

# Bank Fraud & IT Security

## REPORT

Prepared by  
Southeast Consulting, Inc.



## The Application of Interactive Analytics to Identify Fraud

By Tony Agresta, Centrifuge Systems

If you have ever visited the FBI's Web site ([www.fbi.gov](http://www.fbi.gov)) and clicked on *What We Investigate*, you will notice at least 10 different types of fraud, from *telemarketing* to *mortgage* to *insurance* and others. You will see *cyber crimes*, *network intrusion*, *identity theft* and other criminal activities listed. Diving deeper, you will notice that each type of fraud has different schemes, such as *market manipulation fraud*, *foreign currency fraud*, *Internet pharmacy fraud* and hundreds of others. Each scheme can be quite elaborate. Some fraud scams have been around for over 100 years and others have come to light in the last 100 days.

**Fraud is Commonplace.** Bank fraud is common and the fraudsters change their schemes often. Thieves frequently morph their fraud strategies to throw investigators off their scent while more elaborate schemes are put in place.

As Internet usage has exploded, consumers have become comfortable with e-commerce transactions and people have flocked to social networking sites which have become a fertile breeding ground for fraud, identity theft, money laundering and cyber crime. Fraudsters like to remain anonymous, and what better way to do that than through the World Wide Web?

**Detecting Bank Fraud.** One approach that has proven highly effective in detecting and identifying fraud in today's environment is a relatively new concept called *interactive analytics*. *Interactive analytics* is a human-focused approach to analyzing

massive amounts of data. This important new approach is based on three modern innovations: 1) interactive data visualization 2) unified data views and 3) collaborative analysis.

Through *interactive analytics*, an investigator can take control of the process while applying his or her training, experience and judgment to discover hidden relationships and insights across massive amounts of data. With this approach, the analyst's brain serves as the ultimate pattern recognition machine and the technology opens up the potential for unconstrained analytical power.

When an investigator detects something relevant, inferences are drawn almost immediately. Suspicious relationships are investigated and confirmed. The result is accurate identification, an essential by-product of the investigation that positively impacts detection, reporting and issue resolution.

**Legacy Technology Falls Short.** Historically, legacy technology has fallen short due to four limiting factors. These factors include the following:

- Difficulty of use
- Insufficient interactivity
- Too disconnected from data
- Lack of collaboration.

First generation fraud detection tools have been difficult to learn and adopt. They lack the interactive analytical approach to investigation and are therefore too static. Moreover, they are disconnected from important data sources needed to conduct a comprehensive investigation, and they support only isolated investigations, thereby preventing users from sharing insights and relevant findings.

Next generation products must address these shortcomings and allow investigators to rapidly assimilate important facts, detect hidden relationships,

socialize results with others, and act on knowledge uncovered during this process. The need for this technology has never been greater than it is today.

**Overcoming Current Challenges.** This article isolates the three most important factors needed to overcome the challenges faced with current fraud detection approaches. At a time when the reputation of our financial institutions industry is at stake and regulatory compliance standards are dramatically increasing, effective next generation approaches could not be more relevant.

**What Is the Challenge?** Fraud detection poses real problems for bank IT security and fraud prevention managers in the following areas:

- *Insufficient Time* – Today, bank fraud prevention managers are asked to do more with less in an attempt to accurately identify fraud before it is too late. However, too often the crime has already been committed, the perpetrators cannot be found, and the money is gone. Government regulations also create a need for fraud investigators to identify and report problems quickly.
- *Existing Technology is Limited* - Not only are current tools difficult to use, they often limit the breadth of the investigation by constraining the analysis to a predetermined set of data and operations. To effectively leverage an investigator's expertise, next generation solutions need to allow investigators to operate at the speed of the human brain while pursuing lines of inquiry on the fly.
- *Not Enough Collaboration* - Investigative analysis is a lonely function in most financial institutions. Even in some of the most well-known banks, business lines and investigative groups assigned to those business lines are separate. With credit card transactions separate from ATM transactions, and both separate from mortgage loans, it is difficult to connect fraudulent activities across functional and product lines.
- *The Whole Picture* - It is difficult to

identify fraud without comprehensive access to all relevant data. Typically, the data is spread out across transaction monitoring systems, account activity, customer profiles and historical silos. If investigators lack a 360° view of events, fraud can go completely undetected.

