July 2017

Fraud Analytics Overview

An article by J. Michelle Abuda, Gregg S. Henzel, and Arjun Kalra, CAMS

Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

With an increasing number of transactions and an ever-growing amount of available data, companies need ways to detect fraud quickly and accurately. Across the board, it is becoming necessary for companies and financial institutions to monitor diverse sets of data. Using statistical methods, or data analytics, financial institutions can detect new patterns of fraud and predict future cases that might require further investigation. The ultimate objective is to decrease fraud losses to institutions and customer bases.

What Is Fraud Analytics?

Fraud analytics programs use historical and current data to identify abnormalities and outliers that may not be detected easily. Outliers in data statistically outside of standard deviations are typically indicators of fraud. Individual transactions may not be suspicious, but a group of related transactions could require further investigation. Analytics are the most effective way of monitoring the large quantities of data and can identify patterns that cannot be found by hand. Summary dashboards produced by analytics teams can also provide an overview of a company's health and highlight areas of concern.

However, simply stating plans to "do analytics" does not do enough to combat financial crimes. Senior management should allocate enough resources to build and maintain fraud analytics programs. Management should also set up a program to monitor the effectiveness of fraud analytics by understanding the potential losses to the institution or customer base. Without a full commitment from the entire institution, fraud analytics programs cannot be successful.[1]

Fraud Analytics Success Stories

One of the earliest examples of fraud analytics dealt with credit cards and payment fraud prevention.[2] In the early 1990s, financial institutions wanting to prevent counterfeit transactions began to use statistical models to sort through the data recorded. Today, thousands of calculations using dozens of statistical models are performed every time a card is swiped to determine if a transaction is potentially fraudulent. Based on this analysis, a determination is made of what action might be required. For example, an out-of-band authentication might occur in order for the transaction to be approved, or the transaction might be blocked automatically. As online purchases using credit cards become more popular, it becomes increasingly important to monitor transactions, as more diverse data needs to be analyzed. Customer account and transaction information, IP addresses, device IDs, click patterns, and social media can all be used to help identify possible fraudulent transactions.

Insurance claims fraud is also a growing area. In a Claims Journal case study, a leading home insurer had to sort through thousands of claims after a major disaster. Even though exploratory analysis was used, new methods to highlight changing trends were needed. Because large quantities of data were captured through the life cycle of a claim, big data analytics had to be used to deal with the new influx of claims. Analytics made the project much more manageable, and were able to pinpoint more potential fraudulent cases.[3]

Fraud Analytics in Your Company

When building a fraud analytics program, companies should implement a variety of methods for identifying unusual patterns. Data analytics can help prevent or recover losses and detect areas for further investigation. For example, a company can look at unusual activity by asking a few key questions: Is there a marked increase in transactions? Are large sums of money being deposited?

Data collected and used in analytic models can be extracted from a variety of sources. One example is transactional data, such as a customer's use of a credit card or activity between multiple accounts. Unusual transaction amounts or increased frequencies might highlight suspicious activity. Another example includes customer data. A customer's purchase in an unusual location might make certain transactions appear more suspicious.

Analytics use a range of statistical methods, including clustering, decision trees, neural networks, or regression models.[4,5] Predictive models can help identify potentially fraudulent transactions and individuals and prevent further loss. Regression models can detect outliers in the data or highlight trends that could be significant. The number of possible techniques is endless, which is good news for institutions trying to prevent fraud.

However, companies seeking to implement fraud analytics programs face a few hurdles to overcome. Cost is one of the biggest issues that institutions struggle with.[6] It is expensive and time consuming to find individuals with the statistical abilities to run an analytics program. The hardware and software technology to run an analytics program can be a large upfront investment as well. On top of the startup costs, an analytics program demands more resources over time to investigate the leads that will be generated and to perform root-cause analysis of fraudulent activities. Root-cause analysis results can be used to feed back into detection models in order to improve detection rates and limit false positive rates. The architecture to support data analytics is another consideration when setting up a fraud program. Data from a variety of sources – including transactions, accounts, customer data, and channel system data – can be extracted and fed into analytics models. Analytics software and models can vary, and the selected models should support the goals and resources of the organization.

