system pinpoints potential fraud in areas where it is hard to detect earlier, such as hospitals, repair shops and individual clients. Lastly, a risk mart generates data for both systems in a separate data warehouse.

The benefits of Hyundai M&F's system include:

- Timely risk assessment.
- Timely payout after selective investigation.
- Better detection and accuracy.
- Easier gathering and maintenance of fraud data.

Hyundai M&F also uses SAS to analyze customer complaints. And the insurer is moving toward a consolidated risk management system.

"Fraud and risk management have a lot in common," Lee explains, "so it's important to have complementary systems." IQ

online

SAS for fraud detection and prevention:
sas.com/industry/ins/fraud

"For an insurance company, enforcing the existing fraud prevention system is no less important than creating new profit."

Chul-Woo Lee,
Manager of the Investigation Team

KOREA'S TOP INSURANCE COMPANIES PREDICT FRAUDULENT CLAIMS USING SAS®

Korea's insurance companies are struggling with preventing fraudulent claims and enhancing customer satisfaction. The country's Financial Supervisory Service reports a one-year increase in fraud of 30 percent. Unfortunately, most insurers do not respond effectively, either because they lack enough claims investigators or because they base their predictive models on existing industry statistics.

SAS Korea is helping insurance companies address risk and fraud to prevent insurance leakage, protect good subscribers and reducing the time for premium payments. Consider Samsung Life Insurance. Using SAS, the company built a risk scoring system, an automatic fraud detection system, a credit data management system, and a document forgery and alteration detection system – first-of-their-kind industry implementations in Korea.

Following the success with Samsung Life Insurance, SAS moved on to help Hyundai Marine & Fire Insurance, Korea Life Insurance, Kyobo Life Insurance, Dongbu Insurance and Samsung Fire & Marine Insurance, all top 10 insurance companies in the country.

THE FUTURE OF FRAUD INVESTIGATIONS

Alison Bolen Intelligence Quarterly, Editor in Chief

In many ways, the early 1990s were the heyday of Special Investigation Units (SIU) for insurance companies, says Tim Wolfe, Director of Special Investigations for CNA, a commercial property and casualty insurance provider. Around that time, states started requiring companies to report suspicious claims and insurers increased staff to meet those regulations. "In those days, SIU consisted almost entirely of former law enforcers. We were hiring people who were used to policing crime."

Today, analytics technologies that identify fraudulent activity are changing all of that. Insurance companies are hiring data modelers instead of security professionals, and they're changing the way SIU departments are organized.

"That doesn't mean you don't need boots on the street," says Wolfe. "You still need field investigators asking the right questions." Technology does not do investigations for you, but technology will identify potential fraud activity that may have been overlooked so you know where to send those investigators and waste less of their time.

The staffing change is reflected at CNA dramatically. In fact, Wolfe's team has outsourced a large portion of its field investigative work and now employs a handful of workers who manage and monitor the investigative process, plus an in-house team of investigators for major investigations and organized crime. The rest of his team is focused on intake, training, regulatory compliance, analytics and process improvement.

"The last data analyst we hired was from the military," says Wolfe. "Her experience was in predicting IED explosions, but we've found that it was a really good idea to hire somebody outside of the industry. They're not just thinking insurance and they bring a lot of fresh ideas."

The change in skill sets is reflected at a national auto insurance company in the U.S., where a senior manager of the Special Investigations Unit tells us they have transformed the home office environment over the last couple of years to be an innovation environment. As a result, his team is really starting to look at how data can influence decisions.

USING DATA TO IDENTIFY FRAUD

Data has been used traditionally in underwriting and claims side of most insurance businesses, but it's a recent practice to use data to manage resources and flag potential fraudulent claims for

"The last data analyst we hired was from the military. Her experience was in predicting IED explosions, but we've found that it was a really good idea to hire somebody outside of the industry. They're not just thinking insurance and they bring a lot of fresh ideas."

Tim Wolfe, *Director of Special Investigations for CNA*

investigation. There are clear, distinctive data points that can be used for modeling. If businesses can identify these data points and convert them into operational decisions while collecting information from customers, they can be more predictive.

In the past, most fraud referrals came from a small percentage of adjusters who know what to look for, take the time to make reports, or have good instincts. Today's fraud systems, however, can identify red flags automatically to help make adjusters and SIU unit aware of potential fraud more often and more quickly.

Another fortunate turn in identifying fraud in insurance is that regulators are now allowing insurance companies to share info as it relates to fraud. For example, a Medical Crimes Database is being built with impetus from the National Insurance Crime Bureau in the U.S. where all major insurance companies can share medical code records (in aggregate without revealing individual patient info) to better detect fraudsters who are making claims across multiple insurance companies.

