Paper 029-2011

Enterprisewide Fraud Management

Ellen Joyner, SAS Institute Inc. Cary, NC, USA

DETECTING AND PREVENTING FRAUD IN FINANCIAL INSTITUTIONS

Fraud has evolved from being committed by casual fraudsters to being committed by organized crime and fraud rings that use sophisticated methods to take over control of accounts and commit fraud. The problem is pronounced in the financial sector where the compromises are more sophisticated than in other industries.

It is essential to get not only multiple sources of data to understand the entities being compromised but also apply sophisticated analytical methods to understand the data, extract optimal information, use high-end pattern recognition and text mining to create features, and advanced modeling techniques to fit the best possible models to the data to reduce false positive rates. The presentation discusses the challenges faced in fraud detection and how they can be addressed using sophisticated analytical techniques.

INTRODUCTION

Scenario #1: Sue was just buying pillowcases, paying with the store's own credit card. But within days, that card number would reach a fraudster in Florida, who punches out new plastic with her number, later used to buy dozens of store gift cards at a time, each for an amount just under the review limit.

❧ ~ ❧ ~ ❧ ~ ❧

Scenario #2: The credit card came back to the table in no time, and Robert signed the tab for dinner. He made sure only the last four digits of his card number were displayed on the merchant's copy. But Robert didn't know that in the 30 seconds the waiter had the card, he had photographed both sides with his cell phone – and would later use the account to order merchandise and concert tickets by phone.

Fraud scenarios

These events are everyday occurrences – thousands of times a day, actually. In the first case, the store's parent company detected the security breach, but only after three years, 200,000 counterfeit cards and $1 million in fraudulent purchases. This particular retailer is not alone; nearly three out of 10 store-brand credit cards are obtained or used fraudulently, according to Javelin Strategy and Research.[1]

And if Robert opened his bill to find surprise charges he didn't make, he was in very good company. Some 6.8 million Americans were victimized by card fraud in 2007, according to Javelin research. [2] His bank's "zero liability" policy meant Robert didn't have to pay the charges, but the bank did.

Such fraud on existing accounts accounted for more than $3 billion in losses in 2007, according to the American Bankers Association[3]. The Nilson Report estimates the cost to the industry to be $4.84 billion.[4] And Javelin estimates the losses at more than six times that amount – some $30.6 billion in 2007.[5]

---

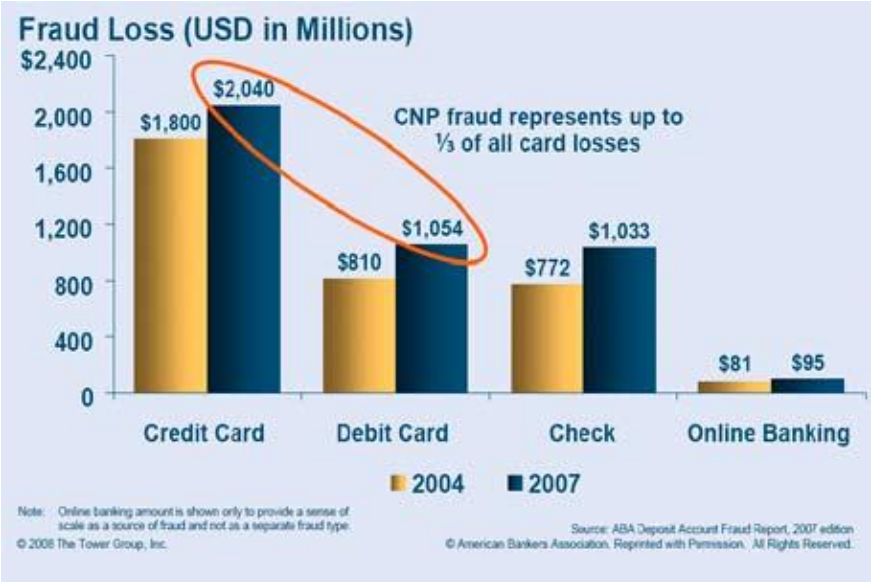
1 Kim, Rachel and Monahan, Mary. Javelin Strategy and Research. 2008 Identity Fraud Survey Report. February 2008.

