USING INDICATORS AND INTERNAL DATA TO FORECAST FRAUD

The presentation will examine the common forms of both internal and external fraud and will look at how specific risk indicators that can be used to monitor exposure to such fraud. This presentation will also show how an internal loss event data can be mined to detect potential internal fraud in such events. It will examine behaviour and red flags and will focus on “KYP” — know-your-people requirements.

MIKE FINLAY
CEO
RiskBusiness International Limited
United Kingdom

Mike has over 25 years’ experience in banking and finance, having started out pricing equity derivatives on the Johannesburg Stock Exchange. The majority of his career has focused on risk, specifically in the middle- and back-office environment. He has been responsible for establishing new business departments in the derivatives area, restructuring international payments businesses, developing regulatory banking law and implementing risk management frameworks in both international banking firms and in large corporations. He developed the initial risk management framework for the Bond Market Exchange of South Africa and led the integration of all trading and financial risk management activities across a leading mining and industrial conglomerate, while on the insurance side, Mike worked with insurance companies in developing an operational risk methodology to support the requirements of Solvency II. More recently, Mike worked on the development of the KRI Framework underlying the KRIeX.org KRI Library, the development of the KRI Library itself, and on the development of loss data consortium requirements for several national and regional banking associations and consortia, as well as leading a large multi-million Euro project in the area of risk and control self-assessment. Mike has also led scenario-based ICAAP assessments, assisted firms in achieving AMA accreditation, and recently assisted a leading Western European regulator conduct their 2010 AMA accreditation review programme.

Part of the focus on risk has included technology, risk assessment, and training. Mike is a frequent lecturer on operational risk for banking supervisors at the Bank for International Settlements, as well as at industry conferences and seminars. Mike is a regular guest lecturer on risk management at Judge Business School, Cambridge University, as well as at the University of South Africa (UNISA). He has worked with the World Bank/IFC in the Russian Federation and across Eastern Europe, as well as with the Financial Services Volunteer Corps and the BIS’s Financial Stability Institute in ongoing risk management education and knowledge transfer in Europe and Africa.
Mike obtained a bachelor’s of commerce degree from the University of the Witwatersrand, Johannesburg and read for an MBA from Henley Management School/Brunel University through the Graduate Institute of Management and Technology in South Africa. He is a Fellow of the South African Institute of Bankers, a Director and Fellow of the Institute of Operational Risk, a member of the Association of Certified Fraud Examiners and a Charter Member of Risk Who’s Who. Mike was recognised in January 2009 by OpRisk & Compliance magazine as one of the “Top 50 Faces of Operational Risk” and was responsible for RiskBusiness being awarded one of ten “Ten Years of Operational Risk Achievement Awards.”

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
Introduction
My background lies within the financial services industry and thus the content of the presentation is shaped by the regulatory environment, market practices, and commercial dealings within this industry, although they are, in my mind, equally relevant to all industry types. The global financial services industry is driven by two key regulatory concepts, that of Basel II and III for banking and in insurance, Solvency II. Both concepts are risk-focussed and both recognise and incorporate fraud as a manifestation of what is known as “operational risk.”

Definitions
Fraud has many legal nuances and can manifest itself in many different ways, so it may be useful to start with a simple definition:

Fraud essentially involves an act or acts of deception to dishonestly make a personal gain for oneself and/or create a loss for another, either in cash or kind or by avoiding an obligation.

The fraudster has:
- An intention to deceive, and
- An objective to influence the victim’s decisions or actions.

It is not necessary to intend to cause a loss to the victim or make a gain for themselves. The criminal act is the attempt to deceive and attempted fraud should, therefore, be treated as seriously as accomplished fraud. The definition applies irrespectively whether the fraudulent act involves a member of staff (or a relative), acting alone or in collusion with a third party (internal fraud) or merely any third party (external fraud).