The value becomes obvious when you see a single person claiming 60 hours of work in a 24 hour day. If you're only looking from one company, you might see five hours of it – but looking across every claim, the crime becomes obvious.

Wolfe says technology is also important because fraud is getting more sophisticated than it used to be. "We're seeing more granulated schemes involving not just doctors and lawyers but people associated with workers compensation who bill for interpretation services when they're not needed. Or transportation providers to drive patients for care when no transportation has took place."

Ultimately, identifying fraud helps everyone. It reduces business costs, which can be passed on to the customer and it helps fight larger societal criminal elements. Plus, claims from legitimate customers get processed more quickly and fewer false positives keep honest customers happier too.

online

Stop Fraudsters Before They Strike webinar:
sas.com/reg/web/corp/1478025

PREVENTING FRAUD IS IN EVERYONE'S BEST INTEREST

While the true dollar impact of fraudulent claims is almost impossible to measure, the Insurance Information Institute estimates that it represents approximately 10 percent of all property/casualty insurance claims. From 2005-2009 in the United States, the dollar impact of that fraud totaled $30 billion. If you think the insurance company just writes that off and it doesn't affect you, you are wrong. Fraudulent claim costs are in many ways passed down to all policyholders in the form of increased premiums: You're paying for the bad behavior of others. So, it's in everyone's best interests to limit fraudulent activity: Insurers, regulators and policyholders.

Learn from industry expert Jodi Pratt how to create an anti-fraud culture:
sas.com/knowledge-exchange/risk/fraud-financial-crimes/creating-an-anti-fraud-culture/

Alison Bolen is the Intelligence Quarterly Editor and the Editor of the SAS blog program. Since starting at SAS in 1999, Alison has edited print publications, websites, e-newsletters, customer success stories and blogs.

HOW TO PREVENT FRAUD IN THE INDIAN TELECOM INDUSTRY

Understand the different types of fraud and what you can do to combat them

Amitava Ghosh Senior VP, Analytics Platform Technology, Wireless Business, Reliance Communications

The Indian telecommunications industry is the second-largest and fastest growing in the world. According to a March 2012 Telecom Regulatory Authority of India (TRAI) report, there were more than 919 million wireless subscribers in the country with an annual growth rate of 0.88 percent. During that same time period, annual telecom fraud worldwide was estimated at US$40.1 billion, according to the Communications Fraud Control Association (CFCA) Fraud survey for 2011.

Globally, telecom fraud decreased 33 percent from 2008 to 2011. However, fraud in Indian telecom, as well as other industries, is rising. According to a KPMG Fraud Survey Report from 2010, 75 percent of respondents from all industry sectors believe fraud incidence has increased in India over the past two years, 54 percent feel that fraud is on the rise in their own industry and 45 percent feel that fraud has increased in their own organization.

To prevent fraud, 13 percent of survey respondents said they are using IT controls for fraud detection and 21 percent are using data analytics to detect fraud.

A growing marketplace presents many challenges, including learning how to curb the fraud and abuse that naturally multiply as the market size increases. In this article, I will classify fraud into three main areas and describe different methods for combating fraud for each type. The categories are:

Sales and distribution fraud:

- *Impersonation and identity duplication.*
- *Subscription fraud.*

Network and device fraud:

- *PBX fraud.*
- *SIM box/interconnect fraud.*
- *SIM card cloning.*

Billing fraud:

- *Unauthorized prepaid to postpaid conversion.*
- *Suppression of billing call detail records.*
- *Billing configuration.*

SALES AND DISTRIBUTION FRAUD

KPMG estimates that 70 percent of telecom fraud in India occurs because of flaws in the subscriber acquisition process, while 10 percent of revenue losses occur due to subscription fraud. Even though these types of fraud are considered entry-level, their sheer prevalence adds up.

Impersonation fraud or identity duplication is a common entry-level fraud in India. Most customers in India subscribe for service through a retailer. While retailers are required by law to verify the subscriber documentation (CAF), the retailer or a subscriber is able to use the same document repeatedly, sometimes just changing part of the name or address. With each acquisition, the retailer makes a significant commission.

SOLUTION: Use good de-duping software to match the CAF against the subscriber. Telecom companies can then check for multiple connections and, if duplication is discovered, terminate the subscription and withdraw the commission from the retailer. If a history or pattern of fraud is uncovered, offending retailers and subscribers can be blacklisted.

Another prevention method is to check for the reuse of International Mobile Equipment Identity (IMEI) numbers. Since most SIM cards are activated by sending an SMS as part of the activation process, the IMEI number of the handset can be captured by a fraudster. Single handsets used to activate multiple SIM cards within a certain time span can indicate fraudulent activity.

