Identity Theft 911
From panic to peace of mind.™

June 1, 2009

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

SUBJECT: **Health Breach Notification Rulemaking Project No. R911002**

Dear Sir and/or Madam:

The purpose of this letter is to offer comment regarding "Health Breach Notification Rulemaking Project No. R911002". First, I feel it important to note that it is with great anticipation that we await the final rules regarding notification requirements in health breaches. As a provider of breach and fraud solutions to 35% of the personal lines insurance industry, and an ever growing group of small and midsized U.S. businesses through commercial insurance carriers, my colleagues and I have handled hundreds of breaches for clients in the areas of financial services, insurance, employee records, and of course, healthcare.

While assessing the damages and putting mitigation tools into place for information security breaches that release Personally Identifiable Information (PII) related to credit, tax and financial data is complicated enough, at least there is a newly developing and recognized approach to handling and approaching these situations based on the various state breach notification laws and evolving industry best practices that have grown and expanded over the last decade.

Unfortunately, assessing and dealing with breaches that involve Protected Health Information (PHI) and/or Protected Health Records (PHR) has proven much more difficult than breaches involving standard PII for a number of reasons. The main reason for this revolves around the fact that there have been no clearly defined notification requirements surrounding information security breaches releasing PHI until now. This first step to "formalizing" the handling of information breaches in the medical information context is necessary to begin discussions on other processes that can better assist the American consumer in medical breaches. We hope that this may even lead to rights of redress to correct inaccurately reported medical data similar to the rights that consumers have to correct inaccuracies in the data found in their credit files.

The lack of breach notification in PHI breaches combined with a lack of a consumer/patient right of redress has combined to make the prevention, handling and resolution of identity fraud related to a PHI breach extremely difficult for professional fraud specialists, let alone for the average U.S. patient/consumer. We hope that the further development of the breach notification regulations around health information breaches is an important step in the right direction.

Identity Theft 911, LLC
www.identitytheft911.com

Identity Theft 911 Knowledge Center™
www.identitytheft911.org

Headquarters
4150 N Drinkwater Blvd, Suite 210
Scottsdale, AZ 85251

480.355.8500 main
888.682.5911 toll free
480.355.8425 fax

With that said, while we have some specifics to comment on regarding the proposed Health Breach Notification rule we feel that most of the content and language in the proposed rule is a vast improvement over disparate state breach notification laws that deal with various forms of more traditional PII and hope that this may eventually act as a template for a more standardized federal approach to other types of breaches involving non-medical data.

Following are the basic concerns with the current proposed rule as it stands. While overall, the proposed rule is well thought out and fill a void in the space of medical breaches, there are a couple of concerns that we felt it necessary to address.

INDIVIDUAL NOTICE

Under the Section labeled as *Individual Notice*, there is discussion regarding proposed paragraph 318.5(a)(1) which states that individuals must be given notice by first class mail or, if the individual provides affirmative consent, by E-mail. This preference must be "*specified as a preference by the individual*" and that the individual must provide "*express affirmative consent*" to receive breach notices by E-mail. The Commission recognized that some E-mail notifications may be screened by consumers' spam filters and felt that this problem was understated and should be addressed in further detail. We agree.

We know from experience in working with our numerous breach clients that the costs associated with providing written, hardcopy, mailed breach notification letters can often be exorbitant. Therefore, it should be assumed that most entities subject to the proposed requirements would automatically and preemptively attempt to obtain the "*express affirmative consent*" from individuals to allow E-mail breach notices immediately upon establishing a relationship with that individual. It should further be assumed that this will simply become standard practice in most organizations due to the cost saving factor associated with this practice.

Our suggestion would be to require that prior to obtaining any "*express affirmative consent*" from an individual allowing E-mail notice for medical breaches, that the institution notify and warn the individual of the possibility that such a notice may be blocked by the individual's spam filter. Further, the institution attempting to obtain such consent should provide some sort of guidance regarding how to set spam filter preferences to allow the sending of such breach notifications via E-mail to ensure that such notifications are actually received by the individual to whom it was sent.

