Learning Objectives

- Learn the Definition of Fraud Analytics
- Discuss the Purpose of Fraud Analytics
- Identify methods on how to use Existing Data
- Review examples of how Fraud Data Analytics can be used
- Identify common barriers to implementing Fraud Data Analytics and how to manage them
“Know your enemies and know yourself, you can win a hundred battles.” This truism from Sun Tzu’s “The Art of War” is as applicable to the battle against fraud as it is to the military battlefield. It is incumbent upon financial institutions to defend themselves and their customers from potential fraudsters.

Implementing fraud analytics is easier said than done.
Definition of Fraud Data Analytics

The definition being used for fraud data analytics is the following:

• Data preprocessing techniques for detection, validation, error correction, and remediation of missing or incorrect data
• Calculation of various statistical parameters, such as averages, performance metrics, and probability distributions
• Models and probability distributions of various business activities in terms of either various parameters or probability distributions
• Computing user profiles
• Time series analysis of time-dependent data
• Clustering and classification to find patterns and associations among groups of data
• Matching algorithms to detect anomalies in the behavior of transactions or users as compared with previously known models and profiles
Types of Statistical Techniques Used in Fraud Data Analytics

There are many types of statistical analyses that can be used. The key is to use those where your organization has expertise and where they can be applied based on your data, infrastructure, and technology.

- Behavior profiling
- Data mining
- Neural networks
- Artificial intelligence
- Behavior
- Clustering
- Decision tree
- Regression
  - Parametric
  - Nonparametric
- Peer group analysis/break point analysis
- Many, many more
How would you describe the current level of fraud data analytics used in your organization?

a) Used extensively across products and channels, including transactional, customer, account, and attribute (Web logs, system logs, call detail records, etc.)

b) Deployed some fraud analytics, in the middle of the program

c) Minimal, just starting to use

d) Unsure/don’t know

Based on a recent response of 400 respondents more than 50% indicated that at least some basic analytics were being used.
What types of fraud analytics are used in your organization?

a) Advanced – use of advanced statistical models to augment rules-based and behavior profiling
b) Medium – rules-based and behavior profiling
c) Beginner – rules-based
d) Unsure/don’t know

Out of respondents that either answered some or extensive use of Fraud Analytics more than 50% were in the beginner – rules-based analytics.
The primary reason to use data analytics to tackle fraud is because many internal control systems have serious control weaknesses. To effectively test and monitor internal controls, organizations need to look at every transaction that takes place and test it against established parameters, across applications, and across systems from dissimilar applications and data sources. Most internal control systems simply cannot handle this. On top of that, as we implement internal systems, some controls are never even turned on.

Remember, you’re looking for things that don’t appear to be normal. Calculate statistical parameters, and look for outliers or values that exceed averages or are outside standard deviations. Look at high and low values, and find anomalies there. Quite often, it’s these sorts of anomalies that are indicators of fraud.

Examine classification of data. Group your data – all the transactions – into specific groups based on something like location. Maybe a number of transactions are occurring outside statistical parameters. Where are they from? Are they distributed evenly across the whole population, or are they all limited to a given geographical area? If they are the latter, then that’s material, and maybe you should delve deeper.
Fraudsters can and will exploit weaknesses wherever they can be found. Data analysis has proven itself reliable in fraud detection and prevention in a wide range of areas. We’ve talked about a few already in accounts payable and accounts receivable. Just think about the possibilities for fraud in credit card management. Consider people buying things they’re not supposed to on their corporate credit cards. We’ve had customers find inappropriate purchases, from clothing to $12,000 worth of casino chips.
Areas where fraud data analytics can be used to identify fraudulent activities

Take a look at your general ledger (GL), especially postings done after a closing period. Check into frequently reversed accounts or weekend postings. Look at GL postings on a quarterly basis, and ask:

- Are these being done according to our internal controls, or are people trying to post to the GL after our closing period?
- Are there certain GL accounts that are frequently reversed?
- Are there dormant accounts that are used suddenly?
- These are the little indicators of something worthy of your scrutiny. You should definitely be using repetitive analysis if:
  - You are looking at very large volumes of transactions, no matter the size of the actual transactions
  - It’s for an ongoing period of time
  - An area is identified as high risk for fraud to occur
What Types of Data Does Your Organization Use?

- Transaction
- Application logs
- Account
- Web proxy logs
- Call detail records
- Web access logs
- Database audit logs
- Configuration files
- Clickstream data
- Web proxy logs
- File system audit logs
- Call anomalies fraud detection
- Sys logs
- Application logs
- Account
- Web access logs
- Sys logs
What types of fraud has fraud analytics uncovered in your organization?

- a) Internal and external fraud
- b) Internal fraud
- c) None
- d) Unsure/don’t know

Over 90% of the respondents indicated for the organizations that use analytics that it if for both internal and external fraud.
Fraud Data Analytics Challenges
Fraud Analytics Challenges

1. Identify sources and systems of record
2. Standardization
3. Volume of data
4. Data quality
5. Reporting, ease of use
6. Resource skill sets
Does Your Organization Have?

