

## Building a better banking world

The benefits of a unified approach to fighting fraud

There's a reason why many industry analyst firms such as Chartis Research and Frost & Sullivan are evaluating anti-fraud technologies based on their ability to provide an integrated, platform-based approach: It's simply the best way to get the most accurate, complete and cost-effective picture of fraud within an organization. Yet the norm is still to have multiple anti-fraud and anti-money laundering systems across different business units.

Ellen Joyner-Roberson, Financial Services Marketing Manager at SAS, explains that a unified framework for handling financial crimes allows an organization to manage fewer vendors, enhance operational efficiency and ultimately reduce fraud. "In a perfect world, everything must be handled within an enterprise framework where the right information is reported to the right people at the right time," Joyner-Roberson says.

As banking evolves with new business channels, these channels can pose new risks. The first concern, Joyner-Roberson points out, is to know and authenticate customers so you know whom you're doing business with. This is easier said than done, which is why a layered defense should be used. Banks must take a 360-degree view of their customer using all available information. And then, when it is time to

roll out new products, fraud risks must be incorporated before going to market. "Fraud isn't always top of mind and needs a seat at the table," Joyner-Roberson says. "Some are moving into this process and addressing mitigating factors, but it's been a slow process." Joyner-Roberson provided the example of no-doc loans. "There was tremendous risk here, but the revenue outweighed the risks."

Banks will continue to build service-oriented architectures to reduce application redundancy, ensure data integrity, facilitate data sharing and lower overall maintenance costs. Including all available data, along with predictive analytics, will be essential for the effective evolution of fraud management. An enterprise data model that understands cross-channel products, lines of business and industry-specific items to better manage operational needs should push some significant improvements in scoring customers and reducing financial crime risk.

"You should be able to go back post-event and use rich information to build better models, generate trends and forecasts, and determine how new products and lines of business will impact financial crimes and the operational environment," Joyner-Roberson says. "You also should be able to incorporate all available data types – customer, household, merchant,

## DID YOU KNOW?

Financial crime is a multibillion-dollar criminal industry, costing Americans more than the combined annual spending of many countries around the world.

cycle-cut, third-party and issuer-specific data, authorizations, deposits and non-monetary transactions – into the analytical process.”

Enterprise fraud management must have rules for routing and case management, as well as the ability to capture fraud, enforce AML policies and flag transactions needing review. Analytics are critical, especially using technology that is able to learn from complex data patterns and use sophisticated decision models to better manage false positives. In addition, organizations should have the ability to load-share, balancing technology and employees’ skills, to allow collaboration and find new areas of fraud. That process must include real-time monitoring and real-time action to stop fraudulent transactions as they happen.

New investigative tools like social network analysis also need to be adopted (see p. 10, “Analytics goes social”). Many fraud cases demonstrate that banks aren’t seeing the forest for the trees, especially in the world of first-party fraud and credit loss. Social network analysis helps investigators by representing complex, previously hidden relationships in a visual way. It proves the old adage that a picture is worth a thousand words. Lastly, it is critical to establish a corporate infrastructure that encourages collaboration by allowing dif-

ferent groups to supply rules and expertise to a centrally managed fraud detection environment instead of only being able to share cases and reports.

There will always be fraud, but banks now have the ability to take the upper hand and better manage and control losses. ●

- ONLINE:
- Download fraud management best practices
- white paper: [www.sas.com/enterprise-fraud](http://www.sas.com/enterprise-fraud)


## The Value of BSA data



Financial data collected from financial institutions by the Financial Crimes Enforcement Network under the Bank Secrecy Act (BSA) has proven to be of considerable value in combating money laundering, terrorist financing and other financial crimes investigated by law enforcement. By allowing for a more thorough identification of subjects using such critical data, such as personal information, previously unknown addresses, businesses and personal associations, banking patterns, travel patterns and communication methods, the BSA helps investigators connect the dots. ●



## Chartis Research evaluates financial crime risk management systems

 Chartis Research is the leading provider of research and analysis on the global market for risk technology.

In the firm's latest report, *Financial Crime Risk Management Systems 2009*, Chartis predicts that best-practice, enterprise-wide financial crime management processes and technology will be based on the establishment of a single, integrated platform.

Chartis highlights SAS as an established leader in analytics and business intelligence software and considers SAS as one of the leading providers of technology solutions for financial crime risk management. Their latest report noted SAS' strengths in credit risk (particularly retail banking) and operational risk as key differentiators. Also, SAS software was ranked high by Chartis in several areas including advanced analytics, data management and integration, configurability and support capabilities. The Chartis analysis is based on data gathered from end users, financial institutions, leading subject matter experts, consultants and technology vendors.

According to Chartis, SAS is one of the few technology vendors taking a true platform approach to developing its financial risk management solutions. SAS' financial crime solutions integrate analytics, advanced decision capabilities and sophisticated rules into a single enterprise financial crimes platform. The solution set enables accurate scoring of all transactions at the point of sale to stop fraudsters immediately and delivers a cross channel, cross-line-of-business approach to detecting and preventing sophisticated and dynamic attacks. The functional components include data analytics and alert generation, alert and workflow management, and case management.

A significant consideration for Chartis is the ability of technology vendors to provide an integrated enterprise risk management offering. The recent financial crisis and high-profile failures have highlighted the importance of "breaking down the risk silos." The ability to analyze and report on the gaps and overlaps between credit risk, operational risk and financial crime was a key factor in their analysis in this recent report. ●

