idexperts®
Leader in Data Breach Prevention & Remediation

May 15, 2009

Office of the Secretary
Federal Trade Commission
Room H-135 (Annex M)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

RE: Health Breach Notification Rulemaking, Project No. R911002

To Whom It May Concern:

I am writing in response to the Federal Trade Commission's (FTC) request for public comment on the health breach notification rule, which was required by the American Recovery and Reinvestment Act of 2009.

ID Experts was founded in 2003 to address the growing problem of identity theft in a very personal and caring way. Our initial focus was on using best practices to provide a highly personal and effective approach to recovery services for those that fall victim to identity theft. We have since branched out to offer data breach response services directly to businesses, but our core mission has not deviated: mitigate the risk of data breaches and identity theft and help victims recover from the emotional and financial issues that flow from identity crime. In short, we help people put their lives back together.

The thousands of victims we've recovered and hundreds of businesses we've helped give us a unique vantage point to inform, from the ground level, the rules that will govern medical identity theft. We appreciate this opportunity.

Our comments are broken down into two sections. The first provides feedback on the rule as written by FTC and the second suggests some additions that will give additional support to victims of medical identity theft. Identity crime is too often considered "victimless," when in reality it causes considerable emotional and financial disruptions in the lives of ordinary people who are mostly left alone to put their life back together. Helping them recover from this crime is an essential part of them re-establishing their identity. We have a considerable amount of experience with medical identity theft and don't want to miss an opportunity to suggest some important "victims' rights" improvements based on cases we've handled.

COMMENTS ON FTC RULE

Nature of entity: We think it's best to define the "nature of entities" covered by the regulations as broadly as possible. We recommend "any entity with management responsibility – whether it's storage or transmission – of a paper or electronic health record." As the notice points out, there will be a lot of overlap between HIPAA and FTC-regulated businesses so the two will coordinate on the final breach notification requirements. Since much of the breach activity comes from 3rd parties, the final rule should encompass all who safeguard medical records.

Products/Services: We don't believe that identifying a covered entity by the products or services they provide makes sense. The marketplace evolves and it's not prudent to cement in statute or regulation today's products and services to a future breach notification requirement. The FTC is well-served to maintain focus on the handling of Electronic Health Records, not how they're being packaged and sold.

Dual role: This is a very legitimate concern as we have experience in mitigating breach risk due to vendor / 3rd Party error, not that of the primary business. There should be a requirement in the rule that the 3rd Party and primary business coordinate (from a practical standpoint, of course, they'll have to) in the response. But, the notification should come from the responsible party – whether it's the primary business or the 3rd Party – in order to assign appropriate blame for the consumer. If the vendor is responsible for the breach, the issue of an "unrecognized" entity notifying the consumer is legitimate. From a transparency standpoint, the 3rd Party should take responsibility and name the primary business (i.e. the hospital) for which they provide services so it's clear to the consumer why they're receiving the notice.

The breach description is broadly defined, which is good, and the FTC is assuming a positive determination. That's strong pro-consumer language. In fact, the only way to avoid notification under the proposed rule is if "reliable evidence" is obtained that proves the unauthorized access was not malicious. The rule, however, does not define what "reliable evidence" is. So, we recommend that the FTC include a "reliable evidence" definition to avoid any ambiguity. The rule refers to personnel interviews and data forensics in another section, but those tactics don't tie back to "reliable evidence." This is going to leave that open to significant interpretation as covered entities come up with new and interesting evidence they can claim is "reliable."

Personal Health Record: The definition of Personal Health Record excludes paper-based medical records, even though it's referenced in another part of the document. Does the FTC mean to suggest that if a hospital or associate loses an electronic record it triggers notification, but a lost paper record will not? We recommend that the FTC include paper records, which our experience tells us is a major source of

identity crime. If it's important to protect medical records then we shouldn't distinguish between electronic and paper.

Unsecured: While there does appear to be some wiggle room in the definition to include process through the use of the term "methodology specified by the Secretary of HHS," it's heavily weighted toward technology. This picks up on the theme of the Personal Health Record definition, which leaves out paper. We recommend that the FTC beef up the language regarding human resources (HR) process (personnel screening, access restrictions, paper storage, etc.) to ensure that we're defining "unsecured" more broadly. While security tends to be defined as hardening data systems, our experience tells us that all too often it is paper records that are compromised. Many health or insurance companies are using temporary workers to help convert paper records to digital. In many cases, these temporary workers have fewer screening requirements that allow criminal elements to slip through HR.

Breach Notification Requirement: We understand that this is an FTC rule and the Recovery Act pre-empts state law. But, given the interest from Attorneys General from around the country in tracking breaches, and a breach's impact on state residents, it is an issue. We recommend including written notification to the Attorneys General in states where members of the breach population reside. The rule goes on to reference "state or jurisdiction" in the 500-person threshold triggering media notification. So, the FTC is already contemplating state-level jurisdictions in the rule.

60-day notification requirement: We support this requirement as it provides a federal standard, where no standard exists today. This will bring continuity to the expectations for when notice should be sent, prevent companies from delaying notification unnecessarily, and assist the victim in protecting themselves in a timely fashion.

Methods of notification: One of our biggest concerns over the last few years has been that proliferation of notification requirements has led to too much public notice of data breaches. Publicly posting notice via a website in cases where 10+ individual notices are returned may be detrimental to the data breach engagement and the reputation of the organization in question. This practice contributes to "over notification" that in turn causes the affected population to become "numb" to notification letters altogether.