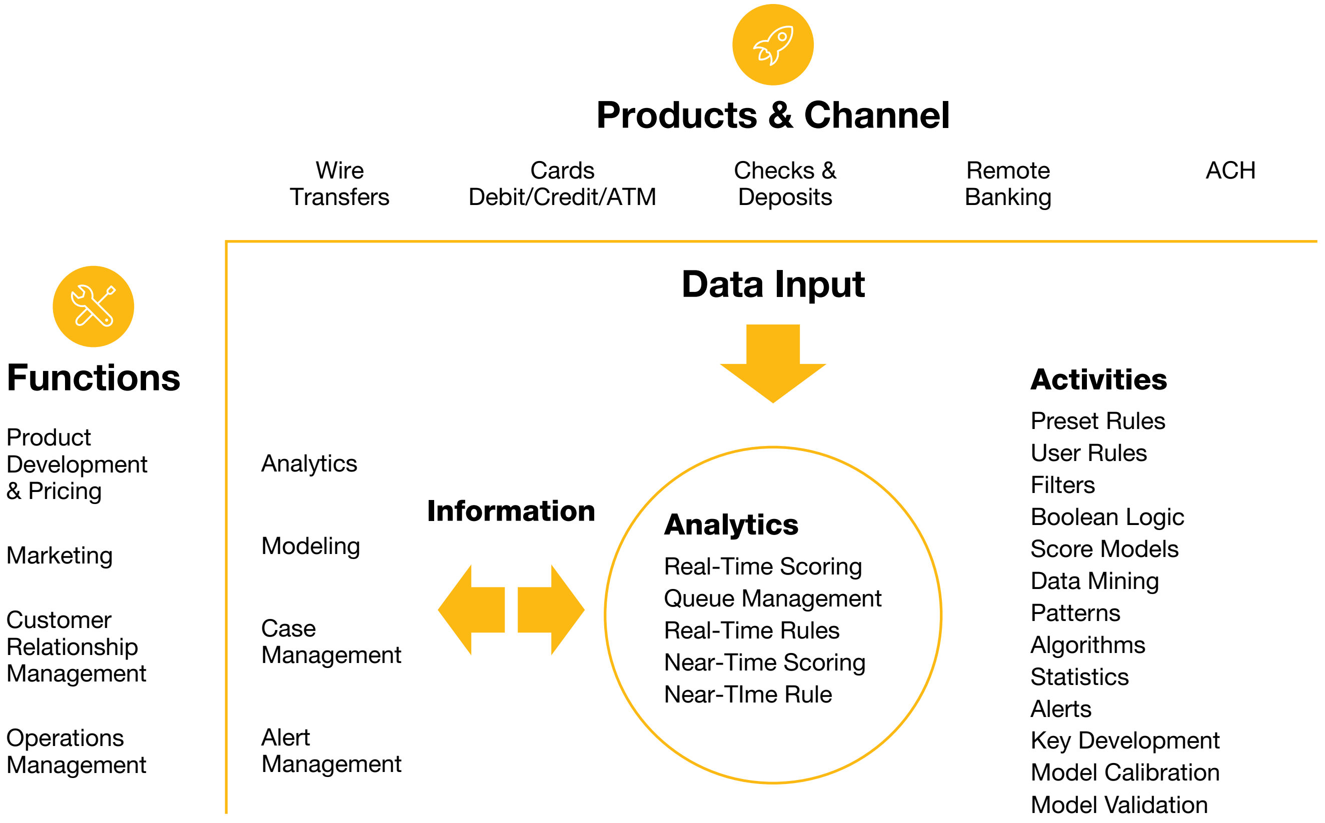
Fraud Analytics Process Diagram

Because of the expense and time involved in setting up a fraud analytics program, companies might consider putting a fraud analytics process in place to help support the success of the program. But what does a fraud analytics process look like?

First, data must be collected from a variety of products and channels, including, but not limited to, wire transfers, checks and deposits, and remote banking. The data must be consolidated for use, and the type of analytics used will be dependent on the goal of the program. The program's goals may vary depending on whether the company is trying to produce real-time scores for potentially fraudulent customers or transactions or whether it wants to see a historical analysis of past patterns.

Exhibit 1: Product, Channel, and Banking Function Flow Chart

This flow chart demonstrates how products and channels can work together with banking functions to provide data inputs into the analytics process. It also shows that by performing analytics on the data inputs, information can be distributed back to the various banking functions.