**Interactive Analytics Overcomes These Challenges.** With so much data, limited time and an inability to see the entire picture, investigative analysis hinges on more than just alerts that detect suspicious activity. It depends on accurate identification of criminal behavior leading to issue resolution. Maintaining the history of events tied to the investigative process supports the criminal case.

**Emerging Technologies.** Three emerging technologies that can improve investigations analysis are *interactive visualization*, *unified data views* and *collaborative analysis*. When coordinated together, these three technologies comprise *interactive analytics*.

**Interactive Visualization.** Information visualization is getting a lot of attention today. Information visualization is the use of visual metaphors to enhance our ability to detect patterns in data. Interactive visualization takes this pattern detection process further and allows us to interact with the visualizations directly to ask followup questions and pursue a line of inquiry. This is very different from the static charts that most tools provide today and has proven to be effective at allowing investigators to navigate, explore and understand massive amounts of data. Data analysts find that, when they see something relevant, they draw inferences almost instantly. As a result, the investigator is able to work at the speed of the human brain. When used effectively, the resulting insights can be remarkable.

**Unified Data Views.** Accurate identification depends on having access to all relevant data pertaining to the investigation. Since important facts exist in disparate systems, the ability to access these data sources without extensive integration and programming efforts is critical. Access to the data should be transparent to the investigator, freeing them to

concentrate on what is most important; that being the investigation itself.

Internal data used in the investigation represents one important class of information. Increasingly, third-party data, news wires, blog posts, network traffic, historical information and many other data sources are equally important. Providing the investigator with the ability to easily reach out to these sources from within the investigative framework is extremely powerful. The absence of this capability often yields an incomplete investigation.

A common complaint is that the investigator needs to use multiple tools to obtain a comprehensive view of the case. This can be tedious and highly disruptive to a particular line of reasoning. The ability to switch between multiple, integrated views of the same data is a powerful paradigm for visual analysis.

Visualizations allow one to detect relevant patterns almost instantly. Integrated views allow one to shift one's lens. For example, one could quickly move from a quantitative to a relational to a temporal view of the same data. This allows investigators to quickly and easily validate findings and eliminate false positives.

With these exciting areas of innovation, we must remember that the single largest obstacle to the adoption of new analytics technology is that they are simply too hard to use. They often involve extensive programming and setup. Investigators need easy-to-use analytical tools that allow them to be productive in hours rather than weeks. What's more, the tools need to be enjoyable to use. An analytical tool should provide a user experience closely aligned with the investigative process.

**Collaborative Analysis.** Banking industry professionals have leveraged the power of collaboration technology to increase productivity and foster the exchange of ideas for quite some time. This needs to be applied to fraud and money laundering investigations. Since investigators are assigned cases, and many of these cases are interrelated, it stands to reason that if investigators can collaborate, notify each other of important findings, and publish results for review, they can solve cases faster while also improving the accuracy of the

identification process.

The ability to document the results of the investigation for audit purposes is also important, especially in the area of compliance and regulation. Knowing exactly what steps an investigator took in the analysis process to arrive at a conclusion is useful for audit purposes, training and notifying other investigators who may have similar types of cases to solve. Automatically notifying others in the organization that results are available for review can dramatically speed up investigations and lead to shorter windows for criminal activity to occur. Saving the results of the analysis to document key findings in the investigation is crucial. These analytic assets need to be protected, archived, retrieved when needed, and used to meet compliance requirements.

*Interactive analytics* allows the investigator to ask questions of the data, such as who, what, why, where and when. Moreover, the fraud investigator must be able to easily explore relationships between individuals, banks, accounts, phone records, e-mail records or other relevant data, regardless of where it resides. The real key to *interactive analytics* is that the investigator is able to leverage their significant domain knowledge and experience rather than ignoring it. This technique has been widely deployed by government agencies in the areas of homeland defense, national security, border protection, cyber crimes, fraud and money laundering.

