

## Financial services: Real-time fraud countermeasures

By Judith Lamont, Ph.D., - Posted Jul 3, 2010

From the simple to complex, fraud committed against financial institutions costs them and their customers billions of dollars per year. Here are some examples:

- Stolen credit card numbers are used to purchase a variety of expensive items in a short amount of time, before the owner notices the charges.
- Legitimate checks are duplicated using high-quality copiers and cashed using falsified identification.
- A member of a fraud ring hacks into a bank account after infecting consumers' accounts with Trojan horses that let them steal log-in information. He liquidates stock in the brokerage account and transfers the funds into a new account set up by a partner. The partner removes the cash and divides it among members of the ring.

Fraud against financial institutions is a problem worldwide. In Australia, for example, fraud doubled in the last six months of 2009, according to [KPMG's Fraud Barometer](#), which monitors the incidence of large frauds coming before the criminal courts in Australia. Banks and financial institutions accounted for one-third of total fraud. In India, financial fraud doubled in 2009, with 87 percent of public and private sector organizations reporting losses, according to the "India Fraud Survey Report 2010."

In the United States, the [Federal Deposit Insurance Corporation](#) (FDIC) issued an alert to financial institutions in August 2009 regarding fraudulent electronic fund transfer (EFT) transactions. The alert cautioned banks about the increase in losses due to compromised login credentials. One small bank in Pittsburgh failed after a single, large fraudulent transfer. A [LexisNexis](#) study estimated the value of fraudulent credit card losses to banks at about \$10 billion. Losses due

to check fraud by banks, businesses and individuals are estimated at \$50 billion.

### **Detecting suspicious behavior**

Although online fraud is not the sole origin of fraud, the proliferation of electronic transactions has opened new options for fraudsters. At the same time, having transactions available electronically also means they can be monitored the same way. Solutions from business intelligence (BI) vendors and specialized software programs are providing an important line of defense against fraud.

The [Banco Agrario](#) in Colombia provides banking services for rural customers and those involved with agriculture, livestock, fishery, forestry and agribusiness. It has more than 8.5 million customers and completes over 7 million transactions per month. The bank wanted to manage its risk and comply with regulations from the Superintendencia Financiera de Colombia, which is the national supervisory agency for Colombian financial institutions. Banco Agrario, therefore, was seeking a method for analyzing the transactions to detect behavior that might be indicative of fraud.

Rather than relying on a retrospective analysis, Banco Agrario wanted to use a predictive model for early detection of potential fraud. In January 2008, the bank selected [IBM SPSS](#) predictive analytics software. The IBM SPSS software was chosen after an evaluation process based on technical performance, vendor experience and professional services. The suite includes data collection, modeling, analytics and reporting components.

The risk department of Banco Agrario is responsible for controlling risks set in the Basel II Accord, and one of the units within the department is specifically responsible for fraud. After obtaining training and consulting from outside the bank, personnel are now able to develop and maintain the models on their own.

### **Looking for outliers**

The IBM SPSS software compares customer behavior to normal models and detects anomalies. Those divergent patterns are used to flag behavior that is consistent with fraudulent actions. Through the use of IBM SPSS predictive analytics, the bank has been able to quickly detect and block fraudulent operations. Its success in doing so produced a very quick ROI.

"We are very satisfied with the results obtained through the implementation of these tools," says Eliecer Perdomo, VP of risk at Banco Agrario. In addition, the use of an analytic solution for fraud detection has produced a cultural change in the organization, with greater awareness of the importance of caution and controls.

In general, the detection of fraud through pattern analysis focuses on looking for outliers. "Inconsistencies in credit card charges is an example of how analytics can aid in fraud detection and prevention," says Erick Brethenoux, predictive analytics strategist for IBM. "A customer can't make legitimate transactions in five different physical locations simultaneously, so that's a clear warning sign."

### **Alert triggers**

Many consumers have had the experience of a credit card company putting a hold on their card if such inconsistencies arise. "Unusually large purchases for someone with a small income, or an unusually large number of small purchases are events that can easily be picked up by analytical tools," Brethenoux says. Rules within the system trigger an alert that allows the bank to follow up quickly.

Detecting fraud in banking has much in common with detecting fraud in other spheres. "In healthcare, we also look at patterns, such as going to a large number of different doctors or filling prescriptions at multiple locations," Brethenoux adds. Demographics, past behaviors and the nature of the transactions are all ingredients for such analyses.

Data mining, which searches for previously unknown relationships in the data, offers greater flexibility than systems based solely on rules. "Sometimes you don't know the questions to ask," Brethenoux says, "and it can take a long time to figure out what is relevant. With data mining, the analyses can highlight these relationships, and then a rule can be constructed to set off an alert." Because the analyses are ongoing, organizations can keep up with a constantly changing set of fraudulent activities.

Organizations can make back their investment in a relatively short time. "Although the ROI varies widely," says Brethenoux, "about 94 percent of our customers break even on the investment within a year, when all the resulting benefits are considered." The change is most dramatic when the product is first deployed, and then tapers off, but clearly

the advantages remain as part of a long-term risk management strategy.

