Crimes of financial passion
High-tech practices to beat enterprise fraudsters at their own game
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Contributors</td>
</tr>
</tbody>
</table>
| 3    | Combating criminal capitalism  
Technology becomes the weapon of choice for those on both sides of the law |
| 4    | Building a better banking world  
The benefits of a unified approach to fighting fraud |
| 8    | Fraud detection with a rapid return  
Within months, Commonwealth Bank of Australia sees a 95 percent increase in check fraud detection efficiency |
| 10   | Analytics goes social  
Social network analysis identifies relationships critical to fraud detection and prevention |
| 14   | Creating an enterprise financial crimes center of excellence  
Security expert Chris Swecker on the role of analytics |
| 16   | Case study  
BBVA Bancomer improves customer service with anti-fraud technology |
| 18   | The inside job  
Tough economic times tempt both current and former employees |
| 20   | Is fraud terrorism’s new ally?  
Expert advice on detecting terrorism financing and money laundering |
| 24   | BB&T tackles AML  
How one bank’s anti-money laundering efforts paid off |
| 26   | Intelligence-driven investigations  
FBI Chief of Financial Crimes Sharon E. Ormsby discusses federal strategies |
| 30   | Case study  
HSBC improves fraud protection |
| 32   | Gauging success: measuring your anti-fraud efforts  
Report results and deploy resources more effectively |

Access this report online:  
www.sas.com/fraudreport
Contributors

Ellen Joyner-Roberson
Ellen Joyner-Roberson is the Global Financial Services Marketing Manager at SAS. She is responsible for researching current market trends in financial services to help determine strategy and direction for new banking technology solutions. In addition to managing the direction for SAS' banking solutions, Ellen is also responsible for marketing activities around the SAS Fraud Framework and positioning SAS technologies to help organizations fight fraud and prevent future fraud losses. Ellen has been involved in multiple research projects to share technologies, strategies and support organizational efforts to increase profitability, manage costs, mitigate risk and maintain greater transparency.  ellen.joyner@sas.com

Dan Barta
Dan Barta has more than 20 years of experience in fraud investigation, detection and prevention, including a position as a Special Agent member of the Bank Fraud Task Force with the Federal Bureau of Investigation in Dallas.

Currently Barta is part of a team at SAS responsible for the development of SAS' Enterprise Fraud program including the development and delivery of products and consulting. He is also responsible for the development of analytical software tools for detecting and preventing fraudulent activity, as well as the development of tools to address alert management and operational needs of fraud detection and prevention.

Barta is a graduate of Armstrong Atlantic State University in Savannah, GA, with a BS in criminal justice, and of Savannah State College with a BA in accounting. Dan is a Certified Public Accountant and a Certified Fraud Examiner.  dan.barta@sas.com

Chris Swecker
Chris Swecker is the former head of corporate security for Bank of America. Under his leadership, the largest US bank took the initiative to move toward an enterprise fraud detection model. Prior to joining Bank of America, Swecker served 24 years with the Federal Bureau of Investigation (FBI) before retiring as Executive Assistant Director over nine divisions including cyber, criminal, international operations, training, crisis management, operational technology, criminal justice information and law enforcement liaison divisions. He currently is consulting and practicing law and shared his architectural insight on how to create an Enterprise Financial Crimes Center of Excellence (EFCCE).

David Stewart
As director of SAS’ Financial Crimes & Compliance program, David Stewart contributes to strategy development of anti-money laundering, fraud management and fair banking initiatives for SAS Americas. Previously, Stewart served as a SAS Business Manager for one of the world’s largest financial institutions. He managed a team responsible for implementing enterprise scale projects devoted to customer relationship management and anti-money laundering initiatives. In addition, Stewart has held various relationship management responsibilities for financial services customers over the past 19 years. Stewart holds a bachelor of arts degree in economics from North Carolina State University and is a Certified Anti-Money Laundering specialist.  david.stewart@sas.com
Combating criminal capitalism
Technology becomes the weapon of choice for those on both sides of the law

Financial crime changes daily and is a multibillion-dollar industry. Financial institutions continue to develop strategies to reduce fraud and diminish the negative business impact of illegal practices that are becoming more complex and common worldwide. There are several safeguards, but most are inefficient, unsophisticated and disorganized. The bottom line is that fraud can be thwarted. But first, we have to understand it.

The various forms of fraud often result in the purchase of drugs, illegal weapons or even funding terrorist organizations. It is like a balloon; squeeze one side and the other side gets bigger. Today’s reality is a new form of capitalism built around pillage, criminality, corruption and complicity where bad or illegal decision making combined with insider fraud and collusion within the industry are affecting financial institutions on a global scale.

In our current economic climate, everyone is rethinking next steps in the financial industry, and most agree that fighting financial crime requires a technology solution that provides enterprise, cross-channel fraud detection. But many struggle on just how to get there. Good fraudsters are creative, highly developed, and hit multiple channels fast. The world has not seen a more sophisticated criminal, and the velocity of financial attacks today is unparalleled. A consolidated and consistent approach provides maximum return on investment as organizations manage fewer vendor relationships and use products at the enterprise level.

Fraud detection technology has evolved and now offers toolsets with predictive analytics, advanced techniques, and the ability to “learn” from experience. This “learning” characteristic enables software to increase in sophistication as more intelligence is gathered over time. The more intelligent the tools, the better the chance of detecting and predicting potential risks before criminals discover an opportunity.

Combining the early generation of fraud-fighting tools with advanced analytics and adaptive optimization gives the financial services industry the opportunity to gain ground in the fraud race. But the weapons are only as good as the data. The obvious solution is an all-in-one system where the data coming in and out is the key. That data – and how an institution leverages technology to use it – will be the weapon of choice in today’s battle.

In these pages, fraud experts and global thought leaders touch on key elements to financial crimes including how to better identify this new breed of criminal, the importance of compliance and data protection, the role analytics plays in the fraud environment, the reality of internal fraud today, and best practices to properly fight your own battle.
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,
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 different 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.