Subscription fraud, another entry-level fraud that is prevalent in India, happens when a retail agent or call center agent attaches a value-added service (VAS) to an unsuspecting subscriber. For example, a ringtone can be added without the customer's knowledge or permission, resulting in a commission for the agent.

SOLUTION: Check the call detail records (CDR) to determine if a subscription request was made by the subscriber via SMS or by contacting the call center. These kinds of audits should be performed regularly.

NETWORK AND DEVICE FRAUD

PBX fraud involves using PBX access codes to make outgoing calls to international destinations. PBX fraud occurs when trespassers access business phone systems that use a PBX phone system and illegally use an access number to gain a dial tone. They often place multiple long-distance calls through these lines for unscrupulous purposes, including the reselling of long-distance for a profit. Service providers often cannot distinguish these calls from any other call originating from that business.

SOLUTION: Monitor calls to hot-listed international destinations that you know are popular with fraudsters. You should also monitor the length of international calls.

SIM box and interconnect fraud is perpetrated to avoid call charges. A SIM box is a device that maps an international voice over Internet protocol (VoIP) call to a SIM card of the mobile operator on the receiving end of the call. By doing this, the international call appears to the destination operator as a local domestic call rather than an international call, thus cheating that operator out of the international terminating charges, which can be significant. The same technique can be used to make a local out-of-network call appear as if it were in network, resulting in significant revenue losses since out-of-network calls have termination charges.

SOLUTION: Telecom companies should be on the lookout for subscribers who have a very high number of distinct called parties but too few distinct base transceiver stations. Also, look for a series of calls where roaming is very low or nonexistent and watch for international calls with masked domestic numbers.

SIM card cloning fraud involves cloning the SIM cards of unsuspecting subscribers. By cloning the SIM card, the fraudsters have free access to all of the services paid for by legitimate customers.

SOLUTION: Extensive call detail analysis must be done using data analytics techniques. For example, checking for call start overlaps from the same multiple directory number is usually a good indicator once conference calls have been ruled out.

BILLING FRAUD

Unauthorized prepaid to postpaid conversion fraud is generally committed by an employee of the telecom company who removes the prepaid flag in Home Location Register (HLR), which then makes the billing postpaid.

SOLUTION: Monitor the system logs in the HLR for unauthorized access and changes. A service request that corresponds to the conversion must be present. Audits should be performed very frequently to make sure the HLR configuration processes don't have weaknesses that can be exploited.

Suppression of billing call detail records (CDR) fraud involves suppressing the generation of CDRs in the network switch and is usually carried out by a company employee.

SOLUTION: Control and monitor access to configuration switch processes to prohibit unauthorized activities. The revenue assurance team must check for a decline in the number of CDRs generated from a switch based on past history. Any significant drop in the rate should be examined.

Incorrect prepaid billing configuration fraud happens when an employee changes the configuration in the prepaid billing systems called IN (Intelligent Network).

SOLUTION: A separate billing system is used, usually called Mediation, to take unrated CDRs directly from the network switch and rate them by using the same billing configuration. This information should then be matched with the data provided by IN. Any significant differences should be examined for fraud. Normally this is the function of a revenue assurance team.

ANALYTICS IS THE ANSWER

Telecom fraud is big business around the world. With rising competition and extremely low average revenue per user (ARPU), the high cost of new acquisitions has dramatically eroded the bottom line of telecom operators. Detecting fraud and plugging revenue leaks have become extremely important to reduce costs.

Fraud connected to prepaid accounts is much easier to commit and harder to combat, since there is very little information on the subscriber, unlike postpaid accounts, where a credit check is usually done. Entry-level fraudulent activities such as subscription and impersonation are very serious since the cost is coming straight from the bottom line in the form of commissions and incentives. All of the Asian and African prepaid telecom markets are affected by each of the frauds mentioned above.

The most important weapon against prepaid fraud is data analytics. At Reliance Communications, we use DataFlux® from SAS to de-dupe subscribers and to check for impersonation fraud; we also use SAS® Analytics to detect subscription fraud. The revenue assurance team ensures that billing and usage records reconcile. We are also implementing a pilot project that will use subscriber history to build profiles and check for anomalies in user calling patterns that would indicate fraudulent behavior. IQ

[1] Highlights on Telecom Subscription Data as of 31 March 2012. Telecom Regulatory Authority of India, 2012. **trai.gov.in/WriteReadData/WhatsNew/Documents/PR-TSD-Mar03052012.pdf**
[2] Global Telecom Fraud Decreases by 33% from 2008, Returns to 2003 Levels. Communications Fraud Control Association, 2001.**cfca.org/pdf/survey/Global%20Fraud_Loss_Survey2011.pdf**
[3] Ibid
[4] India Fraud Survey Report 2010. KPMG, 2010. **kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Fraud_Survey_2010.pdf**

HOW FAST IS THE INDIAN TELECOM MARKET GROWING?

