CONTINUOUS FRAUD MONITORING AND DETECTION
VIA ADVANCED ANALYTICS

Business analytics and big data are highly publicised terms, but what is the core value proposition? The advent of systems automation, enhanced by advanced analytics, has established the capacity for continuous fraud monitoring and detection solutions. This session will provide an overview of the main advanced analytics techniques available to tackle the problem of fraud, and a practical case will be examined in order to demonstrate the principles at work for a hands-on perspective.

SCOTT MONGEAU, PH.D.
Manager
Deloitte
Netherlands

Scott Mongeau has more than 20 years of experience in project-focused analytics functions in a range of industries. He is an active university researcher; lecturer; conference presenter; and writer in the areas of business analytics management, decision analysis, decision model management, model risk, organizational management, social network analysis (SNA), evidence-based decision-making, and analytics methodologies. Previously he owned and operated his own independent analytics consulting company, SARK7.

“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.
Fraud Detection and Mitigation via Advanced Analytics: Trends and Directions

Scott Allen Mongeau
Deloitte Netherlands
smongeau@deloitte.nl

Nyenrode Business University
s.mongeau@edp1.nyenrode.nl

ABSTRACT
This paper seeks to summarize trends and implications associated with business analytics and Big Data for the benefit of practitioners working in the field of fraud detection and mitigation. A brief definition of business analytics is offered, followed by an examination of existing and emerging applications to the problem of fraud. It is proposed that the emerging state-of-the-art is a hybridization of advanced analytics methods, increasingly powerful IT hardware, and software systems which manage human workflow related both to forensics and detection model management. Combined with growing market demand, packaged, integrated software frameworks are appearing to fulfill a need for enterprise fraud detection and mitigation solutions. Although yet in the early stages, it is proposed that these solutions will ultimately fuse with 3rd party data providers to serve both established enterprise markets and to provide cloud-based solutions (software as a service) for smaller customers in need of real time credit, risk, and transaction validation services across a range of industries.

Keywords
Fraud, forensics, continuous monitoring, advanced analytics, business analytics, data analytics

Disciplines: Financial / risk managers, investigators, fraud experts, analytics experts

Industries: Financial Services, Credit Provision, Banking, Insurance, Law Enforcement, Public Sector Finance, Risk Management, Corporate Risk Management
INTRODUCTION

Business analytics and Big Data are highly publicized terms, their prolific use leading to confusion concerning their fundamentals. Fraud detection and mitigation is often cited as a use-case for advanced business analytics. The advent of the ability to store and analyze large data sets introduces the prospect of enterprise-scale fraud detection and suggests real-time prevention.

This paper proposes a definition for fraud analytics, examines advanced applications, and explores emerging trends.

but what is the core value proposition? This targeted presentation will drill-in on specifics concerning the use of advanced analytics for fraud detection and mitigation.

The advent of systems automation enhanced by advanced analytics has established the capacity for continuous fraud monitoring and detection solutions. Advanced analytics approaches such as machine learning allow for cyclical fraud detection improvements. An overview of the main advanced analytics techniques available to tackle the problem of fraud will be reviewed. Specific attention will be focused on ‘self-improving’ machine learning approaches. The virtuous cycle of continual improvement for fraud detection and mitigation will be explained as the combination of advanced analytics processes, people managing alerts and cases, and deployment of the proper tools and systems. A practical case will be examined in order to demonstrate the principles at work for a hands-on perspective.

UNDERSTANDING ANALYTICS

Descriptive analytics
Predictive analytics
  ▪ Statistical techniques: correlation (Nigrini)
  ▪ Time series analysis (Nigrini)
  ▪ Machine learning
Prescriptive analytics
  ▪ Optimization (linear programming)
  ▪ Iterative model management
  ▪ Factory metaphor
- Lean / six-sigma
  - Diagnostic analytics
  - Semantic analytics
    - Relational communication patterns
    - Semantic content
    - Hybridization (meaning neworks)
    - Pattern libraries

Analytics is traditionally described as being descriptive, predictive, or prescriptive. Descriptive analytics is retrospective, describing what happened in the past and is associated with the field of business intelligence. Predictive analytics seeks to forecast trends and to determine probabilities. It is associated with time-series analysis, econometrics, and the determination of statistical probabilities. Prescriptive analytics seeks to determine optimal systems states and is associated with the field of operations management and management science.
The designation of diagnostics is increasingly distinguished, involving techniques for identifying and validating models.

Semantic analytics is also an emerging trend, involving the

Visualization is increasingly popularize

With the increasing importance of data, data quality has become a particular area of focus and concern. Data quality concerns itself with issues related to master data governance, particularly ownership, stewardship, and master- and meta-data models.