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.
Banks often take a siloed approach to addressing fraud — check fraud is handled by one group, credit card fraud by another. The Commonwealth Bank has taken a single platform approach to address all financial crime, including money laundering. Why did you choose a platform approach?

Geurts: Financial crime is constantly evolving. Local and transnational criminal groups are very fluid in their structure and approach. Equally as important, the Commonwealth Bank provides a range of integrated financial services including retail banking, private banking, business banking, institutional banking, funds management, superannuation, insurance and investment, and share brokerage products and services.

We adopted a platform approach because we needed a holistic view of fraud and financial crime that was independent of product, channel or geography. We were also looking to achieve an economy of scale, reducing data storage costs, enabling re-use across the group. In addition, we needed the flexibility to add new products, services and channels to the platform at a far lower incremental cost than installing another customized fraud detection system.

An integrated approach also provides us with the data integrity and modeling sophistication that allows us to make substantial operational improvements in alert volumes, false-positive ratios and rate of fraud detected. We simply needed to be able to future-proof our fraud systems to adapt to any foreseen or unforeseen changes in our business requirements.

Did you do migrate everything at once?

Geurts: No, we took a staged approach with our financial crimes platform and have migrated our siloed capability onto the platform, including: Internet fraud, internal (staff) fraud, application fraud, check fraud, merchant fraud and debit card fraud. We also use the platform to conduct the analysis required to get the best out of our credit card fraud system, which is provided by a bureau. And of course, transaction monitoring for anti-money laundering/counterterrorism financing compliance uses the same platform. This has saved us an enormous amount of data integration and data management rework.
How did you address the issue of staff malpractice or internal fraud, which is an area that you can’t typically get from an “out of the box” solution?

Geurts: I must make it clear that we do not specifically monitor our staff’s bank accounts, which is a common misperception. Our staff are entitled to the same degree of privacy and protection that all of our customers receive. I believe we have a sophisticated approach that balances the need for privacy with the need to protect the group and our customers from internal fraud.

In the past it felt a little like finding a needle in a haystack. We understood most of the methods of how one would commit such crimes, but it was almost impossible to detect who was perpetrating these acts without detailed data readily available. You are dealing with individuals who know and have access to the bank’s systems and have an understanding of our internal control environment. This is the value of a platform approach, enabling sophisticated models and data mining to detect unusual behavior between our staff and single or multiple accounts held with the bank.

Check fraud and application fraud – you couldn’t get this detection capability without a platform approach.

Did your aggressive goals for fraud detection present new challenges in terms of the data required?

Geurts: We initially underestimated the complexity of the task. The data previously available was never designed to assist us with what we were now looking to achieve. The level of aggregation and the availability of data were not appropriate. To overcome this, we needed to extract some data from the source systems, particularly for the bank’s demand deposit system. We had to prioritize where to start, which system to address first, and so on. This was a huge undertaking but when I look back I realize that, in building such a significant asset to be leveraged by the Commonwealth Bank, getting the data right was critical.

What results are you seeing so far?

Geurts: Check fraud detection efficiency has improved from a false-positive rate of one in 2,000 to better than one in 100 – which is a 95 percent improvement, with a similar improvement in alert volumes. We are also detecting twice the level of check fraud in the SAS-based FCP (financial crimes platform). We have achieved more than a 60 percent improvement in Internet banking fraud alert volumes and are detecting a higher rate of fraud; we are consistently achieving a one-in-12 false-positive ratio in our cards-fraud detection platform, which again is better than industry benchmarks.

Most importantly, on an indexed basis, our check and Internet fraud loss-to-turnover ratios are 50 percent and 80 percent better, respectively, than five years ago, and our card-fraud losses are marginally better. Given the sustained growth in business volumes in those five years, the reduced loss ratios have translated to a real and substantial reduction in fraud loss expense for the group since the FCP was implemented in July 2007.

What ROI did you achieve?

Geurts: We achieved very rapid benefits, within months, in terms of the efficiency of the rate of fraud detected as well as the financial benefit from retiring multiple legacy systems. As we’ve grown, we haven’t had to add staff. The staff we have can handle the work with help from the SAS solution.

What did you learn from the experience?

Geurts: We need to access highly granular data at its source; that the system must be used for transactional analysis, modeling and data discovery; and that your partner is important. SAS brought a significant amount of knowledge to this solution.
The financial services industry remains under continuing pressure to increase operating efficiency through better utilization of data. At the same time, they also must manage a wide range of risks. Many now are exploring the use of social network analysis (SNA) to drive better intelligence out of networked data to avert fraud.

Ellen Joyner-Roberson, Global Banking Marketing Manager for SAS, says social network analysis is a powerful tool in understanding the structure of social and organizational networks. Also known as link analysis, SNA is the mapping and measuring of relationships and flows between people, groups, organizations, computers or other information/knowledge processing entities. The nodes in the network are the people and groups, while the links show relationships or flows between the nodes.

“Social network analysis provides both a visual and a mathematical analysis of complex human systems,” Joyner-Roberson says. This analytic approach has practical importance because SNA tools combine data extraction, manipulation, analytic and visualization tools to distill massive databases into a visual representation of any unusual set of linkages. “Basically,” Joyner-Roberson says, “it analyzes and presents data that shows who knows whom, who calls whom, and who does business with whom.”

A new environment
Turbulent credit markets, a downturn in the economy, and the rise of organized crime all have resulted in a sharper focus on new ways to fight financial crimes.

“In this new environment, we are seeing a new criminal that is immune to conventional risk scoring,” says Joyner-Roberson. “Traditional data and record-matching techniques struggle with poor data quality and missing data, and many times miss or delay discovering deliberate attempts by criminals to hide their identities.” Legacy systems mostly resort to inexact or fuzzy matching, but this tends to generate a significant number of false matches.