According to a March 2012 Telecom Regulatory Authority of India (TRAI) report:

- There are more than 919 million wireless subscribers in India.
- The growth rate in India's telecom sector is 0.88 percent.
- Overall teledensity (number of wireless connections per 100 people) is 76.00.
- Urban teledensity is 162.82. (Many urban people have more than one phone.)
- Rural teledensity is 38.33.
- India has the third-largest number of Internet users in the world, with more than 121 million in 2011.

[5] Highlights on Telecom Subscription Data as of 31March 2012. **trai.gov.in/WriteReadData/WhatsNew/Documents/PR-TSD-Mar03052012.pdf**

As a Senior Vice President at Reliance Communications, Amitava Ghosh implemented a SAS analytic platform for the wireless business. He has many years of experience constructing complex systems in all types of operating systems and a solid background in building scalable, high-performance solutions.

CUTTING TAX ERRORS IN HALF

Swedish Tax Agency finds erroneous tax returns using predictive analysis

The Swedish Tax Agency has two important objectives: to ensure that taxes are correctly reported and that the resulting tax debt is then paid. Using new analytics solutions, the agency can now identify risk profiles more easily, thereby preventing and stopping tax fraud and neglectful tax returns.

Like many other public sector organizations, the Swedish Tax Agency is facing a future of diminishing resources. "This increases the need for automated solutions and requirements for better resource management through well-founded risk analysis," says Andreas Voxberg, Analyst/Section Coordinator at the Swedish Tax Agency's Analysis Unit.

We have high tax compliance in Sweden, both in terms of reporting and paying it," explains Voxberg's colleague, Analyst and Statistician Joacim Danielsson. "This is underpinned in part by good system solutions where, for instance, employers pay their employees' preliminary tax and submit a statement of income to the Swedish Tax Agency. Even so, the aim is still to ensure there are as few discrepancies as possible."

In Sweden, the tax discrepancy, defined as the tax that should be reported but isn't, is estimated to be roughly 10 percent of the theoretically correct tax. One of the Swedish Tax Agency's goals is to half the tax discrepancy, and one of the Analysis Unit's tasks is to identify anything that could jeopardize meeting this goal.

To reduce the percentage of tax errors, the agency has endeavored to make life easier for tax payers wherever possible, gradually simplifying its tax returns. It has also introduced various control measures and conducted information campaigns.

"We have published information about some of our controls online, so that individuals and companies can run checks themselves before submitting their returns and avoid being flagged in our control system. This saves time for them as well as for the agency," Voxberg explains. The process of identifying tax returns with the highest risk of errors takes place within the framework of the Swedish Tax Agency's selection project, for which Voxberg and Danielsson are project manager and assistant project manager, respectively. All tax returns are scrutinized. They undergo an automated check, and some are also selected for a more in-depth examination according to certain criteria which may vary from year to year.

"We need to identify the non-payers as early as possible. Using predictive models, we can identify risk profiles and indicators so that we can focus where the risk of non-payment is greatest."

Joacim Danielsson, *Assistant Project Manager, Analysis Unit, Swedish Tax Agency*

"All income and tax returns, from individuals and companies alike, pass through an auditing net, which is set up by the Swedish Tax Agency's selection project. It is the project's task to identify risks at return level, based on the operational plan and the various activities therein. The risk analysis at a more general level is dealt with by the agency's Analysis Unit, and is used as a basis for decisions on what measures should be implemented to deal with the risk groups," says Voxberg.

To produce as reliable risk profiles as possible, the agency uses analysis solutions such as data mining and statistical analysis. According to Voxberg, this is not simply a means of "rating" tax payers, rather it is a model for pinpointing high-risk behavior.

Thanks to the agency's new analysis solutions, it has been able to broaden its risk examination from the component to the general level. Voxberg and Danielsson regard the move from company level to network level as the next fascinating challenge. Putting the risk into a broader context – a network – is a way of building a more substantial picture.

The aim is to further complicate tax fraud. When it comes to the risk of non-payment of tax, this has become an increasingly important area, particularly in the wake of the credit crunch. Tax payment compliance is at 99.7 percent, which means that only 0.3 percent is not paid.

