

# PRIVACY & SECURITY BULLETIN

## Missouri Enacts Data Breach Notification Law

---

On July 9, 2009, with the Governor's signature of House Bill 62, Missouri became the 44<sup>th</sup> state to enact a data breach notification law. The law becomes effective on **August 28, 2009**. It requires all Missouri and out-of-state businesses that maintain personal information about Missouri residents in computerized form to notify affected individuals if the security protecting their personal information is breached, and the data is compromised. This Client Alert provides an overview of the new Missouri law, and offers some practical guidance for complying with the law.

### Who Must Comply

Missouri's data breach notification law applies broadly to two classes of businesses: (1) any person or entity that retains personal information (as defined below) of Missouri residents as part of its internal customer accounts, or for the purpose of conducting transactions with the individuals ("data owners"); and (2) any person or entity that maintains or possesses personal information of Missouri residents on behalf of a data owner ("service providers"). As with the laws of other states, the Missouri law applies not only to Missouri businesses, but also to out-of-state businesses that maintain personal information of Missouri residents.

### Scope of Missouri Law

**Personal Information Covered.** Missouri's breach notification law applies to any personal information of Missouri residents maintained in computerized form. "Personal information" is defined to mean an individual's first name (or first initial) and last name, combined with any one or more of the following data elements: social security number; driver's license number; government issued identification number; medical information; health insurance information; or account number plus security access code. An account number means any financial

account number, credit card number, debit card number, unique electronic identifier or routing code.

**Personal Information Not Covered.** Missouri's breach notification law does not apply to: (1) personal information maintained in paper or other non-computerized form; (2) personal information in computerized form that is appropriately encrypted, redacted, or otherwise altered to make the name or data elements unreadable or unusable; or (3) personal information that is lawfully obtained from government records made available to the general public, or from other publicly available sources. Missouri's rules for encryption and redaction differ from the rules implemented in other jurisdictions. For example, in Missouri a social security number may be redacted by shortening it to *any five* digits. Other states require truncation to the *last four* digits only, while some states do not specify any form of permissible redaction.

### Breach Notification Requirements

**Definition of Security Breach.** Missouri's law defines a "breach of security" or "breach" as unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the personal information. Good faith acquisition of personal information for legitimate business purposes does not constitute a breach, so long as the personal information is not used in violation of applicable law, or in a manner that harms or threatens the security, confidentiality or integrity of the personal information.

**Notifying Affected Individuals.** Subject to the exceptions discussed below, upon discovering or receiving notification of a breach (including notice from a service provider), a data owner must notify affected individuals *without*

*unreasonable delay*, consistent with any measures necessary to determine the scope of the breach, determine sufficient contact information, and restore the reasonable integrity, security and confidentiality of the system subject to the breach, and further subject to delay at the request of law enforcement (as discussed below).

**Notification by Service Providers.** A service provider that maintains or possesses personal information must notify the data owner (but not the affected individuals) *immediately* upon discovering a breach of security, subject only to delay at the request of law enforcement (as discussed below).

**Delay by Law Enforcement.** Notification may be delayed if (and only for so long as) providing notice may impede a criminal investigation or jeopardize national or homeland security. In order to be effective, the request must be made in writing by law enforcement, or documented in writing contemporaneously with the request by the delaying party.

**Notification Not Required.** Notification is not required to be provided to affected individuals if, after an appropriate investigation or consultation with law enforcement, it is determined that the risk of identity theft or other consumer fraud as the result of the breach is not reasonably likely to occur. Such determination must be documented in writing and maintained for five years.

**Contents and Form of Notice.** A breach notice must include: a general description of the incident; a description of the breached personal information; contact information for consumer reporting agencies; advice that directs affected individuals to remain vigilant by reviewing account statements and monitoring free credit reports; and, if one exists, a telephone number for affected individuals to call for further information and assistance. Notice may be delivered in writing, by e-mail (but only if the individual has provided a valid email address *and* agreed to receive communications electronically), or by telephone (but only if phone contact is made directly with the affected individual).