**Interactive Analytics in Action.** The following examples illustrate ways in which *interactive analytics* can be used to analyze massive amounts of disparate data.

From hundreds of thousands of fraud alerts going off across banking business lines globally, the fraud analyst is able to produce a heat map that summarizes the money currently at risk. She does this in seconds by dragging *Alert Type* and *Alert Name* onto a palette and summarizing the data by *At Risk Value*. Prior to this approach, the alerts were in silos by business line and she needed the bank's IT staff to help with the heavy lifting and data integration. But now, every morning, charts, maps, event timelines, tables and relationship

graphs are ready for analysis. Today, *High Appraisal Alerts* in the *Home Mortgage* business line represents the most risk. These alerts represent over \$2.2 million in money at risk. See Exhibits 1 through 4.

After spinning off just this set of alerts, the fraud analyst quickly displays the linkages between the customers, the accounts and the branches with which they are doing business. Current banking customer data is highlighted. Since this technology is highly interactive, the fraud analyst can zoom in to see people of interest. At the center of the graph is an individual who is connected to many different accounts and branches. His hypothetical name is Jack Kilpatrick.

After the analyst filters the data to select only the customers with the last name Kilpatrick, an interesting picture is seen. The analyst decides to also grow the picture to add the location of the property and the name of the account officers involved.

The geographic location of the homes for Jack is Maryland and Virginia but he has accounts with the Los Angeles and Florida branches as well. There also happens to be other Kilpatrick's within this set of mortgage alerts. Their home locations are not close to the branches they are doing business with, with the exception of Tim Kilpatrick.

Based on her knowledge of fraud, these relationships are clearly worth investigating further. Additionally, account officers have been identified. Could these individuals be associated with a series of high appraisal alerts? Are they working with the loan officers? Are the customers related? Do they have a history of alerts within the bank? Should the manager for *Home Mortgages* in each branch be notified of this problem right away? When were the loans granted?

All of these questions, and more, can be answered as the fraud analyst continues to explore the data. She can bring in other sources of data on demand, such as historical alerts. She can access identity verification services and repositories of personal assets. At any time, she can share the results with other members of her team.

**Conclusion.** These examples only begin to touch on insights that can be exposed by utilizing *interactive analytics*. Bank fraud investigators given the freedom to explore data can draw rich visualizations that unify disparate sources and complete the picture. As insights are uncovered, they can collaborate with other members of their team, law enforcement and bank management. This technology has been applied in similar applications including cyber crime analysis, counter-terrorism and homeland security. It also can be applied to many other application areas such as sales, service and marketing analysis and advertising effectiveness. The volume and velocity of data coming into our financial institutions is increasing at a pace that far exceeds other tools. Now, with *interactive analytics*, fraud and security analysts can meet the challenges they face every day.

*Tony Agresta is VP of Marketing for Centrifuge Systems. He has 25 years of experience in the analytics software market.*