Traditional approaches have inhibited the ability to visualize how relationships are taking place. By monitoring the communication patterns between network nodes, its structure can be established. Identifying the structure of an insurgent network enables identification of critical nodes and their relationships. However, this analysis is only half the battle. Predictive analysis is impossible without understanding the “pattern of life” within the network. Together, network analysis and predictive analysis give financial institutions the ability to identify the network, determine critical targets, and predict when and where targets may take advantage of an opportunity.
Joyner-Roberson notes examples of first-party fraud and bust-out fraud as a growing area of loss for banks. “This is not just typical bad credit debt. Many are establishing accounts for the sole purpose of committing fraud, and that information is going undetected by standard rules-based systems.” But with the use of SNA, banks have a unique network visualization that enables investigators to actually see connection points so they can uncover previously unknown relationships and conduct more effective investigations.

Analyzing social relationships could be particularly useful in combating organized crime rings. SNA uncovers connections that better assist investigators and analysts in producing usable intelligence. Using this technique they can uncover fraud more quickly, identify indirect crime and deceptive patterns, and leverage information linking fraudsters to illegal activities. The more sophisticated fraud rings may not be detected right away by looking at just individual transactions. Conventional systems typically fall into that category and only use rules-based analysis. But by integrating advanced analytics with existing business rules, end users can incorporate a different dynamic of analytical business rules, such as clustering analysis, mean and standard deviation, data mining and other predictive analysis to have one powerful ally in fraud prediction and protection. By using this hybrid approach to network analysis, banks can optimize their existing investment and evolve their detection process to incorporate more intelligence and refine the alert monitoring and detection process.

SNA methods in the context of an ongoing fraud or criminal investigation can eliminate antiquated guesswork and ad hoc reporting. While those methods can be economical, they do not provide the flexibility to follow a trail of links that may not be immediately apparent. An interactive reporting system enables investigators and analysts to query data and search for interesting or unusual connections.

Overall, SNA reduces the time to detect fraudulent situations while automating the time-to-resolution as companies pick up on subtle and illegal behaviors that typically went undetected.

**SNA as part of an overall fraud framework**

SAS Social Network Analysis – a solution for banking, insurance, healthcare and government – is a unique offering in the software market today. “The SAS platform approach capitalizes on SAS’ historical leadership in analytics,” Joyner-Roberson says. “It provides enhanced fraud detection, greater insight into SAR (suspicious activities report) management responsibilities, and improved operational efficiency – while decreasing fraud spending.”

SAS Social Network Analysis is a component of the SAS Fraud Framework, which delivers a technology infrastructure for preventing, detecting and managing financial crimes across the various lines of business. The platform marries the three components of detection, alert management and case management, while providing category-specific workflow, content management and advanced analytics.

These components are fully integrated with social network analysis and offer both top-down and bottom-up functionality in making hidden and risky networks more visible. Advanced, large-scale network analytics work across internal and external data sources to link customers and accounts based on common attributes or more subtle patterns of behavior. By integrating SNA into the entire fraud framework process, previously undiscovered alerts and flags can be fed back into the alert monitoring process for fine-tuning the ability to detect fraud. Social network analysis can also be integrated into the fraud framework SAS already delivers, or it can be implemented into an organization’s existing infrastructure.

While social network analysis has been present in some form or another for

**DID YOU KNOW?**

Forty-nine percent of financial crimes are committed by criminals over 40 years of age, and only 17 percent are under 30.
decades, taking the concept to fraud prevention is where leading-edge companies will make their mark in the coming years. SNA is a tool with great potential and hits on a profound truth about the way humans interact. Observing behaviors through SNA allows views that may alter the way we think and touch on deeper realities about what we need to do to protect customers.

SAS Social Network Analysis includes reporting and dashboard capabilities to help track fraudulent claims by region, calculate amount of claims by channel, and integrate additional fraud and audit reports. Dashboard metrics and displays are customizable and the interactive dashboard provides critical information and reports formulated to meet user needs.

In this fraud scenario, people with different names were opening accounts, but they were linked by a similar address or phone number. This social network analysis view shows a first-party fraud ring with open, unsecured credit lines (green nodes) and a suspicious mortgage application (red node). Note the number of open credit lines that could indicate a “bust out” fraud ring.

ONLINE:
Visit www.sas.com/fraud-sna

Creating an Enterprise Financial Crimes Center of Excellence

Security expert Chris Swecker says analytics is key to prevention

Public perception of how safe a financial institution is can be just as important as the security systems, policies and procedures put in place. Banks in particular have been warned that when it comes to securing the enterprise, regulators and government agents are watching to make sure the job gets done correctly. Security consultant Chris Swecker says analytics is the most critical area right now and that making sense of your data and using technology to drive prevention efforts is essential to success.

Swecker is the former head of corporate security for Bank of America. Under his leadership, the largest US bank took the initiative to move toward an enterprise fraud detection model. Prior to joining Bank of America, Swecker served 24 years with the Federal Bureau of Investigation (FBI) before retiring as Executive Assistant Director over nine divisions including cyber, criminal, international operations, training, crisis management, operational technology, criminal justice information and law enforcement liaison divisions. He currently is consulting and practicing law and shared his architectural insight on how to create an Enterprise Financial Crimes Center of Excellence (EFCC).

EFCC is a bold concept, a working group bringing together all aspects of financial crimes to take a thorough inventory of tools, rationalize the use of multiple technologies and vendors, and focus on investigations, AML compliance, information security and fraud prevention across the entire organization. Swecker says the initiative at Bank of America involved taking a proactive approach to managing technology acquisitions and leveraging technology across the various financial crime organizations not under the same hierarchy. It also required looking back to inventory existing technology and driving the integration of multiple platforms. “In other words,” he describes, “we put together an integrated acquisition strategy where we were managing the technology, not vice versa.”

Swecker advocates bringing together all technology components that support the various financial crime organizations and conducting a workshop to inventory their applications and identify overlaps. Next, he says, organizations need to map out the processes that technology supports and look for overlaps and similar functions. An agreement has to be reached to vet all technology acquisitions through the EFCC and work to create a multigenerational plan to reconcile the various existing technology platforms. Lastly, those involved need to apply a measure of patience and perseverance. It will take time, relentlessness and steady motion through budget challenges and daily distractions.
Swecker says the overall strategy should be built around prevention and protection. Having a prevention mindset is a major component to fraud deterrence. Another critical component is the idea of customer ownership and the need to increase customer awareness.