**Substitute Notice.** If the cost of providing notice would exceed \$100,000 *or* the number of affected individuals exceeds 150,000, then a business may provide substitute

notice by: (1) emailing the notice to all affected individuals with a valid email address (even if consent has not been obtained); (2) conspicuously posting the notice or a link to the notice on the company web site; *and* (3) providing notice to statewide media. Substitute notice also must be provided where any particular individuals affected by a breach cannot be identified, or cannot be contacted due to insufficient contact information or lack of email consent; however, standard notice still must be provided to all other affected individuals.

**Alternative Notice Under Internal Procedures.** A data owner that maintains its own breach notification procedures as part of an information security policy may use those procedures in lieu of those outlined in the Missouri law, so long as the timing is consistent with Missouri's notification requirements. This exception applies only to the content and form of delivery for the notice, and not to other aspects of the law, such as what constitutes a breach or the data elements that define personal information.

**Alternative Notice Under Federal or State Laws.** A data owner that maintains breach notification procedures in compliance with the laws, regulations or guidelines established by its primary federal or state regulator may notify affected individuals of a breach in accordance with those procedures in lieu of those outlined in the Missouri law. This exception applies to the content, form of delivery *and* timing for the notice, but does not affect other aspects of the law, such as what constitutes a breach or the data elements that define personal information.

**Notifying Attorney General and Consumer Reporting Agencies.** If the number of affected individuals receiving notice of a security breach exceeds 1,000, then in addition to notifying Missouri residents, the data owner must notify both the Missouri Attorney General's Office and all nationwide consumer-reporting agencies of the breach.

## Penalties for Non-Compliance

Under Missouri's breach notification law, the state Attorney General has exclusive authority to bring an action for damages suffered as the result of non-compliance. In

the event of a willful and knowing violation, the Attorney General may seek a civil penalty, not to exceed \$150,000 per breach or series of similar breaches discovered in a single investigation. The law does not provide Missouri residents with a private right of action.

## Practical Considerations

**Multi-Jurisdiction Breach Notification.** Missouri's breach notification law applies only to the personal information of Missouri residents. Commonly, a security breach affects data containing personal information of residents in multiple jurisdictions. In these situations, a business must comply with the Missouri law as it pertains to the personal information of Missouri residents, and look to other laws (including those of other U.S. states, Canada, and the European Union) for the breach notification requirements pertaining to non-Missouri residents. Missouri's law provides some leeway for adopting a single breach notification procedure that satisfies Missouri's requirements at the same time that it satisfies those of other federal and state regulators. However, other regulators may not provide similar reciprocity. Since breach notification requirements vary by jurisdiction, providing multi-jurisdiction notification can be a time-consuming and costly process, requiring careful advance planning.

**No Computer, No Name, No Problem?** On its face, Missouri's breach notification law protects a narrow set of personal information. Notice to Missouri residents is not required for breaches of non-computerized information, such as paper records obtained by dumpster diving or other illicit means. More curiously, Missouri's law defines personal information to include only a record that is combined with an individual's first name (or first initial) plus last name. If taken literally, this means that a breach of security involving the unauthorized acquisition of an individual's last name, address, phone number, financial, health and other personal information would *not* be subject to Missouri's law, if the record did not also include the individual's first name or initial. In practice, the Attorney General and/or courts confronted with this scenario may interpret the law more liberally, and require compliance even if the record set omits first or last names, where it is reasonably foreseeable

that the individual(s) could be readily identified from the remainder of the data set (e.g. via reverse look-up of phone number or physical address).

