

# Safe From Prying Eyes

Employee-monitoring systems protect customer information, from the inside out

By Lauri Giesen

**T**rust: It's one of the most important words that a customer can use to describe his or her relationship with a bank. Community banks have found that consumers want to be able to trust that their bank will protect vital information related to their identity—even from bank employees.

For most community banks, the ability to protect customers from identity theft requires a combination of policies to outline acceptable and unacceptable employee behavior, and technology to monitor employee activities and detect potential violations.

“There is a lot community banks can do today to protect their customers,” says George Tubin, research director of delivery channels and financial information security for the consulting firm TowerGroup Inc. in Needham, Mass. For example, banks can use technology-based detection systems to alert them if an employ-

ee's actions indicate something may be amiss, he says. “There has been a lot of activity by vendors to develop internal-monitoring systems that analyze the employee behavior to make sure that the

employees are making an appropriate use of customer data.”

Systems on the market today can detect, for example, if an employee is pulling up an unusually large number of customer accounts at one time or a small number of accounts on a basis that is more frequent than what should be required for his or her job. And monitoring systems can detect if employees are taking customer data outside a bank organization. Systems can also detect patterns of abuse with respect to customer data to help locate where a breach may have occurred.

Once a bank has been alerted to potential problems, the systems guide bank personnel in conducting the proper investigation by providing the necessary documentation. But while the use of the latest technology may be important, it cannot be used as a substitute for careful vigilance within the bank. Community banks must have clear policies of what behavior is appropriate and let employees know they won't tolerate any violations, bank security experts say.

Once those policies have been established, there are specific types of systems that can be employed, each of which serves a unique purpose, says Avivah Litan, vice president for consulting firm Gartner Inc. in Stamford, Conn. “There are a number of systems in the market that specialize in preventing internal fraud, and most are effective at





## ID Theft Prevention Options

In the banking industry, there are five specific types of systems employed to help banks detect and root out fraud, according to Gartner Inc. Here is a brief description of the purpose of, and recommended use for, each of these five user-monitoring approaches:

- 1. Database Activity Monitoring** helps maintain the separation of duties for users who have privileged database activities by monitoring administrator activity. This system is useful in overseeing database administration activity and database access, especially when native database auditing is not enabled.
- 2. Content Monitoring and Filtering** uses a variety of linguistic and data analysis technologies to monitor the use of sensitive content and enforce policies. Use this system to detect and prevent inappropriate movement of sensitive data across the network.
- 3. Network Behavior Analysis** provides transparency in network operations based on traffic flows between systems. Use this system to monitor network traffic flows between applications, and to discover anomalous traffic and associate it with a specific user.
- 4. Fraud Detection** involves the real-time analysis of activities by users against customer accounts. It is best used as a means to monitor or stop suspect user activity at the access or transaction layer.
- 5. Security Information and Event Management** supports threat management and security incident response through the collection and analysis of security events from a variety of data sources. It is typically deployed for such things as monitoring external threats, monitoring the activities of privileged users, and monitoring activities of a user across multiple systems and applications.

doing so, assuming the bank has done its part in establishing good business practices to begin with,” Litan says.

### Record and Playback

One company that provides monitoring systems is Raytheon Oakley Systems in Salt Lake City. “Our system works a lot like TiVo in that it watches everything it has been told to watch and can provide a record of activities,” says Tom Bennett, vice president of marketing. “Later, a bank can play back what we have recorded and see exactly what an employee has done as it happens.”

What that means is that a bank can spell out what types of activities it wants flagged: an employee calling up a large number of files; an employee e-mailing data

to his or her home or to a third party; or an employee transferring files to a USB port. Once an employee’s behavior is flagged, the system responds by recording that employee’s activities from five minutes prior to the incident to five minutes after.

The bank can see exactly what happened as it happens, Bennett maintains. “[It] might notice that the employee got an e-mail from an outside party requesting [that] certain information be e-mailed out of the bank, or note that the employee got a call, a few minutes before [a breach], from home telling [him] that there has been an accident and [that he] needs to come home right away,” Bennett says.

The latter may be an example of an accidental policy violation

(as opposed to intentional fraud). Other common accidental violations involve employees taking data home with the intention of working remotely. The problem with such violations is that once data leaves the security of the bank, it could be lost or violated, even without the intention of the employee to commit fraud. Either way, banks need to know that a rule has been violated, Bennett says.

Oakley Systems, another internal-monitoring systems provider, offers a “pre-built policy” option for banks that do not have a written policy that can be adopted and adapted to fit their internal requirements. For example, some banks might only flag an employee that has pulled up 100 or more customer

files. Another bank may decide that 10 is too many. A bank may also provide key words or phrases that it wants the system to look for in employee e-mails and flag messages that contain those words. The system can also be adjusted to fit the security level and responsibilities of individual employees, Bennett says.

Another company that has developed an employee-monitoring system is NetEconomy, a division of Fiserv Inc. in Milwaukee, Wis.

Like the Oakley Systems software, NetEconomy's model analyzes employees' interaction with customer information and flags questionable actions for

bank security personnel to review. "We keep track of how employees are interacting with customer information," says Andrew Davies, general manager of NetEconomy. "You might have an employee who usually only looks at an account once a day who suddenly is calling up accounts with an increased frequency. That would be the starting point of an investigation."

In addition to flagging questionable interactions, the system captures information regarding the action for investigation.

### **Pattern of Misconduct**

Besides employee-monitoring systems, there are other types

of technology tools banks can use. San Diego-based ID Analytics, for example, has a system that looks at customer behavior to detect patterns that would indicate that bank information policies might have been violated. Once a violation occurs, the system can then analyze the patterns to pinpoint the origin of the breach.

The company's system might find, say, that 16 customers of a bank have all filed a credit application in the same month using the same cell phone or address. Those commonalities present a strong indication that something is amiss with those customers' identity

## “Our technology looks at patterns to determine if something is happening that would indicate there has been misuse of information.” – Mike Cook, ID fraud-prevention expert


data, explains Mike Cook, chief operating officer. “Our technology looks at patterns to determine if something is happening that would indicate there has been misuse of information,” he says.

Once ID Analytics finds a pattern, it can help determine if there are other common occurrences or activities among those customers in question in their relationship to the bank. For example, the system could determine whether the same 16 people all talked to the same call

center representative on a given day. The bank then knows where to investigate.

On its Web site, ID Analytics also provides free reports that show trends related to identity theft, which further aids banks and other companies seeking to prevent identity theft. On the site, banks can see, for example, which communities have recently experienced the biggest increases in identity theft.

So far, ID Analytics has only worked with larger banks, but Cook says his company is inter-

ested in a cooperative deal with community banks that could lower the cost to individual institutions. He notes the system is often used in conjunction with employee-monitoring systems. “There is other great technology out there that we do not compete with,” he says. “Any technology can be defaulted, but if you use several systems in conjunction, you can substantially limit your exposure.” 

---

*Lauri Giesen is a free-lance writer in Libertyville, Ill.*