It's more about maintaining that level," says Voxberg, while noting that even 0.3 percent of Sweden's total tax revenue still equates to billions of kronor. "We need to identify the non-payers as early as possible. Using predictive models, we can identify risk profiles and indicators so that we can focus where the risk of non-payment is greatest," says Danielsson.

Along with two master's students from Copenhagen Business School, the Swedish Tax Agency is currently going through the extensive research literature, so that, if possible, it can improve its credit risk models with further indicators of inadequate solvency at both a company and a macroeconomic level. Danielsson can see many benefits in the improved risk analysis, in addition to increased efficiency for the Swedish Tax Agency:

It is good if we can find any debtors and reach out to them early so we can help out, and they can pay before the matter is referred to the enforcement authorities. Obviously it's also a plus for society in general if we have a stronger tax foundation to fund welfare initiatives, for instance." IQ

online

Stop fraudsters before they strike webcast:
sas.com/reg/web/corp/1478025

REDUCING TAX FRAUD LEADS TO BETTER CUSTOMER SERVICE IN BELGIUM

Federal Public Service Finance uses analytics to master huge fiscal database

Analyzing tax returns, verifying import and export customs declarations, consolidating and checking the data from dozens of local tax collectors' offices – those are just a few of the jobs that Belgian Federal Public Service (FPS) Finance has entrusted to SAS software for reasons of speed, efficiency and flawless execution.

FPS Finance is a government institution that collects huge amounts of data from a variety of sources. For a start, there's the Collection and Recovery Department of FPS Finance that collects money from taxpayers and pursues late payers. It also recovers funds due from non-paying individuals and companies, using all possible legal means.

To give you an idea of the magnitude of the operation: Every year, the department handles information related to more than 3 million income tax returns, which results in one of the largest databases in Belgium. The department also manages the analysis of real estate for estimating real values, the analysis of all tax returns from legal bodies as well from as private citizens and the VAT, and the risk evaluation of import and export customs declarations for merchandise.

A PERFECT FIT

"For the past few years, we have been keen users of SAS® Enterprise Guide® and SAS® Enterprise Miner,™ mainly for risk management in the various fiscal domains," says Dierk Op 't Eynde, Data Mining Coordinator at FPS Finance. "The reason is very simple: They are excellent solutions for data analysis and data mining, two crucial missions for our administration considering the size of all the fiscal data to be analyzed, the fast-changing Belgian legislation and the European directives. And the nice thing about it all is that the SAS tools fit perfectly with the IT standards of FPS Finance."

It used to be quite different altogether. Efficiently managing and exploiting vast databases of information is a challenge for any system; processing times used to be quite lengthy, which wasn't exactly conducive to higher efficiency or service quality. That's why in 2010 several specialized services of FPS Finance switched to a SAS environment for data mining, risk analysis and performance management.

The ICT department created a business analytics environment in which a data warehouse was directly linked to a risk analysis environment, used by business analysts from several departments for

Moving to SAS is "like switching from a handcrafted data analysis environment to an industrial one."

Dierk Op 't Eynde, *Data Mining Coordinator, FPS Finance*

a variety of operations, ranging from data mining and risk analysis to ad hoc inquiries. "Currently we have some 30 users supported by two administrators," Op 't Eynde explains. "But in due time we will increase this number by 30 percent in view of the high expectations from our policymakers regarding the handling of fiscal fraud."

FIGHTING FRAUD AND MORE

Using SAS software to combat fiscal fraud is a major undertaking, says Op 't Eynde. "It is our duty at FPS Finance to guarantee a correct and fair tax collection, and that means that every taxpayer should pay what he or she legally owes, neither more nor less. Fighting fiscal fraud is a major focus here."

In addition to handling fraud detection and tax collection, Op 't Eynde says the analytics are also used to improve customer relationships with citizens and for creating statistics, forecasts and simulations regarding all fiscal earnings. "Our use of SAS solutions goes far beyond the fair collection of taxes, a more efficient deployment of tax inspectors or policy supporting information for audits. Specific analyses will enable us to recognize our stakeholders and enhance our service to citizens and companies. Our strategy is evolving toward a more compliant and shared approach that reflects the various risks and is primarily aimed at preventing abuses."

Apart from monitoring the tax collection, risk analyses are carried out on a regular basis to identify which individuals or companies are at risk of not meeting their fiscal liabilities, and which are likely to become insolvent or bankrupt. Here, data mining is put to good use to spot various forms of fraud or to check on figures that might help predict bankruptcies at an earlier stage.

Previously it took the analysts up to half a day to produce a scoring list, but they can now obtain this list in a few minutes, simply because the SAS tools are better at handling huge volumes of data. Op 't Eynde called the move to the SAS environment "like switching from a hand-crafted data analysis environment to an industrial one."

