



# REAL ESTATE TECHNOLOGY NEWS

November 30, 2005 • [www.retechnologynews.com](http://www.retechnologynews.com)

## Florida MLS Adopts Token System to Improve Security

*Technology helps eliminate data leakage and deadbeats*

**F**lorida Realtor Kathleen Gallagher McIver long suspected there were security issues for the MLS serving her area; she found out up close and personal when she listed her home for sale.

“I don’t think anybody realized how many people were stealing our MLS information,” Gallagher McIver said — her included. After she listed her own home, she got a letter from a mortgage company that basically said, “We see you put your home on the market; we can help you finance your next one.”

“Obviously, someone had been feeding them our MLS information,” Gallagher McIver said. Worse, unauthorized users were getting rich while ripping off the information. “We went to a conference in February and heard stories of people making up to \$100,000 a year selling passwords to moving companies, mortgage companies, appraisers and others.”

That changed Sept. 19, when the Mid Florida Regional Multiple Listing Service (MFRMLS) went live with its LoginKey authentication system designed to restrict MLS information to paying customers. The system employs a token that fits on a keychain and displays a six-digit numeric pass code that changes randomly every 60 seconds. Users enter the pass code along with their personal identification number to sign onto the MLS.

Because users provide something they know — their PIN — and something they have — the token’s random pass code — the system ensures data is available only to authorized users. RSA calls it a two-factor authentication solution.

For the next three weeks, more than 20,000 RSA SecurID tokens from RSA Security were distributed to MFRMLS subscribers, which include the Orlando Regional Realtor Association, Bartow Board of Realtors, the East Polk, Greater Lake and Osceola county associations of Realtors and the Greater Tampa, Lakeland and West Volusia associations of Realtors. It was a first for MLSs and “the largest single-stage deployment in the history of the information security industry,” RSA said.

### Deadbeats and data leakage

Before starting the project, MFRMLS’s biggest security concerns were unauthorized (unpaid) system users and data leakage, according to Belton

*Compliments of:*





Jennings, CEO of the Orlando Regional Realtor Association and MFRMLS corporate secretary. The latter — data leakage — means MLS members were their own worst enemies, giving their access codes to others. Realtors most often did that, it's thought, so that clients could search for properties on their own. Others were appraisers and mortgage and title companies, Jennings said.

To the uninitiated, information on an MLS might seem mundane, but it could be the mother lode for burglars and others bent on nefarious deeds. Each listing contains marketing remarks, instructions, directions or special considerations intended only for professionals showing the property. It could have data ranging from instructions on handling family pets to information about an elderly parent home alone and information about the security system. However, putting security access codes in the database is forbidden; buyer's agents must contact the listing agent to arrange access.

"While much of this information may seem innocuous, let's just say it could be pieced together to provide someone with perhaps more than they need to know — sellers' names, telephone numbers, lifestyles, work habits, etc.," Jennings said.

Gallagher McIver, vice president and sales manager of RE/MAX Town & Country Realty and 2004 President of MFRMLS, called the RSA SecurID project "my baby" and earned an Orlando Realtor Group volunteer award for helping birth it.

She remembers another pre-SecurID incident.

"An agent gave the password to a customer, and the customer gave it to someone else. It just kept getting passed around until finally, somebody had a problem with accessing the MLS and called MLS help desk." Needless to say, the password was terminated.

"We (authorized users) have no trouble getting into the system," she said. The first week in operation was like a university Rush Week, Gallagher McIver said. But overall, things went pretty well.

In addition, membership in the MLS has gone up, which is driving revenue.

"We have 160 new appraiser members in Orlando," she said. "They need it to do appraisal reports for banks. Before, they were basically using our information and not paying for it." By choosing RSA Security technology, MFRMLS expects to save more than \$1 million over three years, compared to competitive solutions.

### **Remember HIPAA?**

Jennings noted that Florida has enacted laws protecting the privacy of personal information. However, there are no specific laws pertaining to multiple listing service-type databases.

"That said, we are aware that the protection of personal information is fast becoming the target of legislation both at the state and federal level," he said.

An example is the recent Health Insurance Portability and Accountability Act (HIPAA), which protects patient healthcare information. MFRMLS wanted to be proactive in applying these types of measures to the real estate business.



“Our organization’s leaders felt it best to get ahead of the curve and act now to place more stringent controls on the security of our MLS database,” he said.

Asked if he thought lenders and settlement service providers would take similar steps to protect data, Jennings said, “Those from outside who’ve looked at this entire industry from a data security standpoint have expressed real concern about the methods in which personal information about buyers and sellers is collected and distributed among all the ‘players’ in a transaction — from brokers to title companies to mortgage companies, home inspectors, termite companies, etc.

“Absent any agreed-upon industry-wide data security protocols, we must rely on the policies, procedures and practices of the individual companies to provide this protection. As one might imagine, other than the large national companies, this protection can be spotty at best.”

### **Expect more MLSs to sign on**

He said the National Association of Realtors is making a concerted push at the national level to increase the awareness of its members and allied industry partners about data security.

“MFRMLS is one of the first organizations to actually take affirmative steps to better protect its data. Based on the number of inquiries we’ve received from other MLSs across the nation, many others are contemplating instituting similar programs,” Jennings said.

Gallagher McIver agreed.

“You’re going to see a lot more MLSs adopt it,” she said.

MFRMLS anticipates the MLS LoginKey system will eventually be used by its subscribers to access several other local real estate applications and services.

In the 2005 MLS Technology Survey from NAR’s Center for Realtor Technology, 76 percent of MLSs and Realtors indicated that data and system security is a concern for their organization (see chart below).

MFRMLS also recently renewed its partnership with Interealty, recently acquired by First American (see the cover story in our Nov. 15 issue). The MLS signed a three-year contracts to use MLXchange, Interealty’s Web-based MLS automation technology. It licensed MLX Professional, providing its members with management tools such as customizable agent Web sites with client portal pages, Internet lead capture and calendaring and scheduling.