“The job is three words: Protect the customer,” he says. “Criminals are realizing that financial institutions are getting better at protecting data so they are going after customers instead. We all have a responsibility to safeguard customers, which also means helping create fraud-proof customers through good education and awareness.”

Knowledgeable in the dark workings of the financial crime underworld, Swecker is well aware of the complexity of the environment, stressing the need for a good team of employees and solid analytics for those employees to decipher and understand. “There are some very bright people who are computer savvy, organized and understand the inner workings of bank processes who are committing these crimes right now. They are good socio-engineers that do not operate in silos … whatever is vulnerable, they will go after. Our job is to stay one step ahead.”

Swecker certainly pushes for analytics to drive prevention and recovery strategies. He adds that only analytics can identify trends, patterns and the cases that should be prioritized as potential loss recoveries. “Identifying trends and patterns allows you to be predictive and thus preventive,” he continues. “I believe the current focus should be on analytical products that are capable of mining data from hundreds of data sources to provide a view of fraud rings by linking common data points shared by multiple fraudsters – i.e., social network analysis.”

The money spent on compliance and data protection is only a small percentage of the financial and reputational value that a business risks without it. There was a 47 percent recorded increase in data security breaches over the last year. Customers are not going to do business with a vendor who doesn’t take these kinds of steps. Business is organic. Organizations must set realistic expectations as well as manage and anticipate change. Perhaps it’s the fragile economy, the media, paranoia or a combination of the three, but combating financial crime is clearly on the business radar and solid analytics will enhance the ability to regain the advantage over criminals.

**DID YOU KNOW?**
About half of financial criminals fail to go beyond high school. Forty-two percent earned bachelor’s degrees and only nine percent have post-graduate degrees. But, as education levels increase, so does the size of the fraud loss.

---

**Five ways to create an Enterprise Financial Crimes Center of Excellence**

1. Inventory technology applications and identify overlaps.
2. Map out the processes that technology supports.
3. Agree that all technology acquisitions go through the EFCCE.
4. Design a multigenerational plan to reconcile the various existing technology platforms.
5. Practice patience and perseverance during the process.
The BBVA Bancomer Financial Group needed a way to detect suspicious credit/debit card activity with greater ease and precision. With more than 10 million cardholders and an average of nearly 300,000 daily transactions, BBVA Bancomer is constantly challenged to improve the customer’s purchasing experience.

How can a company guarantee optimum card service to the customer while also increasing controls to reduce losses due to fraud? Bancomer executives answered this question by improving the depth of card-use analysis and by analyzing fraudulent use to identify patterns of behavior. This analysis helped bank leaders define operational models and create effective authorization and fraud-detection strategies.

BBVA Bancomer chose SAS as part of its fraud detection and prevention strategy. Made up of nearly 25,000 employees and more than 10 million customers, the multinational group adopted SAS Fraud Detection and Prevention for Financial Services. It also developed more efficient operational and security methodologies. The end-to-end knowledge structure has been designed to create fraud intelligence consistently and reliably in a long-term sustainable way.

The solution monitors suspicious transactions and analyzes transaction data to identify new patterns and refine fraud alert engines so bank leaders can efficiently handle cases of potential fraud.

According to José Gastón Huerta Gutiérrez, Director of Fraud Prevention for BBVA Bancomer, an important factor influencing the choice was the critical handling of confidentiality within its fraud containment activities and processes. This meant the team also was looking for a provider that was solvent in all respects.

Using SAS Fraud Detection and Prevention for Financial Services as part of a package of key improvements, BBVA Bancomer has achieved significant results. “The negative impacts on customer service when customers use their card have been significantly reduced,” says Huerta Gutiérrez. “Likewise, our dedicated staff can now perform other types of analysis and take advantage of their experience and abilities to develop new knowledge, something they were not prepared to do before.”

Huerta Gutiérrez says SAS has provided significant advantages in fraud protection. “SAS developed a data mining model that allowed the best criteria for effective discrimination between customer purchases and fraudulent purchases,” he explains. In addition to reducing possible losses, the project also will reduce operating costs for combating fraud and create a more flexible platform that allows BBVA Bancomer to respond more quickly to new threats.

Overall, BBVA Bancomer has increased the precision index for identifying fraudulent transactions and improved customer service. These results are reflected in a 40 percent improvement in customer service from customers using cards for purchases. When combined with other measures implemented, the institution has simultaneously reduced its losses by more than 30 percent.
Financial institutions continue to focus most of their investment dollars and attention on external fraud applications, although industry research confirms that internal fraud is just as big a problem. At the highest executive level, internal fraud once was considered a cost of doing business. However, that focus has shifted because internal fraud is costing considerable funds and also threatens a company’s reputation.

According to the Association of Certified Fraud Examiners (ACFE), 60 percent of bank fraud cases are committed by employees. A typical US organization loses 5 percent of its annual revenue to internal fraud, with the banking industry being the hardest hit. The ACFE notes that 14.3 percent of all internal fraud cases occur at banks, with a median loss of $258,000 per case. Analytic tools similar to those used to monitor and detect external fraud can be used for internal fraud. Industry insiders estimate that internal fraud cases typically take 18 months before a company detects a scheme. Therefore, internal fraud-detection technologies provide a valuable return on investment by allowing banks to identify suspicious employee behavior before the damage is done and losses are incurred.

Dan Barta is Director of Enterprise Fraud and Risk Strategy at SAS and has more than 20 years’ experience in fraud investigation, detection and prevention. “It’s important to have a good understanding of total exposure,” Barta explains. “With the economy in the tank, people are going to look for ways to gain income. This scenario has provoked more internal fraud within the last year and caused a lot of heartburn because the global economic climate has put a bunch of experts out there who are jobless and looking for money.”

