Before the
FEDERAL TRADE COMMISSION
WASHINGTON, D.C.

In the Matter of	)	
	)	**Project No. R911002**
Health Breach Notification Rulemaking	)	
	)	

COMMENTS OF
THE AMERICAN LEGISLATIVE EXCHANGE COUNCIL (ALEC)

The American Legislative Exchange Council believes the Commission must proceed with great care in finalizing its proposed rules for data breach notification relating to personal health records. The Commission should undertake additional study of delegation and preemption issues raised by an expansive application of its proposed rules to entities outside its existing jurisdiction. It should likewise provide additional clarity to its proposed rules to avoid conflicts with state laws that could require consumers receiving multiple notices for the same breach and subject personal health records vendors to legal uncertainty.

STATEMENT OF INTEREST

The American Legislative Exchange Council (ALEC) is the nation's largest nonpartisan, individual membership organization of state legislators. ALEC's mission is to promote the Jeffersonian principles of individual liberty, limited government, federalism, and free markets. ALEC develops public policy through its policy task forces, including its Commerce, Trade & Economic Development Task Force, Health & Human Services Task Force, and Telecommunications & Information Technology Task Force.

ALEC's has adopted a number of official policies concerning personal health records and personal information security. Official ALEC's policies relevant to this rulemaking include its *Statement of Principles on Health IT*, *Statement of Principles on the Internet and Electronic Commerce*, and its important model bill: *Breach of Personal Information Notification Act*.

ALEC has promoted sensible data breach notification requirements in the states. In turn, a number of states have adopted data breach notification legislation based on ALEC's model.

Based on its policies and experience with state data breach notification requirements, ALEC offers these brief comments to aid the Commission in its careful consideration of its proposed rules for personal health record data breach notification.

ANALYSIS

The *American Recovery and Reinvestment Act of 2009* is the first federal statute to require data breach notification. This proceeding implements important data breach notification requirements contained in the *Recovery Act*. The Commission proposes to issue rules requiring vendors *not* subject to the *Health Insurance Portability and Accountability Act* to notify consumers or other entities in the event of a breach of security involving personal health records. Concerning the Commission's proposed rules, ALEC offers the following analysis.

I. The Commission's Proposal to Apply its Data Breach Notification Rules to Entities Outside its Enforcement Jurisdiction Raises Delegation and Preemption Problems

As a threshold matter, ALEC has concerns about jurisdictional issues raised by the Commission's proposal to apply the data breach rules under consideration to entities beyond the Commission's traditional jurisdiction under Section 5 of the *Federal Trade Commission Act*. ALEC believes that the Commission's proposal might exceed the scope of its delegated authority and pose federal preemption issues.

Although Section 13407 of the *Recovery Act* applies to "vendors of personal health records and other non-HIPPA covered entities," the Commission claims that it can apply its proposed rules to entities otherwise beyond its regulatory authority "since the Recovery Act does not limit the FTC's enforcement authority to its enforcement jurisdiction under Section 5." 74 Fed. Reg. 17914, 17915 (2009). However, if Congress had intended to expand the scope of entities regulated by the Commission under Section 5, it could have made a clear statement of such a delegation in the *Recovery Act*. ALEC disfavors agencies' reliance upon assumed or indirect and implicit delegations of authority to expand the scope of their regulatory jurisdiction. Application of the proposed rules by the Commission to its traditionally regulated entities appears a more straightforward and harmonious reading of both the relevant *Recovery Act* sections and Section 5 of the *FTC Act*. At the very least, ALEC believes further examination of the scope of the Commission's delegated authority in light of both the *FTC Act* and the *Recovery Act* is warranted before the proposed rule is finalized.

