JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
OFFICE OF FINANCIAL AND INSURANCE SERVICES
DEPARTMENT OF LABOR & ECONOMIC GROWTH
DAVID C. HOLLISTER, DIRECTOR

LINDA A. WATTERS
COMMISSIONER

DATE: January 5, 2005

LETTER NO: 2005-CU-01

TO: The Board of Directors and Management of Michigan State-Chartered Credit Unions

SUBJECT: Gramm-Leach-Bliley Act of 1999 (GLBA)

Purpose of this Letter

OFIS examination findings consistently cite partial compliance or non-compliance with the financial privacy and safeguard requirements of GLBA. This letter is to reaffirm that all Michigan chartered credit unions are required to comply with GLBA, and to clarify compliance requirements.

Background

GLBA, also known as the Financial Modernization Act of 1999, includes provisions to protect consumers' personal financial information held by financial institutions. OFIS and NCUA issued guidelines to credit unions to assist in understanding and implementing what is expected for GLBA compliance. Specific reference resources are included in the ***conclusion*** statement of this letter.

Guidelines

Management, from the Board of Directors down, should approach GLBA compliance with a logical process including a thorough ***risk assessment***, and a ***comprehensive program*** to address identified risk. This approach should include security of systems and resident data, regardless of size and complexity of the information technology (IT) infrastructure.

Risk Assessment Program:

The risk assessment program should focus on securing member information in the electronic marketplace. Management must identify and evaluate internal and external threats based upon the types of systems and services provided. For each system and service, the risk or threat should be described, prioritized as high/medium/low, and characterized by risk probability. Mitigating controls should then be identified. In summary, the risk assessment program should:

- Identify services and systems provided (hardware and software).
- Identify the risks associated with each system and service.
- Determine the likelihood of risk.
- Identify and evaluate methods to mitigate risk.
- Develop policies and procedures to address identified risk.
- Include training and education of staff.
- Review, monitor and adjust policies and procedures regularly.

Comprehensive Information Security Program (CISP):
After completing a risk assessment, management must develop a CISP, which should address:

- Board of Director's oversight and assignment of responsibility.
- Program adjustments in light of strategic or technology changes.
- Monitoring procedures.
- Access controls and restrictions to systems and workstations.
- Physical security.
- Internal and/or external security assessments to regularly verify network security posture.
- Remote access procedures and controls.
- Virus protection standards.
- Encryption standards for electronically transmitted or stored member data.
- Backup and recovery procedures.
- Vendor oversight program.

Conclusion
During future regulatory examinations, a Document of Resolution (DOR) will be issued for non-compliance with GLBA issues addressed in this letter. The Board of Directors is responsible for the information security program, and should approve all aspects of the program.

Please refer to the following resources:

- FDIC's Financial Institution Letter-68-99, titled *'Risk Assessment Tools and Practices for Information Systems Security' (July 7, 1999)*
- NCUA Rules and Regulations *Part 748*
- OFIS's Credit Union Letter No. 2001-CU-04 titled *'Comprehensive Information Security Program'*
- *'Interagency Guidelines on Safeguarding Member Information'*, available via FDIC website
- FDIC's Financial Institution Letter-22-01, titled *'Security Standards for Customer Information' (3-14-01)* FDIC Rules and Regulations – Part 364 – Appendix B, Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

Sincerely,

Roger W. Little, Deputy Commissioner
Credit Union Division