There are better mechanisms with which to ensure an organization is noticing the most up-to-date addresses and not using an overly antiquated data set to subvert costs associated with the notice. Utilization of a skip tracing service helps reduce the number of returned packages when dealing with an antiquated data set, increasing the number of letters delivered accurately and benefitting all parties. Also, a company could simply spend more time or resources on data collection to begin with. Oftentimes, that is all it takes for an organization to mail to more recent addresses than those that may have been lost. Frankly, any guidance in this area

would be helpful for our clients. This in one of those state laws that is ambiguous across the board. Once a company mails a letter, how much money and effort are required to find better addresses?

It has also been our experience that details that should not be made public (due to an investigation, for example) are made public when information is posted on websites in an automated fashion. Transparency is a good thing in data breaches. But, information that is made available to people outside the breach population or compromises investigations is counter-productive to both the breach response and the effort to catch perpetrators when the breach is malicious.

The direct mail notification is paramount and tightly drawn. In order to notify by email, there needs to be express permission given in advance by the consumer. This is reasonable and ensures the highest-level of outreach occurs as a default practice.

Notification content requirement: Organizations will be required to include contact information for obtaining information or assistance. We think this is a significant step in helping a potential victim locate a knowledgeable representative to get them started in the process of protecting their identity. Too many times, information to contact a company representative is elusive or non-existent. Companies are merely satisfying a legal obligation – the state notification requirement – not seeking to assist members of the breach population. Removing the anonymity in the notification process for the sake of adequate protection to the individual is also a benefit.

Including both the date of breach and date of discovery in the letter could be problematic. Sometimes it is out of an entity's control when they discover a breach has occurred and communicating two dates may present challenges to the affected population. We recommend that the date of discovery be a requirement. If there is a significant amount of time between the breach and discovery date - say over 90 days - we would suggest that the company give an explanation as to why it wasn't discovered sooner.

Media notification: We have seen media notification lead to over-reaction and anxiety. More importantly, responding to the many people who are not affected impedes an organization's ability to respond to those who are. Assuming an organization has adequately investigated and thoroughly inventoried the data that was lost, notice that makes its way to populations beyond those who are affected is unadvisable. When the media controls release and content of notice the facts are not always delivered objectively or accurately.

Substitute Notice: As one reads the rule, the conclusion is that substitute notice can only be triggered after primary methods are exhausted. Having said that, the trigger is that more than 10 people in the breach population cannot be identified through mail, phone, or email. Does that mean that a covered entity *must* attempt the entire universe or only up until they have 10 out-of-date records? Again, a reasonable

person reading this would conclude the former. But, it could be made clear with a sentence or two.

Extent of coverage: Again, we believe the mandate should follow the medical record not the nature of the entity.

REQUIREMENTS TO ENSURE VICTIM SUPPORT

There are many issues that directly correlate between financial identity theft and medical identity theft. As a result, a few rights should be granted to the potential or actual victim. Based on the many cases of medical identity theft we have worked on, several critical steps can be made that will help the victim more easily recover and give them the documentation they need to prove the crime. That documentation *will* be needed as the residue of identity crime has a way of returning several years after the initial theft. Many of the issues that have appeared in our cases are outlined below. If you'd like more information about these recommendations, we would welcome a follow-up discussion.

Medical Collection Agencies:

- Provide information to the consumer with clear instructions on how to dispute any issues connected to medical identity theft
- Recognize Power of Attorney for third-party disputes
- Information should be provided regarding where account charges originated and contact information for those facilities
- Provide clearance letter to consumer when account has been cleared due to fraud
- Notify bureaus to remove fraudulent collection account

Health Care Providers:

- Provide consumer with clear instruction on how to dispute fraudulent information
- Acknowledgement of Power Of Attorney for third party dispute
- Inform consumer of any other treatments received under their SSN/insurance information at the facility (often a victim will only know about a single incident when there may be multiple times that their SSN/insurance was used, for example an ER visit, radiology, f/u appointments with an MD, etc).

- Improved communication between billing department-collections department at facility/medical provider (this would help victims discover multiple events more quickly)

- Disassociate all consumer PII from fraudulent records and name fraudulent file or record "John Doe" or "Jane Doe."

- Provide documentation to consumer on when services were rendered, with date and time, so victim can provide documentation of where they were (letter from HR dept) when services were received.

- Communicate with consumer as to how fraudulent records are expunged/flagged and what the process is for disassociating those records.

- Tell consumer whether or not insurance information was provided for treatment or just SSN

- Provide clearance letter to consumer when account(s) have been cleared due to fraud

Requirements of Insurance Companies:

- Provide consumer with clear instruction on how to dispute fraudulent information

- Acknowledgement of POA for third party dispute

- If insurance number is used fraudulently, consumer should receive new #

- If insurance # is compromised-# should be flagged (similar to a fraud alert on credit file)

- Provide information regarding where account/charges originated-provide contact information for facility, doctors office, etc

- Provide clearance letter to consumer when claims have been cleared due to fraud

Thank you for your leadership in the area of identity crime. The FTC has been an invaluable resource for thousands of victims, and it is appropriate that you would now take up leadership in helping combat medical identity theft. If ID Experts can answer any questions you might have about our experience in managing data breach events or restoring victims, please don't hesitate to call.

Sincerely,

Rick Kam
President