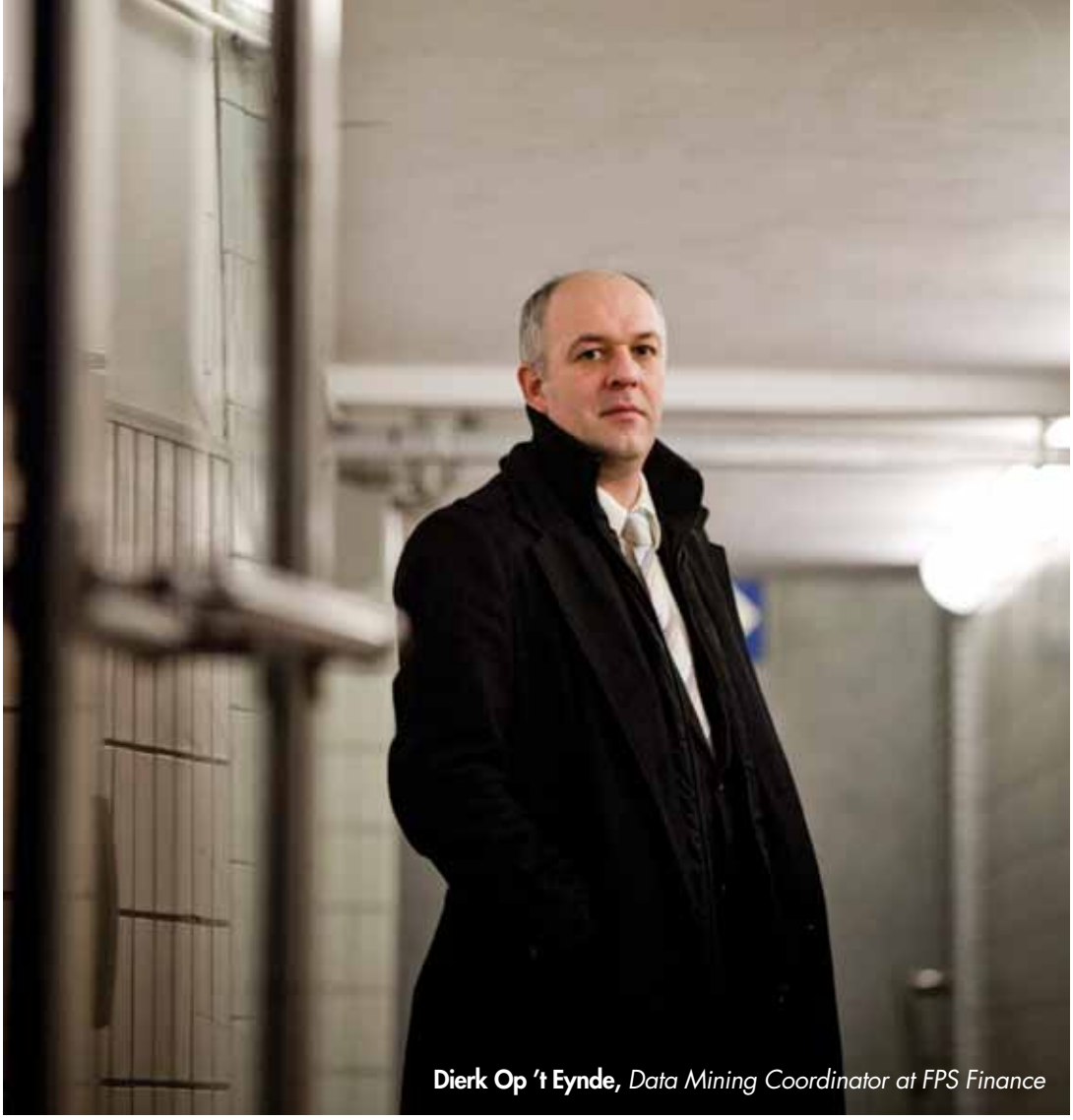
USER-FRIENDLY

One of the things that Op 't Eynde really appreciates is the fact that the huge range of analytical options offered by SAS is accessible via user-friendly wizards. "On the one hand it means there's a fairly short learning curve for new users. While on the other, more experienced users enjoy the added value of taking the next step to proper development. Of course, it is all strictly within the well-defined standards for nomenclature, documentation and version control."