*He can be reached at  
aagresta@centrifugesystems.com or 571-830-1390.*



Exhibit 1: Heat Map

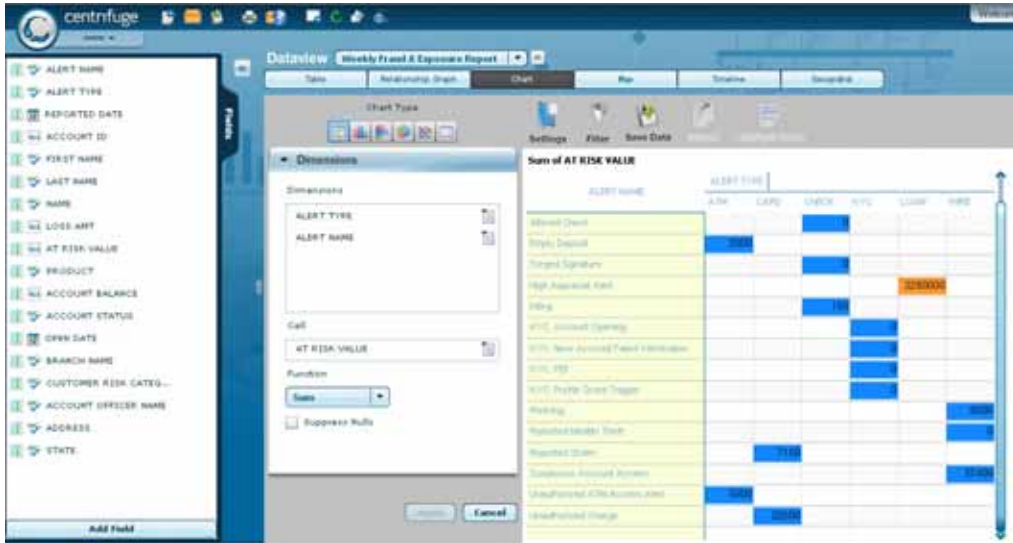
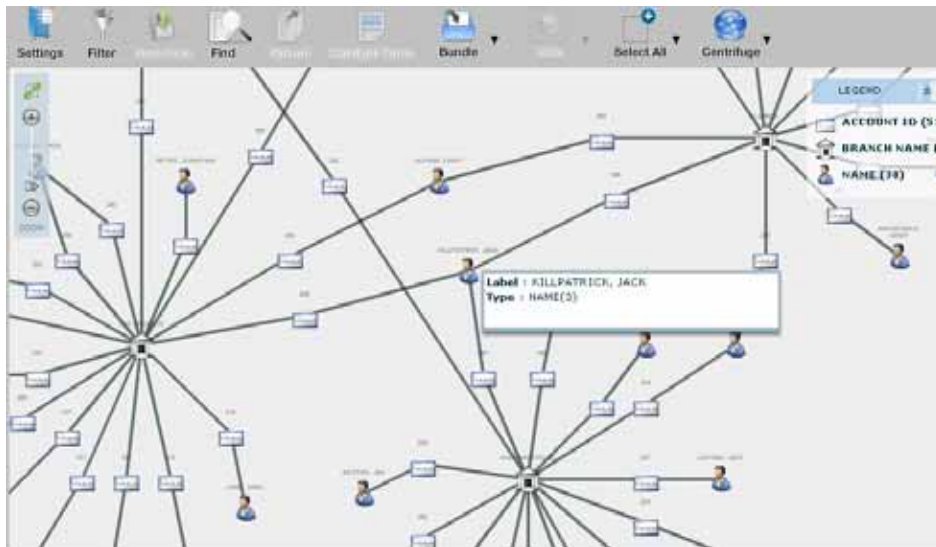
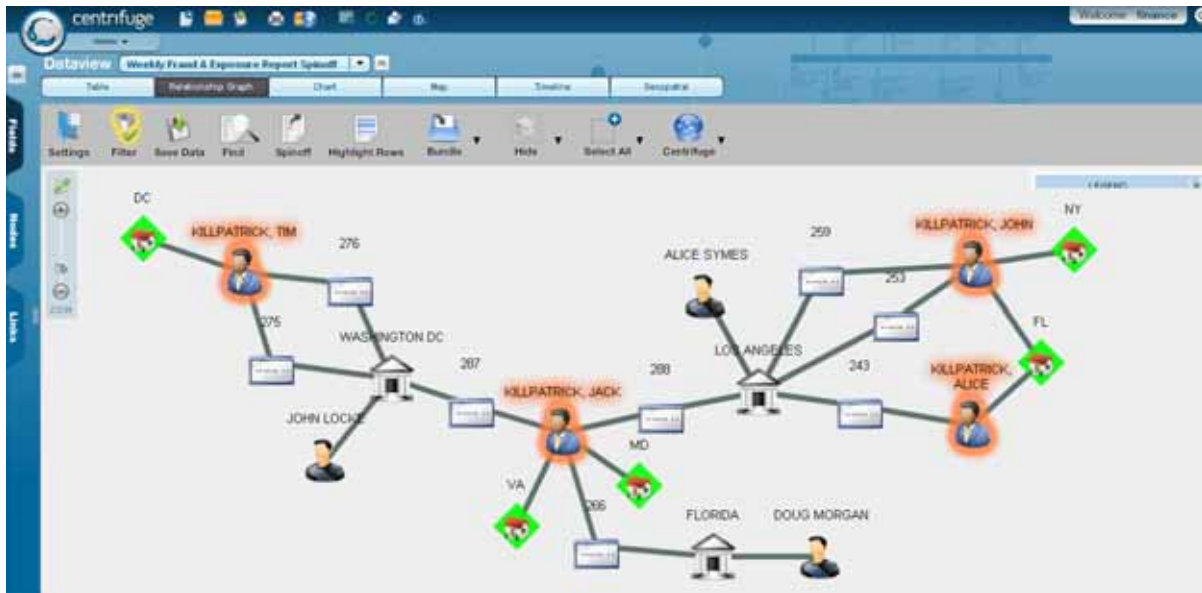


