Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Missouri

Mo. Rev. Stat. § 407.1500

H.B. 62

Effective August 28, 2009

Application. Any individual, legal or commercial or government entity (collectively, Entity) that owns or licenses PI of residents of MO.

Security Breach Definition. Unauthorized access to and unauthorized acquisition of PI maintained in computerized form by an Entity that compromises the security, confidentiality, or integrity of the PI.

- Good-faith acquisition of PI by an Entity or that Entity's employee or agent for a legitimate purpose of that Entity is not a breach of security, provided that the PI is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the PI.

Notification Obligation. Any Entity to which the statute applies shall provide notice to the affected consumer that there has been a breach of security.

- Notification is not required if, after an appropriate investigation by the Entity or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the Entity determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for 5 years.

Notification of Consumer Reporting Agencies. In the event an Entity notifies more than 1,000 consumers at one time pursuant to this section, the Entity shall notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notice.

Attorney General Notification. In the event an Entity provides notice to more than 1,000 consumers at one time pursuant to this section, the Entity shall notify, without unreasonable delay, the state Attorney General's office of the timing, distribution, and content of the notice.

Third-Party Data Notification. Any Entity that maintains or possesses records or data containing PI of residents of MO that the Entity does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in this section.

Timing of Notification. The disclosure notification shall be made without unreasonable delay and consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government body;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information (information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional); or
- Health insurance information (an individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual).

PI does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.

Notice Required. Notice may be provided by one of the following methods:

- Written notice;
- Telephonic notice, if such contact is made directly with the affected consumers; or
- Electronic notice for those consumers for whom the person has a valid email address and who have agreed to receive communications electronically, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

The notice shall at minimum include a description of the following:

- The incident in general terms;
- The type of PI that was obtained as a result of the breach of security;
- A telephone number that the affected consumer may call for further information and assistance, if one exists;
- Contact information for consumer reporting agencies; and
- Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $100,000, or that the class of affected consumers to be notified exceeds 150,000, or that the Entity does not have sufficient contact information or consent, for only those affected consumers without sufficient contact information or consent, or that the Entity is unable to identify particular affected consumers, for only those unidentifiable consumers. Substitute notice shall consist of all the following:

- Email notice when the Entity has an email address for the affected consumer;
- Conspicuous posting of the notice or a link to the notice on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notice procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the Entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system.

Exception: Compliance with Other Laws.

- **Regulated Entity.** An Entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the Entity notifies affected consumers in accordance with the maintained procedures when a breach occurs.
- **Financial Institution.** A financial institution that is (i) subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance; or (ii) subject to and in compliance with the National Credit Union Administration regulations in 12 C.F.R. Part 748; or (iii) subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley Act shall be deemed to be in compliance with this section.

Penalties/Enforcement. The state Attorney General shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

Other Key Provisions:

- **Delay for Law Enforcement.** The notice required by this section may be delayed if a law enforcement agency informs the Entity that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the Entity documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the Entity its determination that notice will no longer impede the investigation or jeopardize national or homeland security.