Big Data is a broad term implying analytics with very large data sets: data which contains many measurements over time and a breadth of variables. The confines of Big Data thus are associated with the engineering challenges of efficiently storing, retrieving, processing, and assessing very large sets of data. Otherwise, the analytics techniques applied are unique only in terms of attempting to detect patterns and trends in large sets.
Big Data also introduces an advancement concerning the ability to rapidly identify reliable predictive models across large sets of variables. Social science traditionally progresses with the identification of a causal hypothesis which is then tested via experimental observational data. The Big Data approach upends this framework by using computational approaches to identify rough correlative models with high predictive accuracy, many times foregoing causal explanation altogether. An example is of Google Flu Trends, a facility made available via Google which is able to reliably predict flu outbreaks in specific U.S. geographic areas based on the propensity of a collection of key search terms. Google does not propose a causal model for the terms themselves, only noting that the collection of terms themselves correlate with subsequent outbreaks of the flu as tracked by the U.S. Center for Disease Control. Similarly, Big Data predictive fraud models need not explain the causal origins of fraud behavior, only be able to correlate sets of key tracked variables with predictive accuracy in subsequent fraud.

These approaches increasingly can be considered a set of tools in a toolkit that can be applied to a range of challenges across a particular domain such as fraud.

UNDERSTANDING FRAUD

- Social problem: taking unfair advantage
- Core factors:
  - Social context: transactional (relational)

All fraud is the outcome of three elements: motivation, opportunity, and worthwhile outcome (Vision on Governance, Risk & Compliance).

Goal: prevention, detection, response

FRAUD ANALYTICS

- Analytics as applied to fraud

Data analytics is being used by a number of large organizations to counter fraud and security threats. Common applications include insider trading, lending fraud, and criminal investigations (Litan, 2013). + academic overview article
A distinction concerns the ability to identify patterns versus predictive power in known models. Identifying patterns can be associated with diagnostics and involves detecting and characterizing the structural characteristics of a particular species of fraud. This is associated with discovery and utilizes both human determination and unsupervised pattern identification, such as cluster analysis (where no patterns are clear in cases). Once identified, patterns can be used to drive predictive detection via supervised techniques (where the parameters which define cases are known).

Increasingly human assessment is combined with pattern identification and Key methods include pattern-based data analysis combined with case workflow software. Linking heterogeneous information sources is key, both structured and unstructured data types, and internal and external sources.

Packaged vendor-based solutions are growing in scale and power.

Industries experiencing particular demand include financial services (banking, lending, insurance, transaction services), enterprise security, government, healthcare, e-commerce, and telecommunications (Litan, 2013).
Figure X. xx

TECHNICAL ADVANCES

- Technical advances: Trends: Hybridization
  - Hardware: real-time / in-memory, cloud computing, big data storage and retrieval
  - Software: forensics and case workflow management (SAP & SAS), unstructured data management, No-SQL / graph databases
  - Hybrid software analytics: machine learning, guided model management
  - Advanced methods: statistical techniques
  - 3rd party data sources: real-time credit and transaction checking, proprietary demographics (to enhance risk modeling and targeting)

Technology providers include Palantir, Detica, SAS, Securonix, Intellinx, and Centrifuge (Litan, 2013).


IMPLICATIONS

- Implications for fraud analytics
CHALLENGES

Organizations seeking to apply fraud analytics must have a clear idea concerning the types of activities they wish to identify and mitigate, the data that is available, and the proper methods to apply. Ideally the organization has an explicit approach to analytics model management, which means there is an explicit effort to design, validate, document, apply, and maintain an end-to-end set of methods and procedures to combat fraud.

An effective enterprise-scale fraud analytics program is a complex system involving the integration of people (organization), processes (methods), and systems (technology). The integration between these factors must be well-considered: how human process-based workflow is facilitated by technical systems to achieve measurable results. Human-computer interaction must be considered carefully, from user interface and workflow design, to the degree to which automated decision systems defer to human experts and vice versa.

CONCLUSION

- Conclusions
  - Cost economics: benefits and parity value with overhead
  - Knock-on benefits of bringing data house in order (regulatory compliance and reporting, sales and marketing)
  - Mirror image of targeted marketing
  - Compelling: operations that become good
  - Concerns and critiques
    - Privacy regulations
    - Cost economics
    - Overhead of getting data house in order
    - Broad social concerns: technically institutionalizing class boundaries
ACKNOWLEDGMENTS
I wish to thank all authors, program and local committee members, and volunteers for their hard
work and contributions to the ACFE Global Fraud 2014 conference. I also wish to thanks my
colleagues at Deloitte Netherlands, particularly Jacques Buiith, Gerrie Lenting, Baldwin Kramer,
and Johan ten Houten.

REFERENCES

Mathematics and Computer Science, Free University of Amsterdam.

(G00247014). Retrieved from Gartner database.

New Jersey, John Wiley & Sons, Inc.

Nigrini, Mark J. (2011). Forensic Analytics: Methods and Techniques for Forensic Accounting
Investigations. New Jersey, John Wiley & Sons, Inc.