2 Kim, Rachel and Monahan, Mary. Javelin Strategy and Research. 2008 Identity Fraud Survey Report. February 2008.

3 ABA Deposit Account Fraud Survey Report. 2007 Edition.

4 The Nilson Report. July 2007.

5 Kim, Rachel and Monahan, Mary. Javelin Strategy and Research. 2008 Identity Fraud Survey Report. February 2008.



TowerGroup estimates that card and check fraud accounted for more than $4 billion in losses in the US in 2007, up 22 percent from 2004.

Of course, fraud is not a domestic product. It's everywhere. For instance, card fraud losses cost the UK economy GBP 423 million (US$767 million) in 2006. Credit card fraud accounts for the biggest cut of the $600 million that airlines lose each year globally, according to Deloitte research[6]. Card losses top ZAR 50 million a year in South Africa (US$6.3 million), according to the South African Card Fraud Forum. The list goes on.

The good news is that the numbers tend to be slightly down from previous years, especially in the US. The bad news is that hackers, identity thieves and money launderers are fighting back by focusing on different channels and spawning new types of attacks that traditional fraud management strategies were not designed to address.

[6] Deloitte. *Airlines face US$600 million fraud loss — 79 percent of airlines report experiencing fraud last year*. August 2007.

OUTWITTING THE CRIMINAL MIND – THE CHALLENGES

Financial services institutions are well aware of the negative impact of fraud. Even at industry-average levels, fraud hurts an institution's reputation, customer loyalty, shareholder confidence and the bottom line. But even the most well-intentioned financial institutions face some daunting challenges in this area.

BANK FRAUD IS INCREASING IN VOLUME AND SOPHISTICATION.

"The credit and debit card fraud category of financial services is among the fastest-growing and best-known means of criminal profit," says Rodney Nelsestuen of TowerGroup.[7] "What makes card fraud of great concern is the fact that international organized crime rings are often involved, turning card fraud from random, criminal activity into industrial-strength enterprises."

The sophistication of their tactics makes detecting fraud difficult and preventing it nearly impossible, especially as the volume of bank transactions grows by about 10% a year.

THE FASTEST-GROWING CHANNELS ARE ALSO THE ONES MOST AT RISK.

ATM and branch office transaction volumes are flat (as a percent of total transactions), while call center channels are growing modestly and electronic access (online and mobile access) is booming. Mobile banking, barely a blip on the radar in 2008, is expected to grow to more than 42 million users in 2012, according to TowerGroup research.[8]

Unfortunately these fastest-growing channels are also the most vulnerable. For example, in a Gartner survey of 50 banks, more than half reported that their institutions had been the target of a phishing attack in the previous year.[9]

The anonymity of e-commerce makes it more difficult to uncover bogus Web communications and hidden relationships.

FRAUD IS USUALLY MANAGED IN BUSINESS-UNIT SILOS.

Customers – legitimate and otherwise – tend to see the institution as a single brand represented across various contact channels: phone, automated contact center, ATM, branch office and online. But the institution tends to see its customers as diverse entities based on product: mortgage, credit card, DDA, home equity, consumer banking, small business, etc. This disparity creates inefficiencies that fraudsters can exploit.

> **"Interestingly, while FSIs struggle to capture a full view of each customer's relationship with the institution, enterprising fraudsters are already achieving this understanding as they strive to gain more information about financial services and products to exploit."** [10]
>
> *Rodney Nelsestuen, Senior Analyst, Financial Strategies and IT Investments, Tower Group*

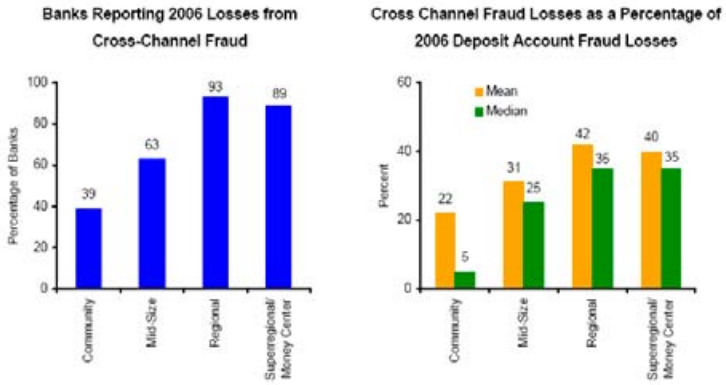
7 Nelsestuen, Rodney. TowerGroup. S*urrounded by the Enemy: The Case for Enterprise Fraud Management*. March 2008.

