ISOLATE AND ELIMINATE FRAUD THROUGH ADVANCED ANALYTICS

With ever-increasing data volumes, more sophisticated fraud patterns, and a drive for strong corporate governance, how can organisations build a culture of integrity and compliance? Learn how data analytics can be used as one of the tools in the arsenal of an organisation’s anti-fraud programme to detect, prevent, and deter fraud more effectively. This session also covers some of the solutions available in the market to help organisations simplify their efforts to catch increasingly sophisticated fraudsters.

BENJAMIN CHIANG, CFE, CISA, CA
Partner, Ernst and Young Advisory
Singapore

Benjamin Chiang is a Partner in EY’s Advisory Services Practice. He is a Chartered Accountant (CA) of Singapore, Certified Fraud Examiner (CFE), and Certified Information Systems Auditor (CISA). He has more than 18 years of IT audit and security consulting experience, with a focus on IT security governance, process and technical security assessments, fraud risk assessments, computer forensics, and incident response management. He was previously a senior internal audit manager, leading the IT audit function for a Nasdaq-listed MNC.

“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, republished, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
A. The Risk of Fraud Is Increasing as Fraud Continues to Evolve
1. For today’s business organisations, fraud is inevitable.
2. With the recent economic downturn, many businesses have gone through reengineering, reorganisation, or downsizing, which might weaken or eliminate control.
3. Massive amounts of personal information collected by a range of organisations and companies also present opportunities for fraudsters.
4. While the development of new technologies, mobile applications, and automations has provided additional means by which criminals might commit fraud, the technology might also be utilised to detect and respond to fraud faster and more effectively.
5. Cyber threats continue to multiply due to connectivity, and the security defences of organisations are under increasing pressure, further eroding the traditional perimeter and, in turn, creating more motivation for fraudsters.
6. Cyber security breaches have already happened. Are you aware of them? How well are you protected for the future?

B. Why Should Organisations Be Concerned?
1. Fraud has proven costly to organisations and companies. The 2014 ACFE Report to the Nations on Occupational Fraud and Abuse shows that with the typical organisation losing 5 percent of its revenue to fraud each year, there’s a potential global fraud loss of $3.5 trillion.
2. A recent study done by EY in 2015 across the Asia-Pacific has also revealed that it is not just monetary losses organisations should be worried about, but also the potential loss of valuable talent, as ethics becomes a vital element in the war for talent.
3. Organisations are also increasingly at risk of cybercrime. Cybercriminals are becoming more organized, and their motivations have evolved from having fun and enjoying the technical challenge to being more politically and financially motivated. (For example, the number of ransomware attacks, such as Cryptowall, will continue to escalate.)

C. What Can Organisations Do to Prevent and Detect Fraud?

1. End-to-end integrity and compliance framework is a holistic program designed to effectively prevent and detect fraud. The program embraces a combination of strategies in the following areas:
   - Policies and procedures
   - People
   - Technology (data and systems)

2. The program begins with governance and tone at the top regarding the organisation’s tolerance of fraud, employee education, fraud reporting, and the organisation’s control, weaknesses, and gaps.

3. In the arsenal of tools and techniques to combat fraud, the adoption of technology and data analytics plays an increasingly important role.

4. The benefits of using data analytics in the fraud management process include:
   - Full population analysis versus sample testing
   - Broader engagement coverage
   - Improved risk evaluation
   - Focuses scope to identify potential errors early
   - Provides directional guidance by identifying insights (risks, opportunities, and weaknesses)
   - Quantifies the impact of errors and problems
   - Efficiencies gained through repeatable procedures
   - Enhances understanding of processes and systems
   - Deepens understanding of root causes
### ISOLATE AND ELIMINATE FRAUD THROUGH ADVANCED ANALYTICS

- Efficient technique for testing large populations

### D. How Can Organizations Apply Analytics to Detect and Prevent Fraud?

There are many tools available that can be used to perform data analytics. The following are examples of data analytics solutions that are designed for the purpose of managing fraud and compliance within an organisation.

#### Employee Payroll and Expense Management

- **Key challenges in existing processes**
  - All organisations have payroll, expense claims, and reimbursement processes.
  - Some organisations continue to use manual, paper-based processes.
  - More organisations are moving towards e-submissions and paperless environments.
  - Billing, payroll, and expense reimbursement make up the highest proportion of all fraud cases.
  - Common types of expenses
    - Travel
    - Subsistence (while travelling for business or working at remote locations)
    - Entertainment (events and meals with colleagues, customers, business partners)
    - Small-value purchases (e.g., stationery, books, portable hard drive)
    - Allowances
- **Potential red flags in payroll and expense claims**
  - Are all receipts and claims submitted genuine?
  - Examples of potential red flags
    - Photocopies
    - Sequentially numbered receipts
    - Amounts just below the maximum allowed
    - Delays in submission
- **Examples of payroll and expense risks and fraud schemes**
ISOLATE AND ELIMINATE FRAUD THROUGH ADVANCED ANALYTICS

- Payroll risks and schemes
  * Ghost employees
  * Inflated hours
  * Falsified wages
  * Commission schemes
  * Improper incentive compensation
  * Excessive or unnecessary overtime
  * Fund transfers made to unauthorized personnel

- Expense reimbursement risks and schemes
  * Mischaracterized expenses
  * Claiming personal expenses
  * Using refunds or unused credits
  * Overstated expenses
  * Fictitious expenses
  * Falsifying receipts
  * Obtaining counterfeit receipts
  * Multiple reimbursements
  * Excessive spending

- Risk ranking framework for analysis
  - Tests and parameters should be customized to the risk profile of your organisation.
  - While all risks identified within a process might be relevant, some will have varying levels of significance within different organisations.
  - Draws upon a library of analytics tests classified using the ACFE occupational fraud and abuse classification system.
  - Multidimensional analysis and proprietary risk scoring engine identify employees who have the highest risk rating.
  - Organisations are able to establish review priorities and focus resources on high-risk employees.

