

SPECIAL REPORT: MORTGAGE SERVICING

Loan Protector Emphasizes Data Security

Mortgage servicers and their vendors have placed a strong emphasis on data security within their internal systems recently, but as some high-profile cases have illustrated, data security may be most at risk when loan information is in transport.

Ron Wiser, president of Loan Protector Insurance Services, says that some people in the industry may be a little too casual about transporting spreadsheets with loan information, for example.

"People seem to be somewhat casual about sending attachments on e-mail," he told *National Mortgage News*. "All attachments with any possible protected information ought to be sent in some type of encrypted fashion."

While this may be inconvenient at times, he said it's worth reiterating the importance of data security, especially with the heightened regulatory scrutiny about identity theft. Attachments with sensitive information should be password protected or electronically locked, he believes. Companies often find it difficult for management to enforce e-mail rules or police employees

One way to cross that hurdle is to use a secure, Web-based interface for accessing data that is used by multiple parties. Loan Protector gives clients access to information via the Web that is under cen-



RON WISER, president of Loan Protector Insurance Services, said people are "somewhat casual" about e-mailing attachments with sensitive information.

tralized control, with security built into the communications link.

Steve Wiser, head of Loan Protector's affiliate that develops software, said that client certificates can be used to limit access to sensitive data. The client-based certificates let the server know that the user is who they say they are. Essentially, the certificate technology allows the Loan Protector server to authenticate the user before letting them advance to the login screen. And because the certificates are stored on the client's

office machines, it prevents employees from making unauthorized access from other machines, such as home computers.

"There's a kind of like an understanding that has to be made between lender and outsourcer, because we do store a lot of data that has to be protected and especially has to be protected when it is in transit," he said.

Data encryption can be used to thwart "eavesdropping" on a Web access system. A further level of protection is provided by authentication technology that limits access. Those authentication certificates essentially "lock down" access from unauthorized machines. Steve Wiser said some large banking institutions are using authentication certificates for their internal users already.