8 Nelsestuen, Rodney. TowerGroup. Surrounded by the Enemy: The Case for Enterprise Fraud Management. March 2008.

9 Litan, Avivah. Gartner Research. Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations. May 2008.

10 Nelsestuen, Rodney. TowerGroup. Surrounded by the Enemy: The Case for Enterprise Fraud Management. March 2008.

Figure 3: CROSS-CHANNEL FRAUD



Source: ABA Deposit Account Fraud Survey Report, 2007 Edition

CROSS-CHANNEL FRAUD IS WIDESPREAD.

Criminals know the above facts all too well. They know bank fraud systems rarely monitor customer behavior across multiple accounts, channels and systems. That weakness opens the door for cross-channel fraud, in which a fraudster gains access to customer information in one channel and uses that knowledge to commit fraud through another.[11]

"Cross-channel fraud is difficult to discover, track and resolve because the activities of the fraudster posing as the customer often mirror those of the customer," says Nelsestuen.[12] "Thus, apparently normal activity can be fraud conducted over an extended period." As a result, cross-channel fraud is common – and costly.[13]

FRAUD DETECTION HAS BEEN SKETCHY.

About half the time, fraud is detected by the victims themselves when they review a monthly statement or are turned down for credit. Imagine the loss of confidence a consumer would feel to discover fraud before the bank did. Only about 25 percent of the time does the bank detect the fraud first.

"Fraud case management and data analytics rarely are performed at the enterprise level, which means that cross-channel fraud, a growing criminal technique, will be missed."

Avivah Litan

Gartner Research[14]

11 Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*. March 2008.

12 Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*. March 2008.

13 Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*. March 2008.

14 Litan, Avivah. Gartner Research. *Fraud Detection and Customer Authentication Market Overview*. July 2008.

SLOW DETECTION LEADS TO HIGHER LOSSES.

Speed is crucial. According to the 2008 Javelin fraud survey report,[15] victims who detected the fraud within 24 hours were defrauded for an average of $428. Victims who did not discover the fraud up to a month later suffered an average loss of $572. Those who took up to five months lost nearly three times as much ($1,207) as victims who detected the fraud within one day. Of course, this is no surprise. What can be a surprise is how much that figure escalates when you add associated costs, such as lost wages, loss of goodwill and legal fees.

Collectively, these realities create a daunting environment for financial services institutions:

- They would like to accurately identify the patterns and perpetrators, but they usually lack the analytical modeling rigor to establish a strong defense.
- They would like to identify cross-channel fraud, but their operational systems often don't cooperate well across organizational boundaries.
- They would like to monitor every transaction in real time, but they can't alienate customers and merchants with long processing times.
- They would like to implement rigorous rules to detect fraud, but they know they would turn up a lot of false positives that are costly and fruitless to investigate.
- They would like to unify the fraud management process, but disparate data sources and cryptic interfaces make the system inaccessible to all but a few.

THE TROUBLE WITH TRADITIONAL FRAUD MANAGEMENT

To detect fraudulent activity, many banks use transaction monitoring systems – often homegrown, niche software that requires manual intervention. Still, traditional systems can work well for detecting individual real-time, point-of-sale fraud. But that's only one slice of the fraud pie and not the biggest slice, either.

Few banks have strong, enterprisewide fraud management programs that can correlate a customer's behavior across all contact channels and products to identify "bust-out" scenarios, social networks and cross-channel fraud. "An institution may have state-of-the-art security and fraud detection technologies and procedures to protect its deposit lines of business, but not the same for small business banking or third-party investments delivered by an alliance partner," wrote Nelsestuen.[16]

Furthermore, even the fraud management process itself is fragmented. "Fraud detection, alert and case management practices are still too often viewed as separate activities, when in fact they should be managed as a whole," says Nelsestuen.[17]

15 Kim, Rachel and Monahan, Mary. Javelin Strategy and Research. *2008 Identity Fraud Survey Report*. February 2008.

16 Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*. March 2008.

17 Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*. March 2008.

Not much changed when the Red Flag rules went into effect in November 2008, implementing Section 114 and Section 315 of the US Fair and Accurate Credit Transactions Act of 2003. This regulation generally only requires banks to formalize and document the procedures they already have in place. Some 60 percent of banks surveyed by Gartner before the rules took effect believed they were already compliant.[18]

However, some banks looked at the Red Flag deadline as an opportunity to improve fraud prevention practices across the enterprise. "Surely, good security practices will lead to Red Flag compliance, but the reverse won't necessarily be true," notes the Gartner report.

