

Wells Installs Security Software from Bharosa

Wednesday, August 30, 2006

By [Will Wade](#)

Wells Fargo & Co. said it has improved its online banking security by installing software from Bharosa Inc. that analyzes customers' computers to ensure that people are using known machines.

The San Francisco banking company announced the installation Monday and said that the Bharosa technology is part of a multilayered security strategy.

Jim Smith, Wells Fargo's executive vice president for consumer Internet channel and products, said in an interview that no single application is adequate to protect customers from the myriad online scams that are common today.

In April his company began business customers passcode-generating tokens from RSA Security Inc. Last year Wells began using transaction monitoring software from Actimize Inc.

Mr. Smith said he expects to implement additional security measures. "This is an ongoing process."

Though he said the multilayered security strategy is aimed primarily at protecting customers, he also said that Wells is complying with guidelines issued in October by the Federal Financial Institutions Examination Council requiring banks to boost their online security.

Many companies interpreted the guidelines as requiring multifactor authentication, but the agency published a list of frequently asked questions this month to clarify its requirements. It said that a layered approach that uses several security applications "may be an effective method to mitigate risk."

Multifactor authentication requires customers to provide information in addition to a standard username and password to get access to a site, but it also makes the login process longer. Mr. Smith said that Wells wanted to avoid "having something visible to customers, that gets in the way" when they log in to its Web site.

John Fisher, the chief executive of Bharosa, said its technology works behind the scenes during the login process. It puts a file on customers' computers when they access the site, then looks for the file and replaces it with a new one the next time they visit.

The Santa Clara, Calif., vendor also uses geolocation data from Quova Inc. to identify the location of a user's computer and evaluate its IP address. This can provide a warning sign for fraud.

"We authenticate the user by looking at the device," Mr. Fisher said.