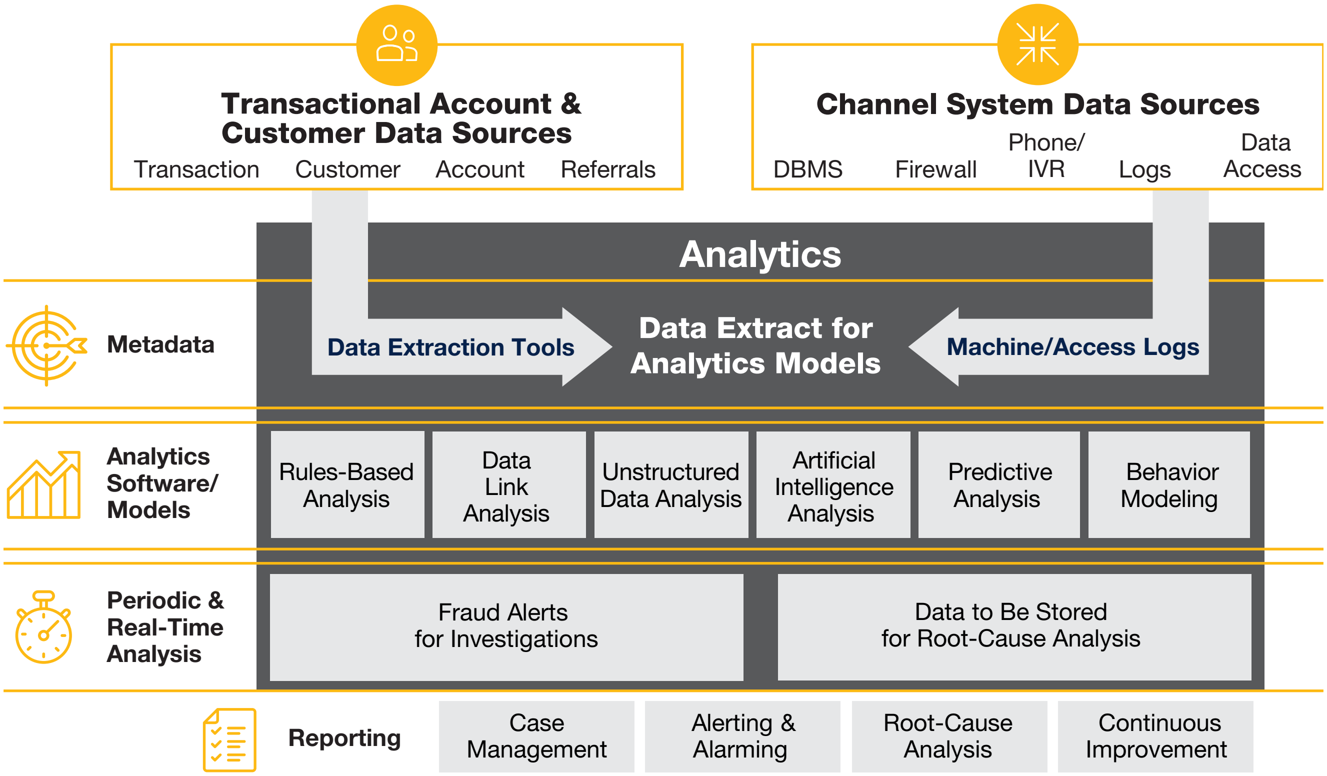


Once the program goals are defined, fraud analysts use different statistical techniques to turn data into recognizable or readable information. Then the institution decides what to do with the information it receives. Some institutions might decide to assign resources to examine alerts and cases, or they might involve analysts to explore predictive models to help set up key performance indicators (KPIs), which can help track the fraud program's success. KPIs might include the time spent on an alert or case, the cost of the review, or the amount recovered.

The most important step in preventing fraud is to take action. Actions could include ensuring that cases are pursued for further investigation, producing reports to highlight weak points within the financial institution, and continually improving fraud analytics programs so that as fraudulent individuals discover new methods, financial institutions can recognize new attacks.

Exhibit 2: Conceptual Architecture of Fraud Analytics

This flow chart represents a conceptual architecture of fraud analytics. By feeding transactional account, customer, and channel system data sources into various analytics processes, useable information can be extracted and reported back to the organization by role.


Transactional Account & Customer Data Sources
Transaction
Customer
Account
Referrals
Channel System Data Sources
DBMS
Firewall
Phone/ IVR
Logs
Data Access
Analytics
Metadata
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 Management
Alerting & Alarming
Root-Cause Analysis
Continuous Improvement

Stay Ahead of the Crimes

As financial crimes become more complex and sophisticated, financial institutions face a growing need to monitor large quantities of data for fraud. Fraud analytics programs can help detect fraud earlier and highlight cases that might require further investigation.

Learn More

Michelle Abuda
+1 614 469 1211
jmichelle.abuda@crowe.com

Gregg Henzel
+1 630 575 4350
gregg.henzel@crowe.com

Arjun Kalra
Principal
+1 415 946 7449
arjun.kalra@crowe.com

[1] Roberto V. Zicari, “On Fraud Analytics and Fraud Detection. Interview With Bart Baesens,” ODBMS Industry Watch blog, Sept. 4, 2015, http://www.odbms.org/blog/2015/09/on-fraud-analytics-and-fraud-detection-interview-with-bart-baesens/

[2] T.J. Horan, “Evolution of Fraud Analytics – an Inside Story,” KDnuggets News, March 14, 2014, http://www.kdnuggets.com/2014/03/evolution-fraud-analytics-inside-story.html

[3] Mohan Babu and Soumya Chattopadhyay, “Claims Fraud: A Big Opportunity for Big Data & Analytics,” Claims Journal, July 29, 2013, http://www.claimsjournal.com/news/national/2013/07/29/233805.htm

[4] “Fraud Detection,” TIBCO Statistica, http://www.statsoft.com/Textbook/Fraud-Detection

[5] Graham Winfrey, “How to Detect Fraud Using Data Analysis (Infographic),” Inc., July 29, 2014, http://www.inc.com/graham-winfrey/how-to-detect-fraud-using-data-analysis.html

[6] Tasha Bailey, “Why Companies Are Afraid to Fight Fraud,” Fraud Magazine, May 2015, http://www.fraud-magazine.com/article.aspx?id=4294988395

crowe.com

Text created in and current as of July 2017; Cover and artwork updated in May 2018.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.