

# The BlackBerry: On the Air and Off The Record

By Carol E. Curtis, Compliance Editor

*June 13, 2005*

The Securities and Exchange Commission's Rule 17a-4 and the National Association of Securities Dealers' Rule 3110 require broker-dealers and exchange members to preserve all electronic communications pertaining to their firm's business, in a format that cannot be overwritten or erased, for three years. The Investment Advisers Act, meanwhile, specifies that records must be indexed, archived in duplicate and retained for up to six years.

"Funds and investment advisers should archive all e-mails containing information that is required to be kept," explains Gene Gohlke, associate director of the SEC's office of compliance inspections and examinations.

It sounds straightforward, if arduous. But when the SEC meted out over \$8 million in fines to financial firms that failed to archive employee e-mails back in 2002, it had yet to see the BlackBerry coming. That same year, the wireless handheld devices made by Research In Motion (RIM)--used mainly for sending and receiving e-mail messages over cellular networks--were just starting to show up in the securities industry. There are now some 3 million of them in the U.S., and while they are used by all types of businesses, they are heavily concentrated in the securities industry. "I don't think that you could find an investment firm whose brokers and traders don't have BlackBerries," says Mitchell Balsam, chief executive officer of CommonDesk LLC in New York.

## Versatile Gadget

The latest BlackBerry devices now support many other kinds of electronic communication in addition to e-mails managed by a central server, including peer-to-peer communication in which the personal ID number (PIN) of the other device can be called to set up a direct two-way radio channel, much like an ad hoc WiFi connection between laptop computers. They also support text messaging, voice communications, instant messaging and Web browsing, including access to Web-based e-mail. And in addition to access to corporate e-mail servers, many BlackBerry wireless carriers now provide a separate e-mail account, hosted by the carrier, for personal use.

"Of all these communication techniques, only e-mail can be captured by a company's e-mail compliance system," notes Balsam. "[Companies] thought they were safe because their IT department said that e-mails were being captured. But they forgot about the six other methods of communication. This is a trap door that has been left open in compliance. There are holes all over the place."

## Off the Radar

A former SEC official, now a lawyer in private practice, describes BlackBerry users as "a whole subculture of communication that falls under the radar of broker-dealer communications" and represents a serious risk. The "dirty little secret" of BlackBerries, he says, is that "there are communications with customers that are not captured, reviewed or archived."

A former options trader provides an example of the kind of problem this can present. Say an institutional desk trader is given a large block of stock to sell. Before the trade occurs, the trader sends a PIN message to the BlackBerry of a friend who speculates in this stock at another firm. His friend then buys put options before the large block trades, and sells them immediately when the block trade hits the market, as the value of the puts goes up.

"Since PIN messages can't be monitored by the company's e-mail compliance system, no one will know the front-running has occurred," says the source.

### **Fast-Moving Technology**

Many companies have already upgraded to the newer BlackBerry models with additional capabilities. The fast-growing technology presents a moving target: While instant messaging is currently an optional feature, for example, it will be preinstalled on future models.

Moreover, companies that feel they have the e-mail compliance problem under control may be in for a surprise. Some, for example, assume that disabling PIN and text messaging in the device's system software shuts down non-compliant channels. "The truth is that this only stops users from sending PIN or text messages," Balsam says. "It does not stop them from receiving PIN or text messages from people outside the company, who don't have [these capabilities] shut off. That could be a cell phone anywhere in the world."

Not surprisingly, a number of companies are rushing to market with potential solutions to the problem. CommonDesk, for example, has a product called PINcushion that Balsam says can capture most forms of BlackBerry messaging. It has two parts: a piece of software installed on the device that records and stores noncompliant messages, and a server located in a company's data center. The server receives message archives from all of the firm's BlackBerries and generates reports for the company's e-mail compliance system.

"Other companies are selling add-ons to existing BlackBerry utility packages," Balsam says. "Our product is focused on compliance only." Like its competitors, however, PINcushion is not a complete solution. If the company is using an older version of the operating system software, it cannot capture phone calls to or from a BlackBerry device, for example.

### **Other Solutions**

New Jersey tech shop AXS-One has been working on electronic archiving since 1993, but not even the current version of its AXS-One Compliance Platform is fully equipped to deal with the BlackBerry threat.

"Our solution addresses part of the issue," says Peter Mojica, AXS-One's vice president of product strategy and management. Like many solutions, AXS-One captures communications that pass through company gateways, but "there are still plenty of ways to bypass that," Mojica says. "When you are using a non-corporate BlackBerry, we are not going to capture that."

There are some tricks of the trade to be applied. BlackBerry text messages, for example, have the default signature "sent from my BlackBerry handheld," which many users don't bother to change. He advises clients to filter for the word "BlackBerry" on the theory that some communications may come back in through the corporate e-mail system, where it can be captured by systems like AXS-One's. Still, "It is basically a loophole within the industry," Mojica says.

According to Zantaz's Lambert, the best solution to dealing with PIN messages and personal BlackBerry e-mail accounts is simply to forbid them.

Orchestria, which assists large banks with communications compliance, uses an approach called active policy management (APM) that configures servers in a way that disallows any unauthorized uses. "We block [the communication] at the server," says Paul Johns, vice president of marketing at Orchestria. "It can be very specific. We are preventing the noncompliant communication from occurring. But we cannot do that with a PIN-to-PIN communication. And if it is a text message, we don't deal with them."

Johns says he knows of no vendor with technology that is able to block BlackBerry text messages at this point. So far, however, regulators have not asked for text messaging logs, but that doesn't mean that they won't once they catch on to the loophole.

A related approach is taken by the AtlasIPM suite, from PSS Systems of Mountain View, Calif. Its Policy Atlas component helps companies define their archiving policies; another tool, called Policy Point, is an agent that automatically enforces compliance on PCs and file servers.

"We do not have a BlackBerry-specific solution," confesses Deidre Paknad, president and CEO of PSS Systems. "The real option is to figure out a policy to retain what you need, and dispose of what you can. Now, we can filter messages, but cannot figure out which ones need to be kept. The challenge is the difference between, 'Honey, I won't be home until eight,' and 'I placed a sell order for you.'"

Another Silicon Valley firm, Zantaz, prides itself on "being best of breed for archiving in-policy communications," says Francis Lambert, senior technical adviser. But Zantaz's Enterprise Archive Solution, a product that archives and monitors e-mail communications, cannot account for messaging not passing through central servers. Says Lambert, "We do not focus on rogue wire capture"--a term that includes PIN messages and personal BlackBerry e-mail accounts. Lambert thinks the best solution to date is simply a policy forbidding such uses. "The best way to deal with it now is to prohibit and enforce," he says.

But with compliance technology moving ahead so rapidly, Lambert thinks that may change. "To monitor [these] communications requires an agent on the device, or you can monitor the backup file," he says. "It all comes down to this: Is there a profitable business to create this [technology], and then go out and market it?"