**Notice to All, Some or None?** In the event of a security breach, even if notice to some or all affected individuals is not required under applicable law, we recommend considering whether providing notice would be appropriate under prevailing industry norms. In the past, some companies have declined to provide notice of security breaches to some consumers on technical grounds. When news of these security breaches leaked (as it nearly always does), consumers were not sympathetic to the data owners' justification that they had technically complied with the law. Although providing notice of a data security breach can be costly, in a number of cases, this price may be less than the cost of concealing the breach. The potential fallout from a breach can be reduced further by providing notice that is concise and easy-to-read, describes both the incident and the response measures taken, offers a toll-free number or other means by which affected individuals can obtain information, and where appropriate, offers credit monitoring or similar services.

**End-to-End Encryption.** Missouri's breach notification law excludes encrypted personal information only if the data actually is acquired in encrypted form. Often, data is encrypted on a company's servers, but unencrypted when downloaded for use by employees on personal computers, transferred onto portable storage media, or transferred to service providers for data processing. As part of a company's overall information security policy, we recommend implementing an end-to-end encryption solution that protects personal information both in storage and while in transit, including on laptops, handheld computing devices, and portable storage media, and while in the possession of service providers.

**Financial Institutions Need Not Comply?** Missouri's breach notification law provides a specific exception for financial institutions that comply with Title V of the Gramm-Leach-Bliley Act (GLBA), or the regulations and guidance promulgated under GLBA by primary regulators. As written, the Missouri law suggests that a financial institution is

exempt from compliance even if the breach of security involves personal information about Missouri residents that is not “nonpublic personal information” as defined by GLBA. In practice, the Attorney General and/or courts may interpret this exception to cover only situations where a breach of security under the Missouri law involves personal information that also is protected under GLBA.

**Relationship to Information Security Program.** Despite companies’ best efforts to safeguard personal information, security breaches are less often a question of “if” than of “when”. The attention given to this issue by consumers, the media and government at all levels has raised the standard of care for all businesses that collect, process and maintain personal information. In addition to harming (or at the very least inconveniencing) affected individuals, a breach can result in significant out-of-pocket costs, diversion of resources, negative publicity, loss of customer goodwill, potential private or class action lawsuits, and regulatory investigation. For all of these reasons, we recommend that businesses develop an information security program with appropriate administrative, technical and physical controls designed to protect *all* forms of personal information, even if not expressly protected under Missouri or other law.

**Proposed Federal Breach Notification Law.** In recent years, several bills have been proposed in Congress that would replace the current patchwork of state breach notification laws with a new federal standard. However, these bills have stalled in committee in each of the past several legislative sessions.

## How Greensfelder Can Help

Greensfelder, Hemker & Gale’s Technology Transactions Practice Group advises clients on a range of intellectual property and technology matters, including information security and privacy compliance, equipment and software procurement, patent, copyright and trademark licensing,

and business and technology outsourcing. We routinely assist clients in preparing for and responding to data security breaches. We can work with you to develop internal policies and procedures that comply with Missouri and other applicable laws; establish appropriate contracts with service providers that handle personal information; and provide training to management and employees. In the event of a security breach, we can coordinate with your internal incident response team, and communicate on your behalf with law enforcement, the Attorney General’s Office, and other regulators. Finally, we can help you establish relationships with third party consultants that provide breach notification mailing, hotline staffing, credit monitoring, and related services, often at significantly reduced costs compared to the cost of handling these activities internally.

For additional information, please contact us:

**M. Spencer Garland, Manager**  
(314) 516-2613  
[msg@greensfelder.com](mailto:msg@greensfelder.com)

**Jason L. Ross**  
(314) 345-4754  
[jlr@greensfelder.com](mailto:jlr@greensfelder.com)

**Zachary L. Hammerman**  
(314) 345-4773  
[zlh@greensfelder.com](mailto:zlh@greensfelder.com)

Copyright 2009 Greensfelder, Hemker & Gale, P.C. This Client Alert has been prepared as general information for our clients and friends of the firm. It is not intended to be, and should not be construed as, legal advice with respect to any particular client, case or circumstance, and should not be acted on without advice of counsel. This material may be considered advertising under certain rules of professional conduct.