The term fraud commonly includes three primary manifestations:
### Using Indicators and Internal Data to Forecast Fraud

- Theft, embezzlement, forgery, misappropriation and money laundering
- Deception, false representation, and concealment of material facts
- Corruption, conspiracy, bribery and extortion

What is an “indicator”? Basically, it is almost anything you want it to be! It is a metric, a piece of data, a piece of information, a statistic, a trend line, a deviation, an exception, etc. Essentially, it is something informative that has value to one or more consumers at a particular point in time.

Typical forms of indicators include economic indicators, risk indicators, performance indicators, and control-effectiveness indicators. Depending on the specific issues being considered at any point in time and the importance and/or relevance of a specific indicator, that indicator may be considered a “key” indicator, giving rise to the concept of “key economic indicators” (KEIs), “key risk indicators” (KRIs), “key performance indicators” (KPIs) and “key control effectiveness indicators” (KCI). Indicators are also often accorded a classification based on the nature of the information they portray, with the typical structure reflecting leading, current, and lagging indicators. The financial services industry has invested heavily in trying to establish standards and reference material on indicators and much of this work can be found at [www.KRIeX.org](http://www.KRIeX.org).

The final definition for consideration relates to the concept of “loss data,” that is information about events that have occurred and manifest themselves as an unexpected or adverse impact on the victim. Within the financial services industry, most firms collect data relating to risk events and when they happen, labelling such data as “internal risk (or loss) data,” often pool internal data with industry peers.
(either anonymously or on a disclosed basis), labelling such data as either “external risk (or loss) data” or as “consortium risk (or loss) data”, and may even collect through research or by subscription to vendors, data on risk events published in the media, usually labelled as “public risk (or loss) data.”

The need for a Taxonomy
The term “taxonomy” is derived from the ancient Greek τάξις, taxis (meaning “order,” “arrangement”) and νόμος, nomos (“law” or “science”), implying that a taxonomy is the “science of arrangement or ordering of data” according to specific laws or rules for classification. So what?

Fraud, as can be seen from the definition, is essentially the risk of an adverse or unexpected event that harms the victim(s). In order to prevent fraud from happening, we need to understand how fraud can manifest itself. Simply appointing a fraud prevention officer, giving them a budget and telling them to go and prevent fraud provides no guidance. The successful achievement of the instruction or objective cannot be measured and overall, will be comparably less successful than if increasing levels of granularity is employed. Consider directing the fraud prevention officer to prevent internal fraud versus external fraud. Or, within external fraud, to focus on external fraud and theft rather than on hacking, systems intrusion or systems disruption for profit. Focus improves with granularity, so within external fraud and theft, focus on credit fraud rather than on payments fraud and, within credit fraud, on fraudulent lending applications and documentation rather than on fraud during workouts and from distressed debtors.

By classifying fraud event data appropriately, the victim can build up a picture of their exposure to the various
manifestations of fraud over time and can look for patterns, causal relationships, specific risk drivers or periodic malfunction of control structures. Through such analytical detail, defences can be improved and the potential for reoccurrence of such events reduced. Without a detailed, unambiguous, yet user friendly classification structure, it is difficult to conduct an efficient war on the scourge of fraud.

**External Fraud**

Within the financial services industry, external fraud represents any fraudulent act committed by one or more individuals without any assistance from the victim or the victim’s staff or relatives, that is, without internal assistance, information or collusion. One grey area is that of former employees, agents or contractors — at which point do they switch from being “insiders” to being “external”? While there is no definitive answer, the typical guideline is that if the victim has had a period of time where it could have made changes to its normal operating procedures, changed its control measures or where sufficient organisational change could have occurred to make the inside knowledge less useful, then it is treated as external fraud. A rough time measure is often six months.