In troublesome economic times with layoffs announced almost daily, today’s insider threat is not just coming from the people currently inside your walls; it’s coming from the people who used to be inside your walls and know the systems and databases, and are bitter about losing their job. Even if access has been blocked, they still have valuable knowledge of how things work internally and take advantage of it. They either participate in schemes directly or are willing to sell information to those who conduct such schemes. Former employees in the banking industry in particular, where processes are so ingrained in the corporate culture, pose a unique danger because they are out of a job and know how to fly below the radar. They know the processes of customer identification, fraud monitoring, ATM processes, credit card transactions, and what constitutes a red flag. Basically, they take the “house” with them, and it’s very common to see former employees selling or taking advantage of the vulnerabilities they know exist.
The fraud triangle explains the conditions under which someone might become involved in fraudulent activity. First, they feel perceived pressure. The pressure might come from someone outside the organization or from their own financial pressures at home. Second, the individual expresses rationalization. Many employees see their company being profitable and think, “Hey, they’ll never miss it.” Finally, when faced with an opportunity to commit fraud, the perfect storm is created. The fraud triangle typically applies to the marginal fraudster; others are career criminals who seek employment with financial institutions for the sole purpose of defrauding them.

So how does internal fraud affect your customer base?

Obviously, there’s the actual loss. For example, a bank teller processing a check may notice a high balance on an account. He or she writes down the account number and gives it to a counterfeit check writer. It’s just that simple. Customers suffer the headache, and the bank is responsible for reimbursing the loss. But, there’s also the reputational risk. The institution’s image is affected drastically and may lose valuable business based on negative publicity.

Banks must take preventative measures to avoid the risk of employees acting fraudulently and incorporate predictive analytics and technology to better identify potentially fraudulent activities. The industry as a whole is getting better at finding internal fraud, but there is certainly room for improvement. Most systems and fraud detection processes are geared toward working individual actors as opposed to understanding how they network. One pops up here, deal with it; another over there, deal with it. But this approach will allow fraud to continue and become more organized over time.

“Internal fraud is massive and difficult to combat and detect,” Barta says. “Employee-associated fraud can potentially devastate a business and destroy reputations. Don’t take a chance with decisions based on assumptions.”

Internal fraud checklist

The following is a managerial checklist to combat internal fraud in banking:

- Create and promote an anti-fraud culture.
- Reward whistleblowers.
- Monitor changes in employee behavior and/or lifestyle.
- Establish an audit committee.
- Monitor approved vendor lists.
- Physically secure the business premises and assets.
- Restrict after-hours access.
- Establish a schedule or rotation of employee responsibilities.
- Make the most of information technology and analytics.
- Review technology security for proper administration and access rights.
Today’s terrorists use many of the same sophisticated business practices as legitimate multinational corporations to achieve their goals. Terrorists are not just stealing funds; they are stealing credit card information, social security numbers – entire identities – and selling them for profit. For example, Al-Qaeda has been known to encourage and instruct terrorist cells in ways they can fund terrorist actions through various financial crime activities.

The threat of terrorism changes the geopolitical landscape. Everyone is concerned about it and the reputational risk it involves. No technology has done an exceptional job at detecting terrorism financing, and many tools available today may be considered as racial or ethnic profiling tools that violate civil liberties. “However,” says David Stewart, Americas Sales Director for the Financial Crimes Business Unit at SAS, “technology can be used legally to monitor three important areas: high-risk institutions and nongovernmental organizations (NGO) such as charities or nonprofits; sanction lists; and high-risk geographies.”

With high-risk institutions and NGOs, transactions can be closely monitored and scrutinized to detect patterns and behaviors. Using sanction lists can align monitoring with the Office of Foreign Assets Control. Banks are required to screen wire transactions for sanctioned persons, lists and entities. For example, no US bank is allowed to do business with the Central Bank of Iran. There are also high-risk geographies where about 50 to 70 countries are strictly monitored and large wires are closely scrutinized. Financial institutions must examine these three areas closely.

**Combating money laundering**

Regarding anti-money laundering, Stewart says, “Compliance officers are faced with an environment of rapid change and need to mitigate their regulatory and reputational risks – and do it at a reasonable cost of ownership.” The regulatory environment is ever-changing and regulatory agencies are placing greater scrutiny on compliance officers. “Let’s be honest,” Stewart says, “we live in a different world today. The global nature of electronic commerce is no longer a problem just for money-central banks; it’s a problem for every financial institution.” Stewart notes risks also lie with instruments like stored-value cards, mobile payment technologies, Internet gambling and other money-service businesses.

To combat money laundering, Stewart advises that organizations must be able to:

- Scale large volumes of data and monitor all customers and relationships using advanced techniques such as link analysis, clustering analysis or near-neighbor techniques.
• Support integrated investigation environments to speed up the decision process.
• Score risks and analyze customer behavior across product lines.
• Apply business intelligence via ad hoc analysis, so the system can look back at data and learn from it.

“By adopting the use of advanced analytics and taking a proactive approach to enhanced due diligence, financial institutions have made it more difficult for regimes to fund terrorism,” Stewart adds. “With added scrutiny on non-governmental organizations, terrorists will have to start looking elsewhere for financing.”

Business leaders in the long term will need to change their thinking from an operational paradigm to one of innovation. Terrorists mingle in and out of the underground economy when it suits their monetary needs and objectives. While they will never publicly admit to taking advantage of stolen personal and financial information, it is evident that it is a much bigger problem than many people realize.

DID YOU KNOW?
Most found guilty of a financial crime are first-time offenders.

Financial Crimes Enforcement Network (FinCEN) is an excellent resource for investigating identity theft and other financial crimes. FinCEN links databases maintained by law enforcement, financial and regulatory communities. Its purpose is to collect, analyze and share information with law enforcement agencies. FinCEN accesses approximately 37 different independent databases in three main categories: law enforcement, financial and commercial. The databases include AutoTrack, LexisNexis, the Social Security Administration Death Master File, Drug Enforcement Administration, Federal Bureau of Investigation, and Internal Revenue Service databases, to name a few.

