April 17, 2006

Suzanne Turner, Compliance Manager
Redstone Federal Credit Union
220 Wynn Drive
Huntsville, AL 35893

Re: Components of Security Response Program.

Dear Ms. Turner:

You recently contacted an NCUA regional office with questions about a security response program and the regional office has forwarded your request to the Office of General Counsel for a response. You have asked if a federally insured credit union must notify the NCUA every time it experiences an incident involving a possible breach of security affecting sensitive member information, regardless of the severity of the incident. NCUA's rule and guidance accompanying the rule in an appendix call for credit unions to conduct a risk-based evaluation of security breaches but do not require notice to NCUA in every instance. 12 C.F.R. Part 748 & Appendix B. You have also asked related questions concerning the form, content, and timing of notices to the agency, which we address below.

You are seeking guidance about your credit union's obligation to notify NCUA of matters involving potential breaches of the security or integrity of sensitive member information. You have described several hypothetical examples in which sensitive member information is involved, ranging from a teller's inadvertent placing of a receipt in the wrong tube at your drive-through facility to an unsuccessful attempt by a computer hacker to gain entry into your system.

The overriding theme of NCUA's guidance to credit unions in this area is risk assessment. When an incident occurs, the first step of any response program should be to assess the nature and scope of the incident and the likelihood of harm to the member whose information is affected. 12 C.F.R. Part 748, Appendix B, §II(A)(1)(a). Where an incident, even one involving sensitive member information, involves little or no likelihood of harm to the member, a credit union need not notify the NCUA.

You have also asked about the form and content of the required notice to NCUA. Our rule and the guidance do not prescribe a specific form or content for notices but credit unions should use a form of notice that is reasonably likely to be

effective. We recommend a form of notice the credit union can document such as letter, email, or fax. If a credit union believes speed is of the essence in notifying NCUA and the credit union provides notice by telephone, we recommend the credit union confirm a telephone contact in some written form. The content of the notice will depend on the circumstances and credit unions should use good judgment in providing sufficient information so the agency can appreciate the nature of incident.

Your final question asks about the period of time that should be covered in a notice. If you are asking about the timing for providing notice to NCUA, the guidance calls for credit unions to notify the NCUA "as soon as possible" after the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information. 12 C.F.R. Part 748, Appendix B, §II(A)(1)(b). If you are asking about the length of time NCUA will consider the notice to cover, we think it important to first understand the concept underlying the notice requirement. NCUA expects to be notified about each discrete incident involving unauthorized access to or use of sensitive member information. Id. The notice does not cover a specific period of time, but rather a specific incident. A separate notice should be provided for each separate incident. In this respect, credit unions should consider providing a follow-up notice to keep NCUA apprised of significant new circumstances relating to a specific incident previously reported.

We hope you find this guidance helpful but, if you have further questions, please feel free to contact Staff Attorney Ross Kendall or me at 703/518-6540.

Sincerely,

/S/

Sheila A. Albin
Associate General Counsel

GC/RPK:bhs
06-0332
Cc: Region III