An issue to be acknowledged immediately is the concept in certain jurisdictions that individuals are considered innocent until proven guilty. This has a significant impact in the manner in which firms classify fraud risk events — even though there may be reasonable evidence of internal assistance, unless there is definitive proof, firms tend to classify such events as external fraud events. This may affect the interpretation and use of historical risk event data; accordingly, it may be beneficial to include in the classification structure the notion of “external frauds suspected of internal collusion.”
Returning to the fraud definition for a moment, it is important to note the accent placed on the “objective to influence the victim’s decisions or action,” as this often delineates risk events that straddle the border between internal and external fraud. Consider the situation where a vendor deliberately “wines and dines” the procurement officer to improve the probability of winning some specific business. There is no doubt that the objective is to influence the decisions or action of the firm while the procurement officer is enjoying some benefits that they should not actually receive. While several jurisdictions, such as the UK with its Bribery Act, are seeking to address these issues, they will always be difficult to prove and police — has the firm actually suffered an “adverse or unexpected event” as the result of the wining and dining? Perhaps not, it may actually have benefitted.

**Internal Fraud**

Conversely, internal fraud consists of three primary sub-forms: an insider who acts alone for their own benefit, groups of insiders acting for their collective benefit, or insiders who act in association with outsiders whereby the insider receives some benefit. What is crucial with regard to the third form is that it includes collusion and coercion, although coercion where participation reflects no willingness is often excluded. Take for example an individual who incurs significant gambling debts and who is then approached and informed that they would be exposed to their employer or perhaps injured unless they do something fraudulent, as opposed to someone whose family is taken hostage and is then forced to do something. In the former case, the individual had the chance not to engage in the activity, hence is a fraudster, while in the latter, there was no choice.
Using Risk Event or Loss Data
Risk or loss data is often divided into two groups, data representing “expected losses” and that representing “unexpected losses.” This is best described by an example where a firm issues credit cards and accepts that every year it will suffer a certain level of loss due to fraudulent activity, composed of very small events, which in order to prevent, would cost the firm more than it loses through such fraudulent activity. This is expected loss. Unexpected losses are, then, those that are unusual, untypical or of such significance that it would benefit the firm to invest in preventing them occurring again. Many firms even price for expected loss; that is, they ensure that they charge their customers and clients a base-level fee that reimburses the firm for the expected losses that they will suffer.

It is crucial for a firm to record information on such events and to track it over time, if only to ensure that its “transfer pricing” or recovery from customers and clients is sufficient to offset the actual losses incurred. If, for example, a firm loses an average of €11.50 per credit card in issue, has an operating cost of €6.50 per card per year and charges clients an annual fee of €20.00; then that firm makes a profit as long as its cost remains at €18.00. But if fraud costs rise to €15.00 per card per year, the firm is now incurring a loss of €1.50 per card in issue per year.

The same applies to unexpected losses — mining the data can provide crucial and important information to the firm. If the average loss is €100,000 per month, that does not necessarily imply that the actual run rate is at that level. If an analysis of the event timing reflects that, in six months of each year, the average loss amount is €30,000, this implies that in the remaining six months, the average loss is actually €170,000 per month. If the analysis then shows that these six months reflect two time periods, high summer
and the end of calendar year festive season, this has very important connotations for fraud prevention activity.

If risk (or loss) events are properly classified and if they include a complete representation of what actually happened, such data can provide a rich source of information for the war on fraud. An informative risk event would contain data on timing, involved individuals and entities, the processes in which the event initiated and then was detected, information on controls that failed and worked, specific products that were involved, geographic and organisational information and possibly, even causal information.

Business activity normally follows the path whereby inputs are processed and some desirable and expected result occurs, as depicted below:
Risk events occur when some causal factors manifests itself and as a result, there is an unexpected or adverse consequence to an intended action, as depicted in the following diagram:

To prevent this, firms invest in controls so as to enforce the achievement of the expected outcome:

By “mining” such events, the fraud investigator can focus on two areas: which controls failed (and why) and what were the causal factors. By identifying whether the causal factors were internal or external, the investigator is better positioned to classify the event as either an internal or external fraud, while the analysis of failing controls can
confirm (or disprove) possible internal collusion or coercion.

