STATE OF NEBRASKA

DEPARTMENT OF INSURANCE
Bruce R. Ramge
Director

July 28, 2015
CB-134

Pete Ricketts
Governor

BULLETIN

SUBJECT: INFORMATION SECURITY PROGRAMS

The purpose of this bulletin is to remind companies of the requirements of Chapter 77 of 210 Neb. Admin. Code, "Standards for Safeguarding Consumer Information." Additionally, it is to establish the expectations that the Nebraska Department of Insurance has regarding compliance with Chapter 77.

Chapter 77 was promulgated under the authority vested in the Director of Insurance by Neb. Rev. Stat. § 44-924(2), which is a subsection of the Nebraska Privacy of Insurance Consumer Act, Neb. Rev. Stat. § 44-901 *et. seq.* The Act was adopted in response to the federal Gramm-Leach-Bliley Act, which in part allows state insurance regulators to establish appropriate standards for insurance companies relating to administrative, technical, and physical safeguards. The Gramm–Leach–Bliley Act at 15 U.S.C. § 6801(b)(2) states that these safeguards should ensure the security and confidentiality of customer records and information, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. A copy of Chapter 77 can be found on the Department's website at **www.doi.nebraska.gov/legal/rule_reg/n77draft.pdf**.

Requirements of the Rule

Chapter 77 applies to all licensed insurers, fraternal benefit societies, producers, and other licensees (hereinafter 'licensees') of the Department with limited exceptions. The rule requires all licensees to implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of consumer information. The written information security program shall:

1) Ensure the security and confidentiality of customer information;
2) Protect against any anticipated threats or hazards to the security or integrity of the information; and
3) Protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any customer.

Chapter 77 contains four minimum actions and procedures to implement an information security program. The Department views the following four steps as important to a proper information security program; however, a licensee should not limit its efforts to these four examples.

941 O Street, Suite 400 • PO Box 82089 • Lincoln, Nebraska 68501-2089
Phone (402) 471-2201 • Facsimile (402) 471-4610 • Website *http://www.doi.nebraska.gov*
An Equal Opportunity Employer

1) **Assess Risk:** Licensees should identify reasonably foreseeable internal and external threats, to assess the likelihood and potential risk of these threats, and assess the safeguards in place to mitigate risks. In a licensee's risk assessment, to the extent that such knowledge is either public or known to the licensee, the Department expects licensees to be knowledgeable regarding the cause, damage, and response of breaches that have occurred at other licensees.

2) **Manage and Control Risk:** Licensees should design their information security programs to control identified risks, train staff as appropriate to implement their information security program, and to regularly test key controls, systems and procedures of their information security programs. To prevent licensees from falling into predictable patterns in testing the security of the information technology systems, the Department suggests licensees should occasionally alter their use of contractors and other testers, as appropriate to the size and complexity of the licensee.

3) **Oversee Service Provider Arrangements:** Licensees should use due diligence in selecting service providers and overseeing service providers to ensure that appropriate security measures are being utilized to secure the licensees' data. If a licensee utilizes a service provider, which is a person that maintains, processes, or otherwise has access to customer information through a provision of services of the licensee, and a breach occurs, the licensee and service provider shall coordinate to ensure compliance with all applicable law, including breach notifications.

4) **Adjust the Program:** Licensees should monitor, evaluate and adjust their information security programs to meet any changing circumstances outlined in Chapter 77. Such circumstances include the licensee's own changing business practices, most notably mergers and acquisitions. The Department expects that during mergers and acquisitions and when integrating new customer information systems, licensees will fully assess the risks associated with the new information systems.

Enforcement of Chapter 77

Information security programs will be reviewed during the financial examinations of domestic insurers and at any other time as directed by the Director for all licensees. Violations of Chapter 77 will be enforced through the Unfair Trade Practices Act, Neb. Rev. Stat. § 44-1522 *et. seq.*

Questions about this bulletin may be directed to Financial Examination Division at 402-471-2201.

Bruce R. Ramge

Bruce R. Ramge
Director