"During the next two years, the most pervasive plans for new fraud prevention and customer-security-related projects include stronger caller authentication for customers that telephone call centers; enterprise fraud detection that manages fraud across customer channels and accounts; and a case management system for managing fraud."[19]

The result would be a fraud management approach that:

- Protects against fraud at the point and time of transaction.
- Accurately detects incidents of fraud in completed transactions.
- Spans all the ways customers interact with the institution.
- Provides structured oversight for the fraud management program.

This is not a halcyon vision. The technology is available today.

Let's take a look at how a robust, enterprisewide fraud management system can redefine the economics of fraud. We'll walk through the process with a hypothetical bank based on a real one – we'll call it First Best Practice Bank (FBPB) – a multiservice institution with more than a million active cardholder accounts.

"Financial institutions are increasing their spending on fraud management systems, according to Gartner[20]. But is this investment going to best use, or is the bank still hoping to simply work harder than the fraudsters?"

Avivah Litan

Gartner Research

18 Litan, Avivah. Gartner Research. *Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations*. May 2008.

19 Litan, Avivah. Gartner Research. *Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations*. May 2008.

20 Litan, Avivah. Gartner Research. *Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations*. May 2008.

BEST PRACTICES IN FRAUD MANAGEMENT –

COMBATING FRAUD WITH THE TECHNOLOGY AVAILABLE TODAY

FBPB wanted real-time scoring of all card transactions – purchase, payment and nonmonetary – for faster, more accurate fraud detection on a global scale. Ultimately, they hoped to prevent fraud before it happened, even as the fraudsters evolved their methods and hid their deeds in obscure relationships.

So in 2007, FBPB implemented a complete, end-to-end IT platform for detecting, preventing and investigating both opportunistic and organized first-party fraud. The IT team knew that an integrated solution would be easier to implement and maintain, and enables the richest possible set of capabilities and data interworking. Investigators knew it would be advantageous to detect, prioritize and manage fraud in a cohesive environment.

Enterprise Fraud Management Components

A best-practice fraud management approach is integrated from end to end.

Step 1. Create an enterprisewide view of patterns and perpetrators.

The new system enabled FBPB to create a true, enterprisewide view of fraud. The knowledge base incorporates data from operational/transactional systems across separate business units, from human resources and audit records, even from external data sources such as fraud consortium databases. Integrated data quality routines cleanse and validate the data.

The data repository offers up data in analysis-ready format. Advanced, large-scale analytics sift through all this internal and external data to link customers and accounts based on predefined rules, common attributes and subtle patterns of behavior.[21]

FBPB customized the system with fraud models unique to the institution. No black-box software here. Rules, models and analytic techniques can all be customized and modified. Since there were no preconfigured system limits on rules, FBPB created a deep set of complex rules for identifying potential fraud.

21 Litan, Avivah. Gartner Research. *Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations*. May 2008.

Step 2. Prevent and detect fraud in enterprisewide context.

Analytics reveal potentially suspicious patterns and transactions.

FBPB's fraud system goes beyond the typical customer view to provide a holistic view of fraudulent activity – including related perpetrators and unrelated channels – and enables a much deeper understanding of customer behavior.

Each transaction – account opening, ATM access, online banking transaction, call center encounter, etc. – is passed through a set of rules and predictive models. In real time, the system checks transaction activity against vast, enterprisewide intelligence about the customer and potentially suspicious behaviors. Is this an unusually large deposit for this individual? Is this account linked to another account known to be in a suspected fraud ring? Does this entity hold multiple accounts or similar identities in unusual ways?

Within milliseconds (for most transactions), the system delivers a score that accurately predicts fraudulent activity – within or across channels. Even though the system can operate on billions of records, this transaction monitoring doesn't bog down real-time decision making and authorization.

Every night, FBPB also runs a batch process of existing customer accounts to detect and investigate existing fraud as well as prevent new fraud. The system parses the data and creates a complete update of all account holders and their key linking attributes. Driven by metadata, all records are exhaustively linked based on combinations of attributes within the data. Then, using statistical techniques, common entities are identified and collapsed to produce single views of entities within networks. Discrete, bounded networks within the data are also generated, representing statistically relevant groups of activities and relationships.

An advanced scoring engine uses independent and combined scores based on three core paradigms:

- Application scoring based on scorecard-driven models and text analysis.
- Scoring of individual customers and their full histories.
- Scoring of associated networks, including behavioral data (transaction patterns, network growth rates, activity levels) and other data provided (current/previous addresses, contact numbers, employers).