Let’s take an example and mine the data to identify what actually happened between Lehman Brothers and Marubeni Corporation.

Lehman Brothers Holdings Inc. has gone to court in Tokyo in an effort to recover $350 million it says it was bilked out of through an elaborate scheme in which employees of a big Japanese trading company allegedly used forged documents and an imposter to raise cash.

The purported swindle, which involved the establishment of a partnership to fund the refurbishment of hospitals, allegedly involved two employees of Marubeni Corp., a 150-year-old trading house, according to people familiar with the situation.

The apparent fraud, which could be one of the biggest and boldest in recent corporate history, involved a funding partnership the New York investment bank entered into with a medical consultancy owned by Tokyo pharmaceutical company LTT Bio-Pharma Co. late last year.

Lehman thought the funds it committed to providing to the partnership were backed by Marubeni, based on documents on Marubeni letterhead that bore a Marubeni board member’s seal, which the investment bank later found was forged. At least two meetings to finalize Lehman's participation in the partnership were held at Marubeni’s headquarters, according to the people familiar with the situation.

Lehman has filed a criminal complaint with Japanese police.
and says it believes Marubeni is responsible for repaying the loans. In a statement, Lehman said it was “working closely with the authorities to seek full recovery of funds it believes to have been fraudulently misappropriated.” Lehman said the incident won’t have a financial impact on the company.

In a statement, Marubeni said an internal investigation showed that the company had no involvement in the forgery of documents used to secure the loans. "Accordingly, we have no obligation to pay any of these demands,” Marubeni said. It said it has filed a criminal report.

According to Lehman’s lawsuit, it first learned about the funding operation in August 2007, when a senior vice president of the firm visited an acquaintance at Asclepius Ltd., a medical consultancy then in the process of being bought by LTT Bio-Pharma, according to the draft complaint. At the time, LTT Bio-Pharma’s president was a former official of Marubeni’s life-care department, which sells medical equipment to hospitals and other medical institutions.

LTT Bio-Pharma, which completed the acquisition of Asclepius, couldn’t be reached for comment.

After several more meetings, Lehman made an internal decision, on October 24, to participate in the partnership that would be used to help hospitals modernize their equipment and facilities. As part of the deal, Lehman would disburse the funds on a project-by-project basis, a person familiar with the deal said.

To seal its participation in the project, Lehman asked to meet with the two Marubeni employees and Koichi Sato,
the current head of Marubeni’s life-care department to discuss terms, the person said.

The meeting took place October 29, at Marubeni’s headquarters, next to the sprawling grounds of Japan's Imperial Palace. When the two Marubeni employees said Mr. Sato couldn’t attend, the Lehman representatives agreed to an initial disbursement but asked for another meeting.

At another meeting at Marubeni headquarters, November 8, a man identifying himself as Mr. Sato met the Lehman team and presented Marubeni business cards, according to Lehman’s lawsuit. Lehman’s first disbursement of funds was for 9.8 billion yen ($98.8 million) to help modernize four hospitals. The investment bank received a receipt promising repayment by February 29, 2008. The receipt bore the name of a Marubeni board member and a seal. Lehman later provided four more disbursements.

Lehman grew concerned at the end of February when the initial repayment wasn’t made. It turned to Marubeni seeking to recoup its money. Lehman began to suspect fraud when it asked to meet with Mr. Sato again and a different man — the real Mr. Sato — appeared, according to a person familiar with the situation.

In a statement, Marubeni said the two employees used a company meeting room without authorization for business related to Asclepius. It also said the contracts and business documents for the deal didn’t conform to its style and practices. “Marubeni is a victim of having agreements and other documents forged in its name,” the company said.

Source: RiskBusiness International Limited, Public Loss Data Service
Form of fraud: For Lehman Brothers, it is external fraud, for Marubeni, its internal fraud.