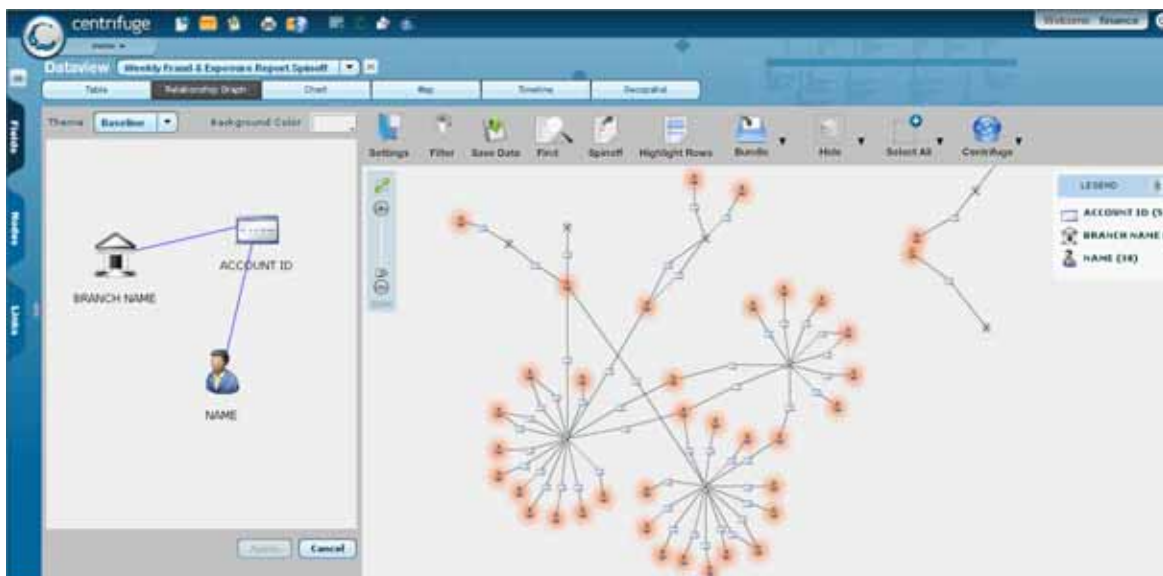
Exhibit 2: Links Between Customers



**Exhibit 3: Customer's Filtered Data**



**Exhibit 4: Name Account and Branch Relationship Graph**



Centrifuge Systems provides next generation business intelligence software that helps organizations discover insights, patterns and relationships hidden in their data. The unique Centrifuge approach, called *Interactive Analytics*, brings together three innovations in analysis: Interactive Data Visualization, Unified Data Views and Collaborative Analysis. Traditional business intelligence solutions require users to define what they want to see in advance and present results in static dashboards. With Centrifuge, users determine what is of interest *on the fly*, ask open ended questions of their data by directly interacting with visual representations of the data, and then manipulate the displays directly in a highly interactive fashion.



centrifuge

Centrifuge is used in some of the most demanding applications in the world, including counter-terrorism and homeland defense, providing analysts with the freedom to explore. It supports a wide variety of applications including fraud analysis, cyber security, performance management, customer relationship management, business intelligence and many other applications.