The same strict rules and regulations apply to data quality. "Let's not fool ourselves," Op 't Eynde insists, "no single administrative databank is perfect on quality. That's why, in order to get as close to perfection as possible, we have initiated two strategic programs. First, there are major efforts underway to modernize operational applications and to make historical versions of the data available for exploitation by building a data warehouse. Second, we are deliberately making great efforts to ensure development, databases and infrastructure are more uniform and standardized." IQ

online

SAS Belgium and Luxembourg:
sas.com/belux



Dierk Op 't Eynde, *Data Mining Coordinator at FPS Finance*

WHERE DOES YOUR INSTITUTION RANK IN FRAUD PREVENTION?[1]

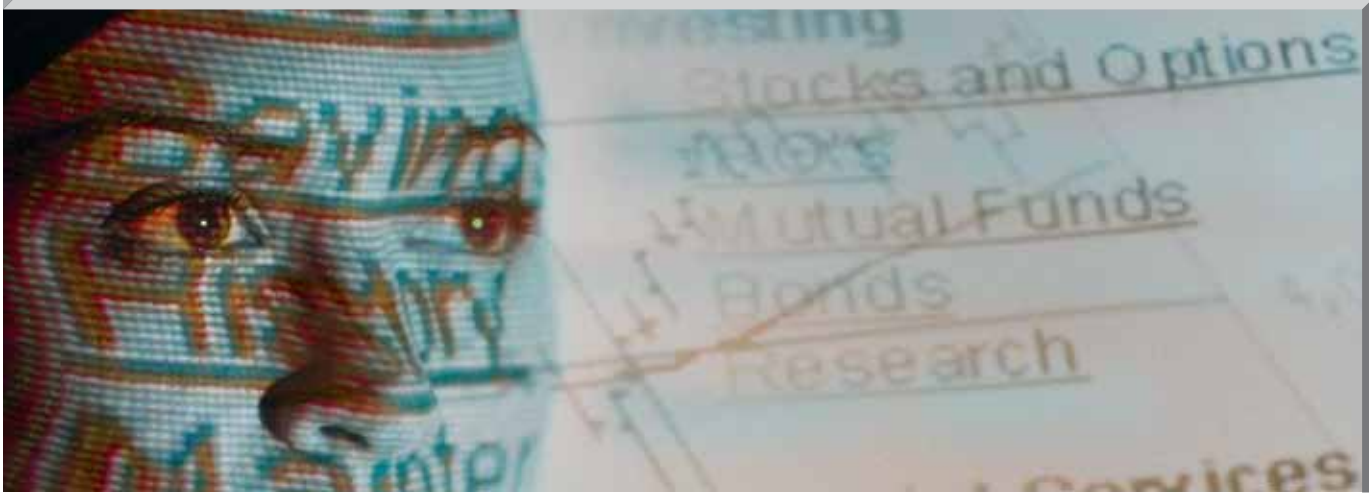
- **Level 1** companies aren't using any tools and can't measure the sources of fraud or the magnitude or direction of payments risk.
- **Level 2** companies have processes and tools, but still base investigations on intuition, tend to keep information siloed, and may not properly apply or understand the technology outside the immediate project team. The debit card side of the house often doesn't know about the customer's checking account habits. And the rich demographic data the marketing side uses to acquire and retain customers isn't used to help understand the customer from a risk perspective. Measuring success isn't common.
- **Level 3** companies have defined processes and use tools to acquire data and assess fraud and risk. However, the ad hoc tools used to acquire data and manage fraud and risk may not be integrated with one another to make cross-channel communication and measurement effective.
- **Level 4** companies have a managed and measured approach. These institutions can benchmark themselves against industry performance, have processes in place to understand and root out new types of fraud, and consider fraud potential prior to entering new businesses.
- **Level 5** companies are optimized. A portfolio approach is used to aggregate enterprise-level, cross-channel payment risk. These companies are completely up to date with regulatory compliance and relevant regulatory guidance.

Learn more: **sas.com/reg/wp/corp/31730**

USING ANALYTICS TO PREDICT FRAUD

Irish tax officer describes how

Duncan Cleary Senior Statistician in Revenue, Irish Tax & Customs



Today, governments and their public sector agencies everywhere are under pressure to perform more efficiently and effectively; essentially, doing better with less. Tax and customs authorities are no exception, many of which are dealing with decreased resources and ever-increasing risks, often in difficult economic circumstances.

Traditional methods for addressing risk have served many authorities well, but there is now a need to use more advanced methods to combat fraud, error and waste. To arm themselves for this battle, more and more tax and customs authorities have turned to data mining and analytics to improve their business processes, resulting in better compliance with new rules and regulations and better customer service.

So where does data mining fit into the risk analysis toolkit of a tax authority? Business rules aimed at detecting risk – and the intelligence gathered from differing channels – have their place and can be effective. Add data mining to the mix and you've got a powerful combination to prevent and detect fraud and error.