Good controls: Documentation verification, onsite meetings, board minutes, meeting with director, client due diligence.

Weak controls: Disbursement controls.

In general, mining historical data provides information on the past, but does not typically assist in preventing fraud in the future. The exception is where the fraud is ongoing and trends give clues as to either the identity of the fraudster or the modus operandi, which in turn, assists in identifying the fraudster. However, it can and often does generate crucial evidence to facilitate achieving a conviction, thus should never be overlooked.

But, as I am sure most delegates would ask themselves, how does this help us in the battle to prevent fraud before it even begins? As may be expected, the answer is: It does not. All it can do is assist in strengthening defences, not preventing actual fraud events.

**Defending the Firm**

While many firms have invested heavily in systems aimed at trying to identify fraudulent activity, the vast majority of such systems are dependent on rules based on what has happened before. Further, such solutions also usually kick in when the fraud is already in progress, so they do not act as a preventative measure to stop the fraud from starting.

As stated previously, fraud is a form of operational risk. *Operational risk* is typically defined as adverse or unexpected events arising from failed processes (breached controls), system failures and issues, external factors and from things that people do. Of these causal drivers, the root cause of fraud is obviously the *people* factor. No system,
even if armed with regular retina scanning, fingerprint readers or even heat sensors will ever detect the intention of a person to deceive or commit fraud; even so-called “lie detectors” and polygraphs have been proven not 100% accurate all the time.

Accordingly, the first line of defence against both internal and external fraud has to lie where the interaction with potential fraudsters occurs — with external fraud, this is with the account manager, the relationship manager, the business manager, the receptionist/teller/security guard who first sees the outsider, welcomes them in and initiates interaction. These individuals need to be trained in key fraud suspect detection skills, so that the red flag can be raised at the earliest opportunity.

With internal fraud, it is the direct supervisor or line manager who carries the onus of identifying the possibility of fraudulent behaviour. It is these people who, through their regular and ongoing interaction, need to be aware of changes in behaviour, changes in appearance, deviation from routine, anything out of the ordinary. Some firms are of the opinion that the responsibility for this lies with either the fraud squad or in the Human Resources function, but if these units have only infrequent (at best) contact with the suspect, how can they ever detect subtle changes in personality, behaviour, attitude, mindset or appearance? It is for this reason that firms are increasingly providing staff managers with training in the area of “know-your-people” or KYP; this empowers the staff manager to identify unusual behaviour, key changes in dress, attitude, bearing, appearance, speech, and other minute details that may provide an early indication that something has changed and that may require monitoring or investigation.
Another issue of relevance relates to national and regional culture that may affect a firm in a number of different ways. The national attitude towards crime, and specifically towards white-collar crime, may encourage or suppress fraudulent activity. While correctly or incorrectly, certain nationalities gain a reputation for certain things — talk card skimming and Romanians are the prime suspects, forged currency and its Bulgarians, advance fee fraud and the Nigerians, or cyberwarfare and the Chinese. This has an impact on a multi-cultural workforce, as is typically found in EU firms and for the firm when seeking to expand into new territories. From a risk management perspective, it implies that the same techniques may not always work in the same manner in every location.

However, a technique that can be useful is employing indicators to look for trends and to provide information on the current exposure to fraud levels.

**Using Indicators to Forecast Fraud**

As discussed during the introduction, indicators are essentially bits of information that have meaning at some point in time. However, by definition, this implies that, by the time management receives and acts on indicator data, they are responding to and acting on the past. Ignoring trends over time for the moment, indicators are typically lagging in nature and, at best, a measure of current exposure and seldom leading metrics of impending problems.