We recognize that one of the largest obstacles for companies in providing notice to individuals whose PII, PHI or PHR has been exposed without their consent is the cost of notification via traditional first class mail. And, while many states have upward cost and notice volume limits that allow for alternate means of notification, this is still not economically feasible for most institutions under most state breach notification laws. Therefore we applaud the fact that this proposed regulation will grant the

Identity Theft 911, LLC
www.identitytheft911.com

Identity Theft 911 Knowledge Center™
www.identitytheft911.org

Headquarters
4150 N Drinkwater Blvd, Suite 210
Scottsdale, AZ 85251

480.355.8500 main
888.682.5911 toll free
480.355.8425 fax

ability to provide alternate forms of notice via electronic means without having to consider cost and volume thresholds.

Obviously, the intent behind breach notification regulations is to provide individuals with the knowledge that their information has been exposed, and to do so in a timely manner. However, this goal will fail to be met if **any** number of notification recipients have their breach notice end up in their Junk E-mail box rather than in their inbox. This is the major concern with E-mail notification Entities that will benefit from the cost savings of NOT having to provide such notice through traditional mail should at least have the burden of attempting to use their best efforts to educate consumers about the risks of notice ending up in a spam filter or junk E-mail box and to help ensure proactively that E-mail notice will actually make it to its intended recipient.

NOTICE TO MEDIA

While we feel that providing notice to the media in larger breach situations is not just advisable but a best practice, we feel that the requirement to notify both the individual AND the media in breaches involving more than 500 people is unreasonable for a number of reasons.

First, the threshold number of 500 affected data subjects seems to be exceptionally low to mandate both individual notice as well as media notice. The risk to requiring media notice in all medical data breaches affecting merely 500 people (or more) is that the media will begin to downplay the importance of these events and will fail to report them as time goes on due to their "non-newsworthiness". This could also result in a fear echoed by many people in the privacy industry: over reporting and over notification of breaches will actually result in a public that begins to ignore these notifications due to them being so ubiquitous.

Another side effect of notifying the media in any breach that affects more than 500 people is the subsequent burden that will then be faced by most institutions as a result of such a media disclosure. Many **other** individuals whose PHI or PHR is **unaffected** will contact the affected institution to inquire as to whether or not they are also involved in the breach as well. In the end, this mandate to notify the media in breaches affecting more than 500 people will result in a confused public and will often unnecessarily tie up an entity's resources when it is forced to handle a high volume of calls from individuals that are completely unaffected by the incident.

Therefore, we see no immediate benefit to requiring notice BOTH to individuals and to the media in breaches affecting less than at least 1000 data subjects. The potential negative fall out far outweighs the benefits. We feel that providing this additional notification rather than using it simply as an alternate means of notification in extremely large breach situation is unwise and will result in more questions for the consumer rather than more answers.

Identity Theft 911, LLC
www.identitytheft911.com

Identity Theft 911 Knowledge Center™
www.identitytheft911.org

Headquarters
4150 N Drinkwater Blvd, Suite 210
Scottsdale, AZ 85251

480.355.8500 main
888.682.5911 toll free
480.355.8425 fax

Identity Theft 911
From panic to peace of mind.™

OVERALL ANALYSIS OF PROPOSED REGULATION

We feel that on the whole, the proposed rule is a very strong and positive step towards safeguarding the medical information and preventing medical identity theft for the average U.S. consumer. While much has been learned by the nation's experience with data breaches large and small over the last six years, the reality is that this is still a very new phenomenon that is unique to the 21st century. With that said, even the best and tightest regulatory provisions on the subject of data breach will be found to be lacking in some areas over time. As our experience in dealing with these scenarios in the context of medical data grows, so to I hope will our approach and solutions to dealing with them.

We further hope that this is simply the first of many important steps in working toward a feasible and realistic approach to managing private medical information here in the United States. In addition we also hope that this eventually results in other future federal legislation that can help to harmonize a very disjointed state by state approach to handling data breaches. We thank the commission for the opportunity to comment on the record regarding the proposed rules and hope that our comments are considered in the final rulemaking process.

Sincerely,

Eduard F. Goodman, J.D., LL.M.
CIPP
Chief Privacy Officer

Identity Theft 911, LLC
www.identitytheft911.com

Identity Theft 911 Knowledge Center™
www.identitytheft911.org

Headquarters
4150 N Drinkwater Blvd, Suite 210
Scottsdale, AZ 85251

480.355.8500 main
888.682.5911 toll free
480.355.8425 fax