

Consumer Privacy Protections and Data Security

- *State insurance regulators have tools to aggressively protect the privacy of insurance consumers.*
- *State insurance regulators focus on both the security and confidentiality of consumers' non-public personal information and have worked through the NAIC to develop and implement privacy protections and data security safeguards.*
- *Any federal legislation addressing data security safeguards must be careful not to undermine or preempt state laws regulating the insurance industry.*

Background

The Gramm-Leach-Bliley Financial Modernization Act (GLBA) required federal financial agencies and state insurance regulators to establish appropriate standards for consumer privacy protection by the financial institutions they oversee. State insurance regulators, through the NAIC, have taken action to develop and implement safeguards to protect the security of consumer information.

The NAIC's *Standards for Safeguarding Customer Information Model Regulation* establishes standards that insurance entities must meet to be in compliance with GLBA's information security provisions. The model requires each insurance licensee to establish a comprehensive, written information security program that includes administrative, technical, and physical safeguards for the protection of customers' nonpublic personal information, appropriate to the size and complexity of the licensee and the nature and scope of its activities. The program may include provisions such as identifying reasonably foreseeable internal or external threats, assessing their likelihood and potential damage, training staff, regularly testing key controls, and exercising due diligence in selecting service providers.

As insurance companies place greater reliance on information technology (IT) systems, regulatory scrutiny of IT used by an insurer has become increasingly important. The NAIC *Financial Condition Examiners Handbook* requires an IT review as part of regulators' examination process and provides guidance for examiners to identify information security risks and evaluate the adequacy of controls and applicable risk management practices. Additionally, the NAIC *Market Regulation Handbook* requires a review of computer security procedures to ensure insurance entities have appropriate controls, safeguards and procedures for protecting the integrity of customer information. State insurance departments work with companies as needed to notify customers impacted by a data security breach.

Key Points

- State insurance regulators have worked to implement strong safeguards to protect the security, confidentiality, and integrity of customer information.
- The NAIC *Financial Examiner Handbook* and *Market Regulation Handbook* for regulators provide guidance on examining IT controls to help ensure that insurance entities are taking reasonable and necessary steps to protect consumers from theft or loss of personal information.
- Where criminal activity has taken place, state insurance departments work with law enforcement agencies to ensure those responsible for violating privacy laws are held accountable.