Over time, each organization has to consider the trade-off between putting in checkpoints for transactions and keeping up the pace of business activities. "If you are going to require approval for expenses over a certain level, you need to make sure it does not slow down the purchaser too much," Brethenoux explains. "Ideally, the amount saved in fraud will not exceed the amount lost to unfulfilled transactions."

## **EFT protection**

[Nationwide Building Society](#), a U.K.-based bank, offers checking and savings accounts, credit card services, mortgages and insurance. With multiple access channels, Nationwide was concerned about the increasing danger of fraud. In addition, new regulations for faster payment established in 2008 meant that more transactions were occurring in real time, placing pressure on the bank to detect fraud equally quickly.

After looking at a variety of fraud detection and prevention products, Nationwide found that a series of products from [Actimize](#) best fit its needs. The speed and cross-channel analyses were the two features that Nationwide

found most compelling. The bank phased in various components of the Actimize solution, which detects fraud in cross-channel remote banking, commercial and retail electronic payments, deposits and ATM/debit cards. In addition, it has a component aimed at employee fraud.

The remote banking solution was the first to be implemented, and it resulted in a 90 percent decrease in online fraud. Attempts at fraud decreased as would-be fraudsters found the bank to have improved defenses. Transactions are monitored in real time, and suspicious activities are scored as high risk. The Actimize software can block such transactions immediately.

As the speed of banking transactions has increased, so has the importance of real-time detection. A top-five U.S. bank is using several products from [Actimize](#) to detect wire fraud and automated clearinghouse (ACH) fraud. The applications use data from the wire instruction to avert attempted wire fraud transactions, so that the fraud is prevented before the funds ever leave the bank.

About 73 percent of fraud attempts were detected prior to the completion of the wire transfer. In addition, real-time false positive ratios tend to be quite high, around 1:50, meaning out of 50

potential fraudulent transactions, one is a real fraud. With Actimize, the ratio is 1:15. Those are occurring in low-fraud environments where there are few attacks, so reducing the ratios to that extent is quite significant.

### **More vulnerable**

The changing nature of banking has led to more opportunities for fraud.

“Customers can now move money in many different ways,” says Paul Heninger, VP of products for Actimize. “They can make electronic fund transfers to many more payees than in the past, transfer from one account to another and wire money domestically and internationally.” The global nature of today’s banking also has had an impact. “A decade ago, a criminal had to be in the city where the bank was located to steal from it,” Heninger says, “but now he can be anywhere in the world.”

Similarly, the number of bank employees who can access the accounts has increased. “With the convenience of pervasive customer service has come additional vulnerability,” cautions Heninger. “And while the great majority of employees are honest, the ones who are not can harm the bank and its customers.” Collusive fraud, in which individuals coordinate to cover each

other’s actions, can have an even more significant impact.

Emerging technologies such as smartphones have opened new doors for fraud. In January, Google withdrew 50 apps for its Android smartphone from its online market, out of concern that they might be malicious. They were “phishing” apps designed to obtain banking information from Android users. Most large banks now offer their customers the option of conducting bank transactions via their mobile phones, making that an emerging market for fraud.

### **Small financial services companies get boost from document management**

[JFS Wealth Advisors](#) provides a comprehensive range of financial services, including personal wealth management, business retirement management, institutional consulting, and tax planning and return preparation services. With 32 employees, it is one of the largest, independent, fee-based wealth advisors in the country. Several years ago, the paper files required by JFS had begun to exceed the capacity of its file cabinets and storage area, so the company began planning the move to go paperless.

After talking with colleagues in the field and carrying out its own research, JFS selected CNG-SAFE from [Cabinet NG](#). “We liked the file cabinet metaphor,” says Laura Blaire, chief operating officer for JFS, “because it could mirror our existing organization and looked familiar to our staff.”

The company took a careful approach to setting up the application in order to be confident that the interface and templates matched its needs. “We wanted to have a consistent system for organizing our data that offered the ability to create well-defined templates,” Blaire explains. “In addition, we reviewed and organized each file folder to ensure our scanning efforts were as efficient as possible and that we did not scan unnecessary documents.”

### **Easier to comply**

Now that the information is stored electronically, access is greatly improved and meeting compliance requirements is easier. “We really like the search

function, and having the system in place has made us more disciplined about how we save things,” notes Blaire. “In addition, when the SEC requests a document, we can easily copy it to a folder for them.” CNG-SAFE facilitates the backup and data security of those documents, which is essential for effective compliance.

James True, VP of business development at CNG, says, “In some cases, smaller financial services companies have hesitated in moving to a paperless environment because of concerns about compliance. Many of them do not have an IT department and, therefore, may lack the resources to implement a document management solution. We give the customer the option of a local client/server or hosted/SaaS configuration, and the hosted model from CNG addresses that concern.” In addition, a new CNG-Online version of CNG-SAFE automates the backup and retention functions of document management.

Posted July 3, 2010:

<http://www.kmworld.com/Articles/PrintArticle.aspx?ArticleID=68146>