The Computer, Financial & Intelligence Division (CFI)

The Computer, Financial & Intelligence Division (CFI) is a division of the Office of Training Operations (OTO) at the Federal Law Enforcement Training Center (FLETC). It designs, develops, coordinates and administers training programs related to the prevention, detection, investigation and prosecution of complex financial and computer-related crimes. The CFI is under the US Department of Homeland Security and serves the needs of the FLETC’s participating organizations and other federal, state, local and foreign law enforcement agencies.

ONLINE:
• Download the white paper: Reducing the cost of AML compliance: www.sas.com/fraud-aml

Take an interactive look at seven areas you should consider when designing your monitoring and surveillance program: www.sas.com/fraud-itour
USA PATRIOT Act

The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes, some of which include:

• Strengthening prevention, detection and prosecution of international money laundering and financing of terrorism.
• Subjecting to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse.
• Requiring all appropriate elements of the financial services industry to report potential money laundering.
• Strengthening measures to prevent use of the US financial system for personal gain by corrupt foreign officials and facilitating repatriation of stolen assets to the citizens of countries to whom such assets belong.
The frequency of false-positive fraud events has caused bankers to wrestle with whether to investigate suspicious activities at the risk of harassing legitimate customers. Reducing false positives minimizes this risk – and the associated costs – without jeopardizing the ability to reduce fraud loss. While there is no way to eliminate all false positives, organizations can reduce them significantly with the following steps:

- Obtain good client information.
- Implement clear policies and provide adequate employee training.
- Reduce the time between fraud occurrence and detection.
- Review each false positive.
- Establish a clear definition of politically exposed foreign persons (PEFP).
- Incorporate analytic software that can match commercial watch lists with client lists.
- Use watch lists to determine who might potentially be a PEFP.
- Provide detailed reviews of applications, databases and data sources.
- Identify how data is being formatted for screening.
- Identify which data elements should be used.
- Perform a comprehensive review of screening matches.
- Conduct an impact analysis of false-positive rules.

Data and diligence can reduce false positives
The banking industry continues to address the need for due diligence in identifying suspicious activity, maintaining financial integrity and reducing operating costs. However, post-9/11 regulations require additional measures in identifying and reporting money-laundering activities, particularly those related to suspected terrorist financing.

In response, BB&T Corporation, the nation’s ninth-largest financial-holding company, turned to SAS Anti-Money Laundering to help meet regulatory requirements. The organization found that SAS provided an easy-to-use program with solid technical support.

“There’s a lot more scrutiny placed on financial institutions to prevent and report financial crime,” says Mason Hinkle, BB&T’s AML Manager. “In a global economic environment, AML tracking really is a best practice from a safety perspective and in terms of the soundness of our institution.”

With more than 16 million accounts tracked daily at BB&T, manual AML monitoring was out of the question. The bank could not handle this monumental task with traditional detection solutions. In fact, BB&T created a 26-member group devoted specifically to AML monitoring. The group came up with solutions to meet regulations and to contribute to the overall stability of the company, including the need for tracking software. BB&T uses other SAS tools and needed an AML solution that was flexible and could grow as business needs and regulations changed.

Implemented in 2004, the database of banking transactions processed through SAS is updated nightly rather than in weeks or even months. Scenarios are run against the database to pinpoint suspicious activities, which are quickly revealed. At any given time, BB&T runs about 25 scenarios, ranging from structuring wire activities to cash transactions. This provides a good overview of the complex activities of a large and growing number of bank clients.

“Consolidation of all the data provides a unique advantage,” says Ann Norvell, BB&T’s AML Investigations Manager. “We can retain and house information with the SAS application. Activities that may not look suspicious or warrant further investigation at the time may come into play at a later date. The historical data and comparative analytics give us a real advantage.”

SAS allows BB&T’s AML group to track transactions overnight with analytical, scenario-based returns that include broad comparative capabilities, historical tracking and relevant day-to-day information. “It is rewarding to read in the press that some of the activities we detected with SAS assisted law enforcement in their investigations,” says Hinkle. “Having a dedicated AML solution provides access to accurate data, which allows us to quickly identify suspicious activity.”
Intelligence-driven investigations
FBI Chief of Financial Crimes Sharon E. Ormsby discusses federal strategies

Given the rise in financial crime and its broad impact from Wall Street to Afghanistan, what is the US federal government doing to tackle the issues? Special Agent Sharon E. Ormsby, FBI Chief of Financial Crimes, has more than 20 years’ experience in investigating white-collar crimes and is the FBI’s top expert in combating this activity.

How have financial crimes influenced the FBI’s organizational structure?
Ormsby: Financial crime is a component to all crime problems and criminal activity. Crime really has two components: financial crimes and violent acts. These are the two underlying components to any criminal activity. Most of the financial crimes we look at usually involve some form of money laundering. When we look at criminal enterprises, most times we look at them from a financial perspective: How do they operate, who’s involved and what is their financial structure? The financial structure will provide a lot of intelligence about a group and what they are doing. They have to find ways to fund their illegal activities, and financial crimes tend to provide that information.

How important is financial crime prevention for national and economic security?
Ormsby: Our financial crimes mission statement is to protect the nation’s financial markets through the use of sophisticated techniques, effective liaisons or criminal organization analysis, training, intelligence, and coordination of national strategies for the purpose of combating white-collar crime on a national and international level. The bottom line is that financial crimes could undermine the economic structure of this country if left unchecked.

In other words, criminals basically need money to do what they do?
Ormsby: Exactly. It’s that underlying greed factor that is always going to perpetuate what they do. After investigating these types of crimes for many years, it always amazes me that the millions of dollars these criminals make illegally probably could have been earned legitimately in the marketplace.