**Identifying Rogue Trader and Compliance Risks by Focusing on the Information Flows**

- Challenges of traditional investigation methods
<table>
<thead>
<tr>
<th>ISOLATE AND ELIMINATE FRAUD THROUGH ADVANCED ANALYTICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Recent regulatory actions that have focused on the flow of information between people</td>
</tr>
<tr>
<td>– Financial services companies looking for more effective and less costly compliance risk identification techniques that go beyond looking at trade data only</td>
</tr>
<tr>
<td>– Problem for the investigator often lies in identifying trades that might have been based on actual material nonpublic or sensitive information.</td>
</tr>
<tr>
<td>– Conversations taken “offline” and switched to communication channels that are less likely to be recorded</td>
</tr>
<tr>
<td>• Know Your Trader (KYT) Analytics Services</td>
</tr>
<tr>
<td>– KYT Analytics applies statistics, mathematics, text mining, computational linguistics, and the experience of financial service professionals to supplement proven compliance monitoring tools.</td>
</tr>
<tr>
<td>– Tests are identified, based on the organisation’s risk profiles, and an extensive library of analytics is leveraged, including free-text data sources (e.g., emails, instant messages, and documents) and structured data (e.g., trade and order data).</td>
</tr>
<tr>
<td>– Communication patterns are analysed over time, based on specific discussion topics and key words.</td>
</tr>
<tr>
<td>– Management is provided a highly visual and objective format for evaluation and decision-making.</td>
</tr>
<tr>
<td>• Key benefits of analysing communications</td>
</tr>
<tr>
<td>– Help identify key compliance risk factors and patterns indicative of rogue employee activities, such as:</td>
</tr>
</tbody>
</table>

**NOTES**
### ISOLATE AND ELIMINATE FRAUD THROUGH ADVANCED ANALYTICS

- Leakage of material nonpublic information that could lead to insider trading risks.
- Misconduct, fraud risks, or violations of company or regulatory policies.
- Assistance with identifying the “flight risk” of key personnel to thwart defection to a competitor.
- Bribery or corruption concerns that might put a company at risk under the FCPA, the UK Bribery Act, or other country anti-bribery legislation.

- Help increase detection maturity by integrating customized analytics that incorporate text mining and communication patterns relevant to the organisation’s risk profiles.
- Through visual analytics, allow management to identify anomalies that are only evident when taking into account the multidimensional attributes in the data, especially in the intersection of written communications and trading data.

### Other Fraud Management Tools and Applications

- The evolution of technology
  - Advancements in hardware and software, leading to increased computing power
  - Significant reduction in cost and time to store and process data
  - Availability of applications developed specifically for fraud management that leverage the power of data analytics
  - Continued need for solutions to be customized for each organisation

**EXAMPLE: DETECTING AND PREVENTING ENERGY FRAUD**

- *Integration with virtually any data source, including mainframe systems*
## ISOLATE AND ELIMINATE FRAUD THROUGH ADVANCED ANALYTICS

- Can screen large amounts of data, using a wide array of proven detection algorithms (detection methods)
- Real-time calibration and mathematical optimization of weightings between algorithms, making fine-tuning detection easy
- Raises alerts for each suspicious situation
- Alert classification results stored within SAP Fraud Management, which become available for the detection of future fraud cases
- Advanced analytics’ (e.g., predictive methods) use of classified fraud cases for self-learning algorithms so the system’s detection efficiency increases over time

### NOTES

- Traditional challenges in detecting energy theft
  - Limited amount of data
  - Lacking algorithms to detect theft
  - Manual process of detection
  - Breaks in investigation process
- A few facts about energy theft
  - The theft of electrical energy is a serious and costly issue, especially in developing countries.
  - Studies estimate the cost of nontechnical losses (NTL) to be between 1 and 15 percent—up to 30 percent in some countries.
  - Financial losses go into the billions. One study estimated US$6 billion in the United States alone.
  - Early detection, as well as efficient management of the findings, can lead to a quick recovery of millions of dollars in revenue for utility companies.
EXAMPLE: CYBER-THREAT INTELLIGENCE

- Analytics can be used as a form of real-time cybersecurity threat detection.
- Tools allow detection, intervention, and reporting on high-volume and velocity-streaming data.
- Typical employee behavioural trends and patterns can be identified, allowing for easy detection of anomalies.
- Authorized personnel who perform unauthorized activities is a red flag.

E. Conclusion

Data Analytics Is a Powerful Weapon Against Fraud

- The risk of fraud and other unethical behaviours are on the rise.
- Fraud and challenges to fraud are evolving.
- The cost of fraud is high—monetary losses, talent wars, data leaks.
- Organisations need to deal with fraud holistically.
- Technology and data analytics play an increasingly important role in isolating and eliminating fraud.
- Data analytics can be used on structured and unstructured data across multiple processes.
- There is an increasing number of analytics tools designed for fraud management, but they are not plug-and-play appliances.
- Experienced compliance, internal audit, and anti-fraud professionals will be required to customize and make the tools work effectively.
- Do not wait until a fraud has been detected to develop a fraud response plan.