

# THE SANTA FE GROUP

October 16, 2009

Georgina Verdugo  
Director  
Office for Civil Rights  
U.S. Department of Health and Human  
Services  
Hubert H. Humphrey Building  
Room 509F  
200 Independence Avenue, SW  
Washington, DC 20201

Re: RIN 0991-AB56 HITECH Breach Notification

Dear Ms. Verdugo,

I am writing to you on behalf of The Santa Fe Group Vendor Council's Identity Management Working Group. We are a consortium of businesses with deep backgrounds, expertise and experience in the protection of personal information and the remediation of data breaches.

The Santa Fe Group Vendor Council was formed in 2007 to bring together industry leaders to discuss critical issues in technology strategy and risk management. The Identity Management Working Group is made up of Vendor Council members and other representatives of the largest and most active private and public sector entities involved in broad, bi-partisan efforts for improving data protection and preventing identity theft. This group was tasked with developing an inventory of best practices for assisting victims and suggesting improvements in law and corporate practice to make it easier for victims to dispute false records and reclaim their identity. That work culminated in the April 2009 release of the white paper *Victims' Rights: Fighting Identity Crime on the Front Lines*.

The purpose of this letter is to provide comments on the implementation of the first-ever federal standard for data breach notification. Clearly, these standards will set a template for future action so it is critical that they be drafted, adopted and implemented in a manner that provides the maximum protection for individuals whose identities may be at risk. Since our primary concern is for the protection of individuals in the breach population, we will confine our comments to the areas that will impact these people most.

We have a number of concerns about the Interim Rule as currently drafted. First, the term “data breach” has not been well defined. Further, this definition should include paper-based breaches, which now account for more than 25% of all reported breaches, in addition to electronic data breaches.

Secondly, we oppose the exception for covered entities and business associates that determine there is no “significant risk of harm” to individuals in the breach population. Generally speaking, we do not support internal risk assessments in combination with a “risk” threshold because they provide entirely too much flexibility in the law for bad actors—or, frankly, even good actors concerned about cost and reputational damage.

Additionally, the idea that a covered entity can perform a self-assessment of a breach and reach an affirmative conclusion that “significant risk” exists is misguided. Our members’ experience with data breaches tells us that only a small percentage of breaches can be traced to an individual or actually reveal signs of intent. Therefore, it’s often very difficult to determine a clear risk to an individual. More common is the fact that *no determination* can be made based on the evidence trail that is reconstructed. When no determination can be made, a covered entity would be unlikely to conclude that significant harm exists and would simply claim that no definitive evidence is present to conclude significant risk and take the safe harbor.

Therefore, the fundamental question on the risk assessment seems to be the default function of the law. Is it to require notification of a breach *unless* significant harm is ruled out? Or, is it to require notification of a breach only *if* significant harm can be demonstrated? If it’s the latter, our experience tells us that lack of evidence will more often than not support a covered entity taking no action. This does not serve consumers.

Finally, while we are sensitive to the risk of consumers being notified by multiple vendors about data breaches, we are not persuaded that less information is better than more. Consumers are intelligent. If a covered entity is required to disclose a breach, it’s incumbent upon that entity to provide details as to the full nature and scope of that breach (subject to any existing law enforcement considerations). Once provided with this information, consumers can make independent judgments as to their vulnerability and take protective steps—or not—based on those facts. This is why the default function of the law is important. If covered entities cannot make affirmative determinations about the nature of the risk due to lack of evidence, this should not lead to a “no risk” conclusion. Rather, the notification should simply provide information to consumers and explain why they *may* be at risk.

We support many provisions of the interim rule, such as its extension to business associates, the forms of notification, and notice to the U.S. Department of Health and Human Services. But all of these issues largely flow from the initial determination of risk. We appreciate the scenarios included in the discussion of the interim rule as it

helps provide fact patterns that covered entities can look to for guidance. Our experience, however, is that the number of possible data breach scenarios is equal to the number of data breaches. Each one is different. As such, it is important to provide strong guidance about default expectations of a covered entity that experiences a breach and the limits to the risk-level exception.

The Santa Fe Group Vendor Council remains committed to working towards establishing the strongest standards through which to protect an individual's personal information and prevent data breaches, and we stand ready to assist in any way we can. We appreciate your consideration of our comments and thank you for your attention to this matter. If you have any questions or require additional information, please don't hesitate to contact us.

Sincerely,



Catherine A. Allen  
Chairman and CEO  
The Santa Fe Group

Cc:

The Honorable John D. Rockefeller, Chairman, Senate Commerce, Science and Transportation Committee  
The Honorable Kay Bailey Hutchison, Ranking Member, Senate Commerce, Science and Transportation Committee  
The Honorable Joe Lieberman, Chairman, Senate Homeland Security and Government Affairs Committee  
The Honorable Susan Collins, Ranking Member, Senate Homeland Security and Government Affairs Committee  
The Honorable Tom Harkin, Chairman, Senate Health, Education, Labor and Pensions Committee  
The Honorable Michael Enzi, Ranking Member, Senate Health, Education, Labor and Pensions Committee  
The Honorable Henry Waxman, Chairman, House Energy and Commerce Committee  
The Honorable Joe Barton, Ranking Member, House Energy and Commerce Committee  
The Honorable Edolphus Towns, Chairman, House Oversight and Government Reform Committee  
The Honorable Darrell Issa, Ranking Member, House Oversight and Government Reform Committee