

NEWS

# To Uncover Laundering Risks, Monitoring More than Employee E-mail May Be Essential

September 02, 2008 [By Matt Squire](#)    

After former Bank of New York vice president Lucy Edwards was convicted of helping her husband launder over \$7 billion from Russian banks, she had one piece of advice for the bank that ended up paying \$38 million in related penalties to U.S. regulators: the compliance department should've known what she was up to.

Keeping tabs on employees who might abuse sensitive information has long been a standard practice among financial institutions. But as communication applications have evolved, what compliance officers need to look for, and at, has changed as well.

"We are beginning to redefine our definition of what communications looks like, so we are not restricting what we are looking at to just e-mail," said Dan Regard, managing director of Intelligent Discovery Solutions in Washington D.C. To not do so, leaves financial institutions vulnerable to abuse by their more tech-sawy employees, he said.

Rogue employees no longer have to depend on phone calls and company e-mail to send sensitive data, and can turn to instant and text messaging, personal e-mail accounts and social networking services like Twitter and Facebook, said Regard.

But monitoring those channels is complicated by the fact that it is "very common for people in normal conversations to switch modes of communication almost seamlessly," he said.

When tracking employee e-mails, financial institutions rely largely on software systems that allow for keyword searches and track the destinations of e-mails that may be on an internal "hot list," said John Walsh, president of consulting firm Sight Span in Mooresville, North Carolina.

Like transaction monitoring software, e-mail monitoring systems detect patterns to discern if suspect employees are contacting questionable parties on a regular basis, said Walsh. "And if the number becomes unusually large, then an investigation is drilled down a little deeper," he said.

The same software, called "packet sniffers," can also be used to monitor other media for suspicious keywords and unusual patterns, though the systems may not have the sophistication to effectively monitor telephone calls for the same words.

Instead, phone systems "can be analyzed for traffic density, frequency and volume and with the right system you can correlate phone traffic with e-mail traffic and other communications traffic to establish a true communications pattern," said Regard.

Broadening how employees are monitored may mean snaring those who don't yet realize that

"if it's done on your work computer, it can be tracked," said Carmen Oveissi Field, a managing director with Daylight Forensic & Advisory in New York.

In one example, a client of Field's had an employee planning a "very serious criminal activity" through his instant messaging service at work in order to avoid being traced through his cell phone. "But little did he know that in a back room they had it projected onto a wall and were watching his communications fly by," said Field.

While most corporations have e-mail and network usage policies, larger multi-national institutions often fail to consistently apply those policies throughout the various lines of business, said Walsh. In some cases, policies differ depending on the risk level of each job slot, he said.

"The higher scrutiny goes with the higher the risk associated with the amount of money that somebody could embezzle or launder," said Walsh. "An investment banker would go under a lot more scrutiny... but it would be a reduced amount for a bank teller."

Because the improper storage and management of data in monitoring systems can lead to compliance headaches, banks need to have policies that allow easy search capabilities of time periods, keywords, origins and lines of business, said Walsh.

Data retention rules, however, vary for different types of transactions and communications and limits on how long an institution can retain the information ranges from one to seven years.

"Information related to whether your employee is shopping on eBay—there would be no logical reason for that information to be databased for five years," said Theresa Loscalzo, a partner with Schnader Harrison Segal & Lewis LLP in Philadelphia. "You might database that information for 30 days and on a separate server."

And banks can make the mistake of lumping all types of communications into a single category, resulting in greater time and cost to process the relevant information, said Loscalzo.

Ultimately, banks need to balance their employee monitoring efforts so that there they have thorough internal security without draconian oversight, said Field. "You have to find where you want to draw that line in your organization where people will still be effective but also not feel disrespected for constantly being watched," she said.

September 02, 2008

By [Matt Squire](#)



[Switch To Edit Site](#)