Also, the Commission's proposal to apply data breach notification rules to entities outside its existing jurisdiction under Section 5 of the FTC Act is questionable in light of federal preemption principles. A number of non-*HIPPA* entities outside of the Commission's Section 5 jurisdiction that

could be swept in under the proposed rules might already be subject to state data breach notification laws. Traditional state police powers include consumer protection. U.S. Supreme Court precedent generally provides a presumption against preemption and also requires a clear statement of legislative intent to preempt laws within states' traditional jurisdiction. To the extent that the Commission's application of its proposed data breach rules to entities outside its Section 5 jurisdiction presents conflicts with existing state laws concerning data breach notification, such conflicts could be considered a result of the Commission's reading to much into the *Recovery Act* rather than conflicts posed by the statute itself. This suggests that the Commission's application of its proposed rules to entities outside its Section 5 jurisdiction that are already subject to state data breach notification laws might be improper. Insofar as it is relevant to an independent Commission, the President's recent *Memorandum For the Heads of Executive Departments and Agencies* on *Preemption* (May 20, 2009) underscores the importance that preemption provisions codified in regulations be justified under legal principles governing preemption. ALEC has no position on whether or the extent to which Congress should preempt such state laws. But in the absence of a clear statement the Commission should examine this matter further before issuing its finalized rules.

II. The Commission Should Clarify that Personal Health Record Vendors are <u>not</u> Required to Provide Multiple Notices for the Same Breach of Security

In light of existing state data breach notification laws and related state data security laws, the Commission's proposed data breach rules will potentially subject vendors of personal health records to multiple and even conflicting requirements. Obviously, ALEC believes that multiple and conflicting data breach requirements should be avoided to the fullest extent reasonably achievable by the Commission.

ALEC's *Breach of Personal Information Notification Act* minimizes the prospect of conflicts by providing that "[a]n entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or function Federal regulator shall be in compliance with this Act." Accordingly, states that have adopted the ALEC model or like provisions better enable personal health record vendors to avoid conflicts and multiple notification mandates. Nonetheless, for those states that have enacted different data breach notification and data security legislation, the potential for conflicting and multiple notification requirements remains.

Through its model legislation concerning data breach notification, ALEC attempts to strike an important balance that fully recognizes the rights of consumers and ensures the safety of their personal information. Consumers have a right to know if and when a compromise of their personal information harms or reasonably threatens to cause harm. But consumers' information security is also endangered by over notification. Multiple notices for a single breach of security might convey to consumers an exaggerated sense of the severity and risk posed by the particular breach. Consumers who receive numerous notices where personal information is not actually acquired or where the risk of identity fraud is extremely unlikely may disregard the importance of such notices when a truly serious breach occurs. Also, proliferation of breach notices themselves poses risks to consumers by scammers who try to wrongly obtain consumers' personal information through phishing or other fraudulent schemes involving copycat or otherwise faked breach notices.

Pursuant to Section 13407(e) of the *Recovery Act*, the failure of personal health records' vendors to comply with the finalized rules to be adopted by the Commission constitutes and unfair and deceptive trade

practice under Section 18(a)(1)(B) of the *FTC Act*. Entities that the Commission proposes to be subject to its data breach notification rules are likely subject to existing state data breach notification laws that attach civil liability for failure to comply. Accordingly, subjecting personal health records vendors to conflicting data breach notice requirements means placing such vendors in a difficult-to-impossible situation.

It is ALEC's view that these serious concerns and dangers associated with over notification and conflicting requirements in the event of a breach of security require that the Commission undertake strenuous efforts to provide clarity. Personal health record vendors must be able to readily understand what is legally required of them, how to legally carry out those requirements, and what the penalties are for failure to comply. They must be able to easily discern what set of rules apply to them and what set of rules do not. In preparing its finalized rule, ALEC believes the Commission should squarely address the potential problems stemming from conflicts between federal and state laws for data breach notification.

CONCLUSION

ALEC urges the Commission undertake additional study of delegation and preemption issues raised by an expansive application of its proposed rules to entities outside its existing jurisdiction. Likewise, ALEC believes that the Commission should bring clarity to its proposed rules to avoid conflicts with state laws that could require consumers receiving multiple notices for the same breach and subject personal health records vendors to legal uncertainty. ALEC recommends the Commission seek a balance that protects consumers' right to know and prevents consumer endangerment through over notification.

Respectfully submitted,

Seth Cooper

Director,
Telecommunications &
Information Technology Task Force
American Legislative Exchange Council

1101 Vermont Ave NW, 11th Floor
Washington D.C., 20005
(202) 742-8524

June 1, 2009