What steps has the FBI taken to prevent financial crimes?
Ormsby: Public and private sector outreach remains an important component. We want to help create a fraud-proof citizen. This is an ongoing initiative to get important information out to our citizens so they can better educate themselves. We also participate in several national working groups such as the Bank Fraud Working Group, the Mortgage Fraud
Working Group and many others to further compel our mission to use intelligence to drive investigations. Task forces really are a force multiplier. This kind of collaboration was encouraged as far back as J. Edgar Hoover. We can never have enough resources to do the things that we need to do, so bringing together the expertise of many gives all of us more of an advantage. Also, the continued development of confidential informants gives us the opportunity to better identify insiders. Those sources act as our experts and provide valuable information on emerging criminal activities. We also use sophisticated techniques (undercover operations) to do proactive work and target active enterprises. Lastly, with an industry perspective, if we look specifically at the current credit crisis, we have been able to create an industry fraud initiative and put it in place. The strategy has multiple parts, but one of the most important parts is to look at all the intelligence that exists in the actual criminal scheme or enterprise. This provides us good information because if the criminal activity occurred in a financial institution, then the financial institution is going to file a suspicious activities report.

What does that report provide?
Ormsby: The raw data helps us to identify who the potential perpetrator is and give a basic outline of the allegations in reference to the criminal acts. It also provides dollar amounts, specific and general city locations, etc. We use intelligence to drive investigations, and this report tells us a little more about what is going on, which helps us to better understand the criminal enterprise as well as the scheme they are developing. The report also helps us develop a trend analysis to look at what they could do, and a threat analysis of what they are doing. That’s one aspect. Then, we take that intelligence and share it with our federal, state and local law enforcement as well as industry representatives. Industry representatives are closest to the pulse of what’s going on. By sharing information, we can look for intelligence gaps and make sure we all understand the information in the same realm. The FBI might be looking at the scheme one way and industry might be looking at it another way. But, by sharing and discussing the information, it allows us to put on the table what we’re seeing, why we’re seeing it, and better address the issue. And, we do it in concert with Department of Justice, industry representatives, and additional federal agencies such as HUD, FDIC, IRS and many others.

The collaboration on intelligence is important, but what about the investigations themselves?
Ormsby: That’s the other part of the equation. The intelligence drives the investigation but the investigation feeds the intelligence. It’s a circular process that is constantly fueled and feeding itself to help us forecast threats and trends.

Do you have an example of this?
Ormsby: In 2004, the FBI put an analysis together that said mortgage fraud and credit issues were going to be a problem if the industry was left unregulated. When you read this, you would think it was written today, based on our current situation. The interesting part is that the residual effect could lead to bank failures. The point here is forecasting. We really need to be forecasting what could be coming next so we can use our resources more effectively and efficiently. That’s a good example of how we want to continue having the ability to predict what’s coming, not just in credit or mortgage issues, but in all criminal activity.

How is the FBI leveraging technology to combat financial crimes?
Ormsby: One of the things we’re doing with technology is using inter-relational databases and products that will help us do link analysis by taking data – whether it’s industry data, internal data, or a hybrid of the two – and find those commonalities. Financial crime isn’t just local; it’s international and across program lines. We deal with crime in a structured sense, but
criminals don’t and they just do whatever is advantageous for them. It’s important that we use technology and exploit as much information as we can about what these criminals are doing.

**How important is good data and intelligence when it comes to financial crimes?**

Ormsby: Since money is the key to almost everything we do, intelligence analysis of financial data is critical regardless of the crime problem. Following the money can really tell you a lot about what a person is doing. It’s absolutely critical that the data be reliable to forecast threat assessments and trend analysis. If the data isn’t accurate, then we’re going to be all over the map.

**What are the most serious threats to citizens from a fraud-risk perspective?**

For us, we really take a deep look at the current conditions of the economy. For example, vulnerability exists for many citizens right now as credit tightens and we see more mortgage fraud. In fact, a recent article by MARI (Mortgage Asset Research Institute) notes that mortgage fraud has jumped 42 percent nationwide, Florida having the highest number of cases. This is a time when lenders are raising credit standards to curve rising foreclosures but not necessarily eliminating the issues of fraud. So, any time we take an action, criminals react and come up with something creative to overcome a law.

**How real is the threat?**

Ormsby: Everybody is vulnerable and everybody can be a victim. The public needs to be conscious of that. Take the example of a consumer making purchases online. Consumers should only use one credit card for online purchases to reduce the threat of identity theft. Or, instead of putting your bills in the mailbox for pickup, drop them off at the post office or a secure mailbox. Also, pull your credit report once a year and look for any potential fraudulent transactions. And be careful with your trash. It is amazing what you can learn about someone from their trash. These are simple measures that can reduce the risk.

In this day and age there is so much data on individuals being sold and transferred around it’s getting harder to protect the information about ourselves.

**How is the FBI working to stay ahead of the threat?**

Ormsby: What happens in our market really does have an effect on the rest of the world. Right now our concerns fall into the area of mortgage fraud, especially reverse mortgages. This is a concern for us because many people could be affected and be taken advantage of in fraudulent ways. We also have a concern that the ripple effect from mortgage fraud will continue to adversely affect some banks and create additional bank failures. Further down the road, we see stored value cards having some impact in one form or another, which falls along the lines of e-currency and eventually mobile payment opportunities. These areas are of concern and preventative measures need to be put in place. Otherwise, the ability to defraud citizens will increase in a variety of new and different ways.

**ONLINE:**
- Read more about FBI initiatives and interesting cases: [www.fbi.gov/whitecollarcrime.htm](http://www.fbi.gov/whitecollarcrime.htm)
Case study
SAS and HSBC partner to revolutionize fraud management

SAS and HSBC believe that fraud prevention and detection should be an industrywide shared goal. That’s why the two companies joined forces to develop SAS Fraud Management, a fraud detection and prevention solution that empowers banks and other financial institutions to combat credit and debit card fraud on a global scale, in real time.

Just three months after the solution’s 2007 implementation in the US, HSBC achieved:

- Enhanced customer protection, because the solution monitors 100 percent of the bank’s US credit card transactions in real time.
- Greater accuracy, since all available data — account, payment and non-monetary — is used in the authorization process.
- Better customer service, by deploying a greater number of rules that reduce the number of incorrect and unnecessary fraud-related customer contacts.
- Improved operational efficiency for HSBC.

