

FFIEC guidelines require us to conform to multi-level authentication methods by the end of this year in regards to our Internet Banking. In response to this, we have established dual authentication methods for our E-Banking customers. Per an earlier target notification, titled Logon Security Enhancements, you have been made aware of the necessity for increased security precautions and enhanced authentication methods for logging on to your E-Banking service.

Due to the need for this conformance, the OCC (Comptroller of the Currency) anticipates increased activity by fraudsters to exploit the FFIEC's December 3, 2006 deadline. The OCC believes communications alleging to be from a customer's bank could inform customers that, due to FFIEC guidance, the bank is required to change its security procedures, and as a result, request customers to re-register or provide personal information that would enable the bank to comply with the regulatory requirement. These attempts may ask for information such as, your social security number, account numbers, passwords, validation questions and answers.

The OCC suspects that "phishing" attempts may use or include the FFIEC logo and may even contain or provide a link to the interagency guidance. Methods used by fraudsters to communicate with customers may include e-mail, telephone calls, and postal mail. Sophisticated schemes may employ multiple methods to "convince" the customer of their legitimacy.

Once again, I would like to stress, **The Bank of New Madrid will never contact you by e-mail, by phone, or by mail requesting your personal information.** Before you ever divulge any of your personal information, verify it is a legitimate organization or person you are speaking with. A way of doing this would be to ask for a phone number and tell them you will call them back. If you receive any correspondence claiming to be from the Bank of New Madrid, and you are unsure of the validity, call us here at 573-748-5551 or toll free at 1-800-530-5515 for verification before responding.

If you have not already done so, please check out the Customer Education tab under our website for more beneficial information regarding "phishing" schemes, fraudulent activity and card skimming.

If you have any questions or concerns regarding this notification, please call the Bank of New Madrid at one of the numbers listed above.