

Antitrust & US Trade Client Service Group

To: Our Clients and Friends

August 5, 2009

NEW DATA-SECURITY LAW BRINGS NEW DATA NOTIFICATION LAWS TO MISSOURI BUSINESSES, INCLUDING HEALTHCARE BUSINESSES

The Missouri governor recently signed into law House Bill 62, a part of which makes Missouri the 45th state to adopt a data breach notification statute. Although the notification requirements are similar to those in other states with such laws, the broad coverage of Missouri's statute, which goes into effect on August 28, 2009, is noteworthy for any company which does business in Missouri and/or with Missouri residents.

1. What Types of Information are Covered?

Missouri's law applies to any person or company, regardless of its size or nature of business, who has the personal information of a Missouri resident. Missouri's law defines "personal information" expansively to include:

- social security numbers;
- driver's license numbers or similar unique identification numbers created by a government body;
- financial account numbers (with a required security code, access code or password which would permit access to the account);
- credit card or debit card numbers (with a required security code, access code or password which would permit access to the account);
- unique electronic identifiers or routing codes (with a required security code, access code or password which would permit access to the account);
- medical information; and
- health insurance information.

Companies, especially those who do business in several states, should note that Missouri's law specifically includes healthcare-related information not always found in data breach notification laws.

This Client Bulletin is published for the clients and friends of Bryan Cave LLP. Information contained herein is not to be considered as legal advice. This Client Bulletin may be construed as an advertisement or solicitation. © 2009 Bryan Cave LLP. All Rights Reserved.

2. What Does the New Missouri Law Require?

In the event that a third party gains unauthorized access to and unauthorized acquisition of personal information maintained in computerized form such that the security, confidentiality or integrity of the personal information is compromised (a “breach of security” under the law), that person or company must provide notice to the Missouri resident that a breach has occurred without any unreasonable delay. That notice must include, at minimum:

1. a description of the incident in general terms;
2. the type of information that was obtained in the breach;
3. a contact number for the person or company for further assistance; and
4. contact information for consumer reporting agencies.

The statute also provides that the notice must be consistent with the “legitimate needs of law enforcement” 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.”

The notice itself may be written, telephonic (assuming the company or business has correct contact information for the Missouri resident) or electronic (again, assuming correct contact information), subject to certain special methods available for circumstances where (i) the notification would involve an expense of greater than \$100,000, (ii) the total number of affected residents is more than 150,000 or (iii) the class of affected residents is unidentifiable.

3. What Can My Company Do Now to Ensure Compliance with Missouri’s Law?

Assuming you have contacts with residents of Missouri, your company should review the scope of its data security programs (or establish such programs if your company does not have them). Effective programs must take into account all state and federal laws that may apply to your business. This is especially important for data security laws because they often, as is the case in Missouri, apply based on the residency of a consumer, not the place where business is (or was) conducted.

In reviewing data security programs, your company should consider how the internet is used at your company, how data is stored and how third parties may gain access to your systems. You should consider:

- Establishing a central executive or management employee to serve as a plan coordinator;
- Identifying reasonably foreseeable internal and external risks to security, including electronic access points and physical (i.e. paper) access points;
- Addressing any red flag rules which may apply to your company (and adjust the plan accordingly); and
- Ensuring safeguards extend to your employees and contractors.

Furthermore, your company should consider adopting an on-going review process for these plans. As technologies change, this ongoing review becomes increasingly important.

In the event a breach occurs, one key to a successful recovery is prompt attention. Having pre-existing protocols in your data security plans which establish how you will respond to a data breach can save significant time and expense in the long run.

If you need help, just ask. Bryan Cave's Privacy and Information Security Team has extensive experience designing comprehensive data-security programs that address security management, red flag rule compliance, online usage policies and data breach recognition training. We leverage extensive state and federal regulatory experience to design data-security programs and to assist in quickly responding to data-security breaches.

* * *

If you would like further information on how our experience can provide unparalleled insight before, and after, a data-security breach please contact any of the following attorneys:

Kansas City

Karen Garrett
(816) 374-3290
klgarrett@bryancave.com

St. Louis

Becky Nelson
(314) 259-2412
rebecca.nelson@bryancave.com

Atlanta

Roy Hadley
(404) 572-4510
roy.hadley@bryancave.com

Atlanta

Toby Butler
(404) 572-5907
tobias.butler@bryancave.com

Washington, D.C.

Dana Rosenfeld
(202) 508-6032
dbrosenfeld@bryancave.com

Washington, D.C.

David Zetoony
(202) 508-6030
david.zetoony@bryancave.com