A hybrid approach combines basic business rules with advanced analytics and social networking. The combination of assessment techniques enables extremely robust fraud detection, whether fraud patterns are known, unknown, complex or marked as "guilt by association."

"As financial institutions become more sophisticated in their fight against fraud, they are going to demand software solutions that provide more flexibility in: addressing emerging fraud issues; analyzing transactions and activities in real or near real time; and identifying fraudulent activity that spans diverse data sources and payment channels."

Dan Barta, Director,

Enterprise Fraud and Risk Strategy, SAS

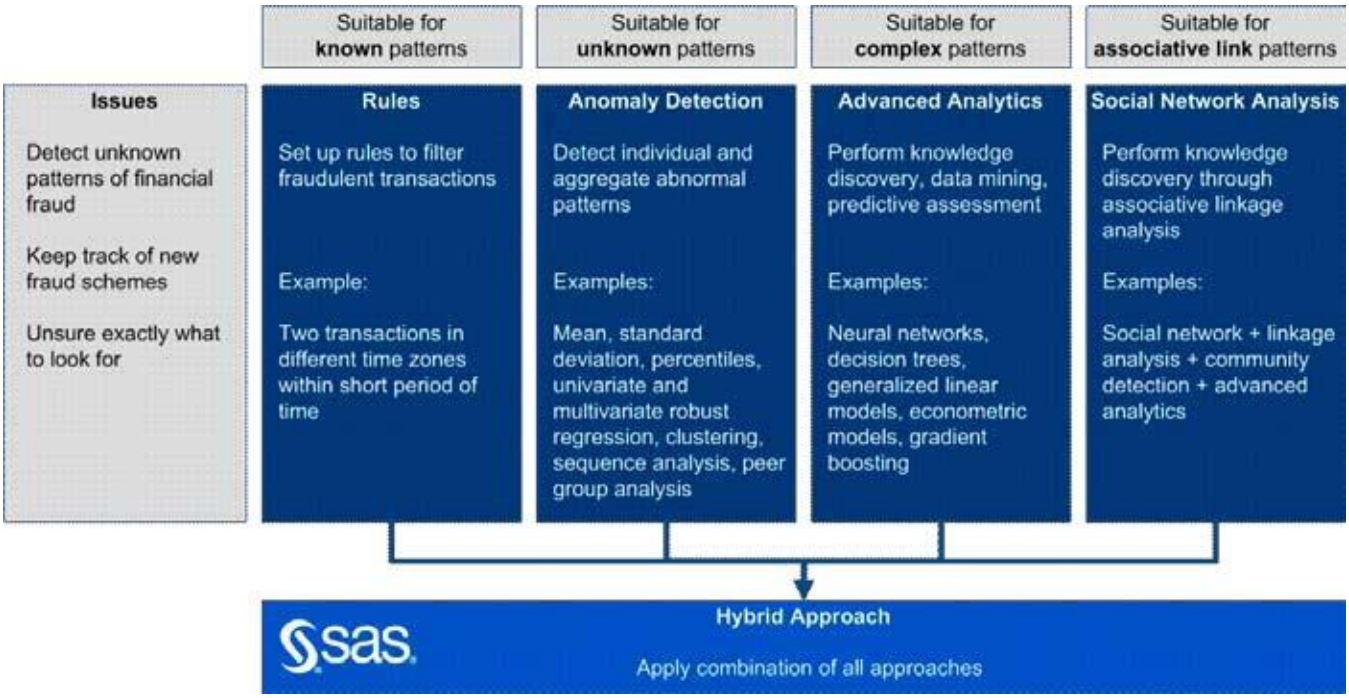
Shorthand customer-state identification: customer-state vectors

Customers are not static. Their personal or professional conditions change. A fraud management system should recognize and work within this dynamic reality. But how do you capture it? It would be unrealistic to try to assess every data point around a customer with every transaction. And if you wait 90 days for a quarterly report, the opportunity to respond to a change of state may have passed.

The answer can be to use customer-state vectors, which are sets of data elements that sufficiently capture a customer's state. Examples might be: dollars spent on airfare, cash withdrawals from a credit account or transactions over the median for the cluster. These data elements are established using regression and correlation analysis. They then can be used in a shorthand method of identifying the customer's state – and the associated marketing opportunities or risk.[22]

"Real-time transaction monitoring is the key to mitigating fraud."