If your organization is having challenges with fraud data analytics, does it have:

– A fraud analytics process
– Fraud analytics architecture
– Data governance
– Information presentation
Fraud Analytics Process

**Functions**
- Product Development & Pricing
- Marketing
- Customer Relationship Management
- Operations Management

**Products & Channel**
- Wire Transfers
- Cards Debit/Credit/ATM
- Checks & Deposits
- Remote Banking
- ACH

**Data Input**

**Information**

**Analytics**
- Real-Time Scoring
- Queue Management
- Real-Time Rules
- Near-Time Scoring
- Near-Time Rules

**Activities**
- Preset rules
- User rules
- Filters
- Boolean logic
- Score models
- Data mining
- Patterns
- Algorithms
- Statistics
- Alerts
- Key indicators
- Model development
- Model calibration
- Model validation
Architecture to Support Analytics

Transactional Account & Customer Data Sources
- Transaction
- Customer
- Account
- Referrals

Channel System Data Sources
- DBMS
- Firewall
- Phone/IVR
- Logs
- Data Access

Analytics
- Data Extraction Tools
- Data Extract for Analytics Models
- Machine/Access Logs

Analytics Software/Models
- Rules-Based Analysis
- Data Link Analysis
- Unstructured Data Analysis
- Artificial Intelligence Analysis
- Predictive Analysis
- Behavior Modeling

Periodic & Real-Time Analysis
- Fraud Alerts for Investigations
- Data to Be Stored for Root Cause Analysis

Reporting
- Case Mgmt.
- Alerting & Alarming
- Root Cause Analysis
- Continuous Improvement
Does Your Organization Provide Role-Based Information? (Continued)

**Senior Management – Strategic**
Dashboard with KRIs and KPIs
Management reports
Aggregated

**Fraud Analytics – Advanced Analysts – Researchers**
Data mining, ad hoc analysis, predictive analytics
Perform scenario modeling
Behavior profiling

**Fraud Managers**
Standard reports based on user specifications
Ad hoc reports, data slicing, OLAP
Reports with drill-downs
“Data is aggregated/historic/periodic”

**Fraud Analysts – Operational/Administrative**
Granular
Real time/daily
“Data is transactional”
What is Data Visualization

Communication

Information Science

Design
Common Types of Data Visualization

Data Analysis
- Graphs
- Charts
- Maps
- Link Analysis

Text Analysis
- Word Diagrams
- Statistical Analysis for Key Text Words

Combination
- Bubble Charts
Example of Data Visualization
Text Mining
Compensation as a Percentage of Total Program Support

Percentage of Total Program Support

- 56% % Paid as Compensation
- 44% % Paid for other Operating Expenses
Data Visualization Examples

Vendor D

Vendor C

Vendor B

Vendor A

Legend:
- New Vendor
- Invoice Date
- Prior Run
- Hand Deliver
- COI Vendor
Data Visualization Examples

![Bar Chart]
Data Visualization Examples
Data Visualization Examples
Data Visualization Examples
Fraud KPIs and KRIs and Detection/Prevention Rules
Fraud KRI/KPI Development

- Define and measure progress toward organizational goals.
- Identify risks and performance of the group.
- Provide decision intelligence directed toward positive (corrective) action.
- Provide required oversight of internal and outsourced or offshored functions.
- Monitor the health of fraud prevention.
- Focus on key indicators, removing reporting of metrics that do not add demonstrable value.
- Ensure exceptional monitoring capabilities.
- Have full transparency and auditability of information.
- Establish a framework that embeds SLA reporting and review.
- Have standardized metrics and an aggregated reporting framework to enable comparisons at management levels and across functions, locations, products, lines of business, etc.
- Establish a clear hierarchy, ensuring that metrics cascade up and down and providing a defined escalation route for information.
- Enhance data integrity through the use of common sources of data.
- Set and monitor agreed-upon benchmarks for metrics.
Thinking about the frauds you investigated over the past 12 months, what referral channel provided you with the most referrals?

a) Internal Analytics  
b) Fraud Hotline 
c) Law Enforcement  
d) Other
Takeaways

• Fraud strategy needs to exist.
• Concentrate on the data that exists, not on what is desired.
• Start small.
• Create algorithms on existing data; don’t just search for the best algorithms.
• Use internal and external resources with the right skills and expertise.
Questions
Thank You

Brenda Buetow
Senior Manager
Crowe Horwath LLP
Office: +1 317 706 2631 | Mobile: +1 765 318 0919
brenda.buetow@crowehorwath.com

Gregg Henzel
Senior Manager
Crowe Horwath LLP
Office: +1 630 575 4350 | Mobile: +1 303 815 4768
gregg.henzel@crowehorwath.com