Specific results from the US implementation included:

- An 87 percent increase in the number of data items processed, including card transactions and customer information.
  - A corresponding 12 percent reduction in mainframe processing overhead.
  - A 53 percent decrease in mainframe processing cost per data item.
- A 30 percent decrease in computing resource costs for processing card transactions flagged as potentially fraudulent.
- A 10 percent increase in efficiency by agents investigating potentially fraudulent cases when compared to the proprietary case management system.
- Reduced IT support costs following the elimination of three software applications.

Since its initial US launch in 2007, SAS Fraud Management is now live across HSBC in the US, Europe and Asia Pacific. Hong Kong, Philippines, Singapore, Thailand, Macau, Brunei and Sri Lanka are all now using it to protect 100 percent of their credit card transactions in real time. HSBC UK, including First Direct and M&S Money, is using the solution to protect all of its UK credit and debit cards. With this, SAS and HSBC are now realising the original joint-development vision of an enterprise-wide risk system.

Online:
- Download the SAS Fraud Management product brief: www.sas.com/fraud-brief
SAS earned the 2008 Technology Innovation of the Year in the field of Enterprise Fraud Detection and Prevention by Frost & Sullivan. After thorough analysis of the fraud solution market, the research firm found that SAS Fraud Management integrates advanced analytics, superior decision-management capabilities and sophisticated rules into a complete scoring and reporting platform resulting in accurate scoring of banking transactions, including those in real time at the point of sale. This integrated approach combines analytics, alert generation and alert management that help a bank adapt to a rapidly changing environment and address new fraud issues as they arise.

“Fraud has evolved into an inexorable and pervasive issue in the banking and financial services domain,” said Frost & Sullivan Research Analyst Achyuthanandan Sampath. “SAS’ radical fraud management solution is equipped with all the capabilities necessary to completely immobilize fraud crimes. Its core technical aspects also stand testimony to the progress made in the area of fraud detection and prevention. This makes SAS Fraud Management indispensable for all banking and financial institutions.”

SAS Fraud Management recognized by Frost & Sullivan

www.sas.com/fraudframework
Gauging success: Measuring your anti-fraud efforts
Report results and deploy resources more effectively

Setting goals, milestones or performance metrics are common for determining success in business. In a broad sense, a company uses a profit/loss or income statement to determine profitability or performance for a certain period of time. This same method can be applied to determine success rates for financial crime prevention.

Fraud detection and prevention metrics have been a challenge in the past. In the early '90s when fraud detection became a focus of the banking industry, the increasing size of general ledger accounts for charge-offs and other losses was becoming a significant contributor to overall expenses and affecting profitability. It was not uncommon for these loss accounts to contain not only fraud losses but also uncollected overdrafts and fees, bank robbery losses, teller outages and a multitude of other items. The end result was general ledger accounting that was not an appropriate or a sufficient means of tracking the detailed losses incurred by banks.

As loss numbers grew, a more detailed analysis occurred and revealed that a significant amount of these balances were in fact due to fraudulent activity of customers and third-party perpetrators. This revelation prompted the creation of fraud prevention departments who then implemented a number of procedures and software products to battle the fraud. These early initiatives focused on fraud awareness training, implementation of check and deposit fraud, and kiting detection software. It has evolved over the years to be a detailed scoring process used to assess success and to better understand the issues at hand. Early on, the raw amount of loss was the primary metric for success. As fraud detection and prevention matured, far more data intelligence has been developed to measure success in other ways.

Measuring success of systems and processes requires maintaining certain types of data and information. The task of optimizing a system or process requires different data and a different way to look at it. The most common rationale to measure fraud is a need to know the extent of the problem to effectively solve it. Without knowing the size and scope of the problem, how do we know where to deploy resources? The scarcity of money and staff to combat fraud suggests that efficient allocation of resources is vital in order to effectively deter and detect fraud. “Understanding the characteristics of the fraud is critical to making the correct decisions regarding the selection and calibration of software solutions,” states Dan Barta, Director of Enterprise Fraud Strategy at SAS. A consistent measurement system is needed to understand the degree of impact various solutions have on the problem. This is especially true in determining whether anti-fraud activities have any impact on deterrence, which may be
even harder to measure than the extent of the problem. Another important reason for consistent measurement is public credibility. Consumers are more likely to buy into solutions if they are convinced a problem exists and will directly affect them.

Companies also must address false positives and false negatives. False positives are those transactions identified by a particular fraud detection software that upon further review turn out to be legitimate transactions that posed no threat. The goal generally is to minimize the number of false positives without affecting detection and prevention. Although not a risk to the bank, false positives are a hindrance resulting in lack of productivity. False negatives are those transactions or activities that are truly fraudulent that went undetected by the system or process and resulted in a loss to the organization. Overall, an organization wants to find the optimal position where false positives and false negatives are minimized and the cost of reaching that position creates an appropriate business case and return on the investment made by the organization.

In today’s economic environment, senior management remains under increasing pressure to produce results in the fight against fraud. Financial institutions need to take a comprehensive look at tools and methodologies to improve efficiency and better understand the fraud environment. Measuring fraud will never be easy and likely will remain controversial. Reaching consensus on definitions and methods will be difficult, especially when people focus narrowly on their own operations instead of keeping the big picture in mind. But such consensus is essential if effective measurement programs are to help spotlight damage caused by crime and ultimately convince the public and decision makers how much fraud affects the economy and our lives. ☝

**Fraud measurement checklist**

- Develop concise definitions of fraud for the purposes of uniform measurement.
- Take a comprehensive look at tools and methodologies to improve efficiency and effectiveness.
- Secure aggregate reporting data to determine whether data could be extrapolated for measurement purposes.
- Develop methodologies for measuring the extent of fraud.
- Address the impacts of false positives and false negatives as well as how they relate to each other.
- Seek an agreement within the industry on how to provide more consistent estimates.
- Resist publishing estimates that are not based on some level of scientifically valid studies.

---

**DID YOU KNOW?**
The FBI received a total of 206,884 fraud complaints in 2007, with total losses at their highest level in history.
Koalas spend most of their time in trees.

They don’t have a better way of protecting themselves.

But you can. With proven fraud management software from SAS.

www.sas.com/koalas