George Tubin, *TowerGroup*[23]



22 Tubin, George. Tower Group. *Consumer Banking Fraud Trends: Welcome to the Ho-Hype Zone*. May 2008.

23 Tubin, George. Tower Group. *Consumer Banking Fraud Trends: Welcome to the Ho-Hype Zone*. May 2008.

Is real-time transaction monitoring too cumbersome?

Historically, running thousands of transactions an hour through a host of complex rules could have been a slow process, noticeably delaying authorization. New processors and processing techniques have radically changed that, so real-time monitoring is feasible even for billions of records.

For example, a bank with 30 million active cardholders in the US adopted SAS® Fraud Management to check every credit card transaction. In the first three months, this bank reported the following results:

• An 87 percent increase in the number of card transactions and customer information processed, while reducing mainframe processing overhead 12 percent – resulting in a 53 percent decrease in mainframe processing cost per data item.

• A 30 percent decrease in the computing resource cost of processing card transactions flagged as potentially fraudulent.

• A 10 percent increase in efficiency by agents investigating potentially fraudulent cases.

Furthermore, the bank reduced IT costs by eliminating three software applications that were no longer needed with their new, integrated fraud management system.

Alerts from multiple systems are aggregated and systematically managed.

FBPB's fraud management system aggregates and prioritizes alerts from the bank's various fraud detection and money laundering tools. Alerts from all these different systems are correlated to provide a full picture of the risk associated with an account or relationship. Analytics can be applied to the alerts to post-score, determine how to route alerts and support other case management decisions.

An alert database stores the alerts and the results of their disposition. This database itself becomes a valuable resource for fraud management in several ways:

• Analysts can mine this alert data to determine how well fraud management tools are generating and feeding the alert management system and to better understand the nature of false positives.

• The database can automatically communicate with the bank's host systems about interventions that have taken place, such as holds placed on funds availability, account closure or other actions.

• Performance management systems can use the statistics and metrics associated with alerts to assess the success of fraud detection and prevention initiatives.

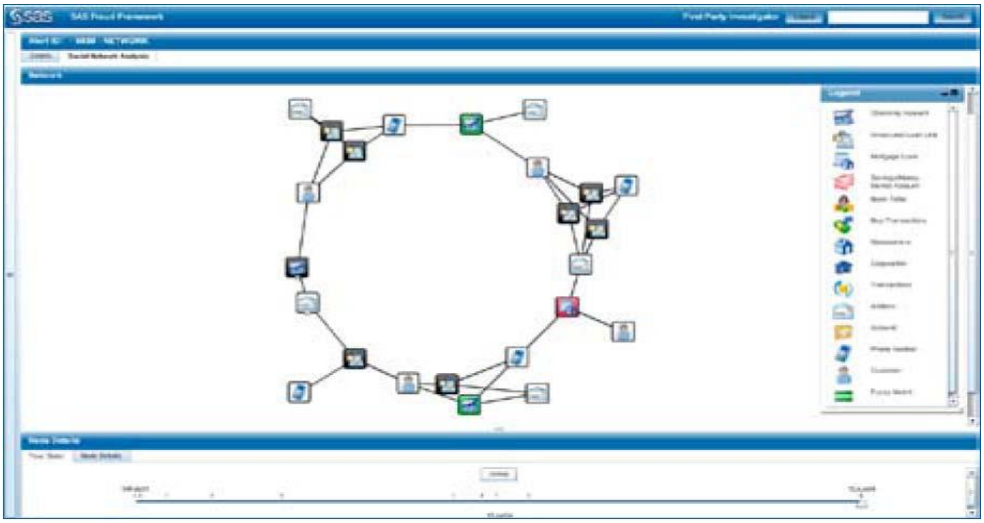
Enterprisewide Fraud Management, continued

Relationships among accounts and entities become clear in visual displays.

FBPB knew that many types of fraud could go undetected because the activity was only suspicious when viewed across multiple accounts. So they go beyond transactional and account views to analyze all related activities and relationships at a network dimension. The system automatically generates network diagrams that correlate data points not only within an account but also across possibly related entities.

Social network analysis enables investigators to see previously hidden connections based on all relevant data sources from a variety of product lines. An intuitive interface provides fast access to full customer details and all related parties and networks.

