STATE OF INDIANA

DEPARTMENT OF FINANCIAL INSTITUTIONS

30 South Meridian Street, Suite 300
Indianapolis, Indiana 46204-2759
Telephone: (317) 232-3955
FAX; (317) 232-7655
WEBSITE http://www.in.gov/dfi

To: All Indiana State-Chartered Financial Institutions

From: Nicole Buskill, General Counsel

Date: December 12, 2018

Re: Disclosure Requirements for Security Breaches

The Indiana Department of Financial Institutions is issuing this advisory notification to Indiana state-chartered financial institutions in an effort to highlight the required data breach notification reporting procedures. Unfortunately, data breaches have become all too common in today's current environment and there is oftentimes confusion as to the statutory and regulatory framework surrounding data breach notifications. While Indiana Code Title 28 does not specifically address data breach notification requirements, there are separate state law requirements that are enforced by the Office of the Indiana Attorney General, including reporting, under the Security Breach Act in I.C. § 24-4.9 (which references financial institutions defined by I.C. § 28-1-1-3).

I.C. § 24-4.9-3-4 requires that a database owner report breaches to the Indiana Attorney General. However, it also provides an exception if a financial institution complies with the disclosure requirements prescribed by the 2005 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the 2005 NCUA Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (Appendix B to Part 748), as applicable. If a financial institution complies with such guidance, it is exempt from the requirement to report the breach to the Attorney General's office.

However, reporting requirements do not necessarily stop there. Please see below for reporting requirements that may be applicable to your financial institution.

Financial Institutions with FDIC Insurance

If a financial institution has FDIC insurance, federal law requires that it adhere to the Interagency Guidelines Establishing Information Security Standards ("FDIC Guidelines"). The FDIC Guidelines provide standards pursuant to section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831 p –1, and sections 501 and 505(b), 15 U.S.C. 6801 and 6805(b), of the Gramm-

Leach-Bliley Act. FDIC insured financial institutions, regardless of charter, are encouraged to review these standards and to direct any questions regarding the same to their primary federal regulator.

The FDIC Guidelines do not place an affirmative requirement that a financial institution notify the state regulator when an incident involving unauthorized access to or use of sensitive customer information occurs; however, the DFI requests that as a courtesy, that the financial institution notify the DFI Deputy Director of Depository Institutions as soon as it becomes aware of an incident involving unauthorized access to or use of sensitive customer information.

Financial Institutions with NCUA Insurance

If a financial institution has NCUA insurance it is required to adhere to NCUA regulations, including its reporting requirements. The Gramm-Leach Bliley Act requires the NCUA Board to establish appropriate standards for federally insured credit unions relating to administrative, technical and physical safeguards for member records and information. The NCUA Guidelines provide standards pursuant to Part 748 of NCUA's Rules and Regulations. NCUA insured credit unions, regardless of charter, are encouraged to review these standards and to direct any questions regarding the NCUA Guidelines to the NCUA.

In part, NCUA regulations require that the credit union have a response procedure that includes notifying the appropriate NCUA Regional Director, and the credit union's state supervisory authority as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information. If an incident occurs, please notify the DFI's Deputy Director of Depository Institutions as soon as the credit union becomes aware in accordance with NCUA regulations.

Credit Unions with Private Insurance or Those Institutions That Do Not Have Programs Consistent with Either FDIC or NCUA Guidelines

Privately insured credit unions are strongly encouraged to review the 2005 Interagency Guidance and implement programs consistent with the issuance. If there are any financial institutions that do not follow the 2005 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the NCUA Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, they are required to comply with I.C. § 24-4.9-3. In addition to notifying the Indiana Attorney General pursuant to I.C. § 24-4.9-3-4, the DFI requests that the entity notify the DFI of the incident involving access to or use of sensitive customer information.

If you have any questions please contact either Chris Dietz, Deputy Director of Depository Institutions at cdietz@dfi.in.gov, or DFI General Counsel, Nicole Buskill at nbuskill@dfi.in.gov.