Data mining can be defined as the application of the scientific method, including statistical analyses, to large amounts of data to uncover valuable information from that data. It can often detect patterns in data that cannot be recognized manually, as well as make predictive estimates of outcomes of interest, such as the likelihood of a tax return containing errors. Broadly speaking, there are three types of data mining that can be used to combat fraud:

1. Supervised techniques (also known as predictive analytics), where a target is predicted.
2. Semi-supervised techniques, where some business knowledge can direct the analyses.
3. Unsupervised techniques, such as segmentation, which are exploratory.

FIGHTING FRAUD WITH PREDICTIVE ANALYTICS

By creating a predictive model, predictive analytics uses a specific set of data that contains known outcomes for a particular target. This target could be likelihood to yield if a case is audited, the likely amount of yield, the likelihood of a business failing, the likelihood of a claim for benefits or refunds being fraudulent, and so on.

Models perform better where the target has been clearly defined. Techniques for creating predictive models are numerous, but it is often hard to beat the well-established warhorses: logistic regressions, decision trees and neural networks.

The real power of predictive models comes from their ability to score new cases against some target of interest, even if these cases or events have never been previously evaluated. Cases can be ranked in descending order of priority and worked according to resources and the severity of the risk. Feedback is critical to evaluating model performance, and improving models is an iterative and cyclical process. Feeding information back into the model will help reduce the number of false positives (false alarms) over time, as well as reducing the number of actual bad cases escaping attention (false negatives).

Many tax agencies are now using these predictive techniques, in conjunction with their other tools such as business rules and intelligence, to prevent and detect fraud and error. Some have even deployed these techniques in real time in their live transactional systems, including the Irish Tax and Customs authority.

EXPLORING FRAUD WITH UNSUPERVISED TECHNIQUES

Unsupervised techniques can be a powerful means of understanding your case base. Often there is so much data available that it is difficult to understand the underlying structure of the population without using such methods as cluster analysis and segmentation. Especially if a target is not available, cluster analysis can help identify groups in the population that are alike within the group but different from members of other groups.

Once segmented, cases can be assigned a group membership. This label can be used to determine treatment strategies, identify service channel options and even monitor the effectiveness of a tax authority's efforts to change taxpayer behavior over time.

COMBINING METHODS: SEMI-SUPERVISED TECHNIQUES

Additional insight can be gained from overlaying outputs from unsupervised techniques with supervised techniques and vice versa. Some segments might emerge as inherently more risky, thus semi-supervised techniques are often useful where some business knowledge can be used, even where only minimal training data is available.

Outlier detection, where anomalies are identified and investigated, also can be an important weapon in the fight against fraud. With any population, there will always be anomalous cases, many of which will be perfectly legitimate. However, some cases may point to fraud, and these can be identified and investigated.

The network view of the case base is also becoming increasingly important in detecting fraud and error, with group risk and risk propagation through a network of connected entities becoming increasingly easier to detect using techniques such as social network analysis. Unstructured data – including text, voice, image and spatial data – has just begun to be used for fraud detection on a large scale, and its importance and usefulness will undoubtedly grow in the future. Since tax authorities have the unusual position of having population data, not just sample data, there are few limits to how data mining techniques can be used to improve their performance.

MAKING ANALYTICS A CORE PART OF YOUR PROCESSES

So what is there to prevent the use of data mining techniques in a tax authority? There are many potential obstacles: lack of good quality data, data that has not been integrated or merged, lack of skilled resources, lack of senior-level sponsorship, IT challenges and cultural challenges.

Do not let these – or other issues – stop you from using advanced analytics to detect fraud, or stop you from using data mining to improve an agency's performance. Starting with a small achievable project with a clearly defined goal can often be the first step on the path to success. The results do not need to be spectacular, but if they show how data mining can add value and potentially reduce fraud and error, then the case will be made and analytics can start to become a core part of the agency's business processes.

Ultimately, it is the taxpayers and citizens who will benefit the most if the public sector adopts data mining as part of its day-to-day business. So if analytics can help to reduce fraud, error and waste, then the taxpayers deserve nothing less. IQ

online

SAS Ireland:
sas.com/ireland/

Duncan Cleary is a Senior Statistician in Revenue for Irish Tax & Customs. He specializes in the use of research and analytics methodologies and their application in the Irish Tax & Customs Authority, including the use of predictive analytics, customer segmentation, risk analyses, large scale surveys, evidence-based decision support, social network analysis and real-time risk.

IQ

JOURNAL OF ADVANCED ANALYTICS

3Q 2012

SAS Institute Inc. World Headquarters +1 919 677 8000

To contact your local SAS office, please visit: **www.sas.com/offices**