Delving into diagrams of social networks, investigators can see a complete picture of individual customers, their products, transactions and connections at the click of a button. They can then drill down into underlying data for full customer details, including other linked customers and networks. Back up at a higher level, they can explore entire networks of identities, accounts and applications – in minutes rather than hours – and take action quickly.



A unique network visualization interface shows social network connections to uncover previously unknown relationships.

Enterprisewide Fraud Management, continued

Investigators can zoom in to look more closely at accounts or entities, and drill down into underlying data for full customer details.

STEP 3. INVESTIGATE AND RESOLVE FRAUD IN AN INTEGRATED ENVIRONMENT.

Entities and transactions from an alert management system that have been flagged for investigation may be sent to SAS Enterprise Case Management. Suspicious cases may be automatically assigned to an investigator based on the type or category of the incident. When an investigator logs into the system, he or she is presented with a list of tasks and a structured environment in which to manage them. Information is entered in online forms that are dynamically linked to workflows. The investigator can:

See active and pending tasks.

- See cases and incidents that may currently or have been previously worked in another department.
- Maintain a complete audit trail of actions taken on the case and who performed those actions.
- Display details by case.
- Add freeform notes to the case diary.
- Generate summary and detail reports on demand.

The case management component is modular, so it is easy to update as regulations and circumstances change.

Investigators know their time will not be wasted. Between real-time transaction monitoring and batch processing, FBPB now sees far fewer false positives. Whereas traditional approaches yielded one accurate fraud hit for every 30 cases referred for investigation, the new solution can accurately identify one instance of fraud in every three – a big improvement.

The case management component also measures productivity and other information to help direct the fraud management function more effectively. For FBPB, the automated system with network visualization has reduced the time and effort of investigating organized fraud by 50 percent to 66 percent. A securities firm reported that the increase in productivity has enabled them to conduct the same volume of investigative activity with 26 percent fewer work hours.

FUTURE TRENDS IN ENTERPRISE FRAUD MANAGEMENT

To more effectively prevent future losses, fraud management systems will have to become self-learning, and adaptable to a dynamic environment and evolving fraud techniques.

Financial institutions already can seamlessly test the effectiveness of fraud-detection rules and models – and update them when test reports indicate the need. Ideally though, the system would automatically capture the outcomes of investigations and reuse those outcomes in future scoring. Models would thereby adapt readily to new knowledge and continually be refined. Auto-generated network diagrams would enable strategists to see patterns and symptoms that lead to improved controls and new monitoring techniques.

This combination of adaptation and visibility would enable financial institutions to better understand emerging threats so they can take action to prevent substantial losses before they happen.

The prospects for the future also extend beyond the scope of any single enterprise. As more organizations adopt integrated, automated fraud management systems, the potential is there to create a broad consortium of financial institutions that can draw on their collective experiences to improve fraud detection across the industry.

"Case management not only provides a tool for corporate security to record losses and develop cases for civil and criminal litigation; it also provides a repository for detailed information about fraud exposure that is essential for maximizing the effectiveness of fraud detection tools across the organization."

Dan Barta, Director,

Enterprise Fraud and Risk Strategy, SAS

"The discovery rate for existing card accounts fraud has been significantly aided by financial institutions' deployment of backend systems and technologies, such as neural networks, fraud filters, clustering, profiling and question-based modeling."

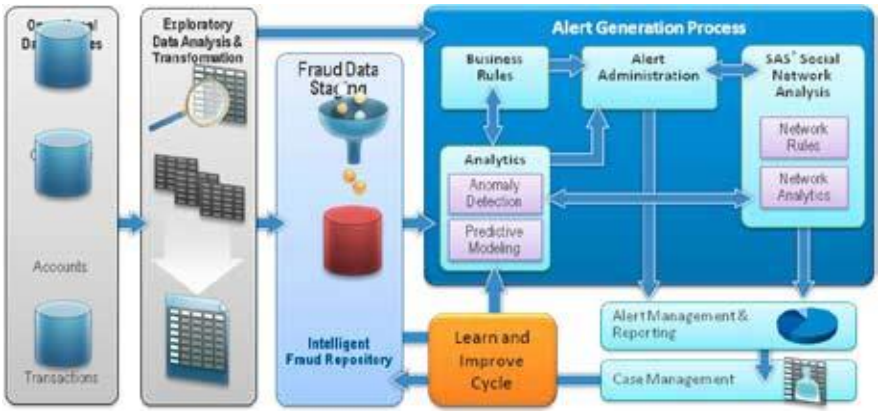
2008 Identity Fraud Survey Report Javelin Strategy and Research, February 2008

CLOSING THOUGHTS

Organizations that respond to regulatory pressures by simply documenting their existing fraud management practices are selling themselves short. This is the opportunity to turn the tide on fraud, fighting back with powerful analytics, holistic intelligence and integrated case management.