Consider some of the following typical indicators used by financial services firms in the fraud area:

- Number of fraudulent loan applications received
- Number of forged customer signatures detected
- Number of complaints about unauthorised transactions
- Number of cheques drawn on accounts without funds
Using indicators and internal data to forecast fraud

- Number of credit cards reported stolen

With each of these, something has already happened and, accordingly, the current value of the indicator does not provide any guidance of whether the exposure is increasing or decreasing. The trend over time and, in particular the delta from one measurement period to the next, provides an indication as to whether the exposure is increasing or decreasing. Indicator data tracked over periods longer than 1 year also assist in identifying time-related trends, seasonal swings and possibly inter-relationships with other metrics when tracked on a similar scale.

There are also internal and external indicators to monitor. Internal metrics relate to information about the firm, its customers, its staff and its business activity, while external metrics relate to the environment within which the firm operates. Some examples are:

- Number (and value) of fraud losses suffered by the firm
  - internal
- Number (and value) of fraud losses within the industry
  - external
- Number of suspicious transactions detected and reported — internal
- Number of arrests by police — external

A different set of metrics, often monitored for internal fraud purposes and which thus focus more on staff information include:

- Number of staff with identified financial problems
- Number of staff exhibiting changes in working patterns
- Number of staff exhibiting unusual behaviour patterns
- Number of staff leavers without exit interviews
- Number of staff resigned while under investigation
Again, none of these metrics by themselves provide any information on future fraud levels, although the two focussing on changes on working patterns and behaviour may allow the relevant staff manager to monitor the situation and possibly reduce possible loss, if picked up in time. Remember also that national and regional differences may have an impact on both the usability of indicator data and on what data can efficiently and reliably collected.

Where indicators can become more forward looking is where multiple indicators that have specific relationships with each other can be grouped and considered together, perhaps even as an index that, when the index starts moving, provides a measure of increase or decrease in fraud exposure. The most difficult aspects in developing such metrics is identifying those bits of information that actually relate to each other. This can be done using, for example, factor analysis or principal component analysis.

Examples of the kind of metrics that could be used to create an index are:

- Number of staff exhibiting unusual behaviour
- Number of days scheduled holiday for key staff
- Number of scheduled cash in transit deliveries
- Number of armed robberies within the industry

Note that of those listed above, the latter is external industry data. By equating these at a point in time to zero or 100, any deviation can then be monitored. This may provide an early warning to a change in the firm’s exposure levels.

What is important when using indicators to monitor fraud levels is to employ thresholds and automated alerts to assist in the monitoring process. Thresholds are essentially upper and/or lower limits which, when the indicator value
breaches such thresholds, an automated alert is sent to predefined individuals, using email, SMS, or other communication techniques. Thresholds can also be layered, allowing for escalation to higher and higher levels of authority, as and when required.

Summary
It is crucial for fraud-related data to be properly classified at a relatively granular level, both as relates to the kind of fraud itself and for all supporting information that may give context to how, when, where and why the fraud happened, as well as who was involved. Once fraud data is properly classified, standard data mining techniques can be applied to identify correlation, similarities, and specific causal drivers; all of which can then be used in the war against fraud to try and prevent fraud cases reoccurring.

While this is crucial for improving our defences, it is relatively static, as it only can address what has already happened. It is thus just as important to also research and analyse fraud data relating to cases that happen to other firms or individuals. This can provide us with information on other manifestations of fraud that we may not yet have experienced and can then allow us to introduce remedial measures before that kind of fraud actually affects us.

Indicators provide primarily static information on what has happened in the past and what exposures we may have at the present point in time. If collections of indicators can be combined, that may give us a degree of forward-looking exposure measures, especially if combined with appropriate thresholds and automated alerts.

However, the most effective counter-fraud measure against internal fraud has to be for staff managers to practice KYP and to be alert for changes in behaviour, attitude, approach.
and/or working patterns. Similarly, the best measures against external fraud are physical security measures that allow external individuals to be monitored when they are within the firm’s environment, suitable due diligence and know-your-customer (KYC) checks, and strong controls around any area of the firm’s activities where cash is handled or funds can be moved.