An enterprisewide approach to fraud management that spans all contact channels and account types is recommended. A best-practice fraud management approach is integrated from end to end, including:

- **Data analysis and alert generation.** The ability to assimilate data from multiple sources and apply predictive analytics to accurately assess transactions, activities and customer state in real time.
- **Alert management.** The mechanism for accepting, prioritizing and distributing alerts from the various fraud detection and money laundering tools used across the enterprise.
- **Social network analysis**. An analysis and visualization tool for uncovering previously unknown relationships among accounts or entities.
- **Case management.** A structured environment in which to manage investigation workflows, attach documentation and record exposure and losses, while using advanced dashboards for management oversight and analytical reporting to track financial crimes operational performance.



A best-practice fraud management system is integrated from end to end, from data management to analysis (using multiple analytical techniques), alert generation and management, and case management.

"Although it's important to fight fraud in each silo, generally with best-of-breed point solutions, it's imperative to give priority to analytics and case management of alerts across the enterprise."

Avivah Litan, Gartner Research [24]

[24] Litan, Avivah. Gartner Research. *Fraud Detection and Customer Authentication Market Overview*. July 2008.

The technology to implement this approach is available today. The right platform will:

- Integrate with the bank's existing cardholder and authorization systems.
- Create and manage "signatures" that identify an account holder's total behavioral profile.
- Use sophisticated analytic models and business rules to perform on-demand scoring.
- Make information and alerts immediately available to the people who need this information.
- Provide a structured environment to manage investigations and track performance.[25]
- Evolve to keep pace with emerging trends in the regulatory environment and fraud practices.

The benefits of this approach are substantial. A financial institution could:

- **Gain a holistic view of fraudulent activity**, including related perpetrators and cross-channel fraud, and gain a much clearer understanding of customer behavior.
- **Improve investigator efficiency** with unique network visualization, data drilldown and other investigation tools.
- **Increase ROI per** investigator through fewer false positives, prioritization of higher-value networks and more accurate investigations.
- **Prevent future fraud** by better understanding emerging threats and taking the right proactive action.
- **Extend the value of the fraud management** solution by using it to prioritize alerts for anti-money laundering, credit risk and marketing applications.

Losses stopped. Fraud avoided. Time saved. The ROI comes from many directions. TowerGroup estimates that for every dollar spent on fraud management, the enterprise gains back as much as $8.[26] If enterprisewide fraud management sounds like a good answer for your financial services institution, flag it for investigation.

25 Litan, Avivah. Gartner Research. *Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations*. May 2008.

26 Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*. March 2008.

ABOUT SAS

SAS provides all the capabilities described in this document, based on the proven SAS platform. The solution takes a unique approach that blends multiple techniques and provides a systematic framework for detecting, investigating and managing fraud cases. This hybrid solution detects and prevents both opportunistic and professional/ organized fraud, including emerging threats. Financial institutions significantly reduce losses by detecting more fraud with fewer investigators.

Compared to niche or point solutions, the SAS solution can integrate with other solutions across the institution, such as systems for risk and customer intelligence.

SAS has worked closely with top financial institutions for more than 30 years to create solutions to address critical business needs. In the financial services industry alone, SAS data integration, fraud detection, risk management, regulatory compliance, CRM and other software is used by more than 3,000 financial institutions worldwide, including 97 percent of banks in the FORTUNE Global 500®.

Our award-winning solutions handle the challenges specifically associated with the volatile financial services industry, and we can help institutions better manage their strategy, risk, customers and channels to maximize profitability, achieve greater shareholder value and gain a clear competitive advantage.

Across industries, SAS solutions are used at 45,000 sites in 113 countries. Since 1976, SAS has been giving customers around the world THE POWER TO KNOW®.

www.sas.com

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Name: Ellen Joyner

Enterprise: SAS institute

Address: SAS Campus Drive

City, State ZIP: Cary, NC, 27513

Work Phone: +1 919 677 8000

Fax: +1-919-677-4444

E-mail: ellen.joyner@sas.com

Web: www.sas.com