COMMENTS OF

INTUIT INC

ON THE

FEDERAL TRADE COMMISSION

GUIDANCE SPECIFYING THE TECHNOLOGIES & METHODOLOGIES

THAT RENDER PROTECTED HEALTH INFORMATION

UNUSABLE, UNREADABLE OR INDECIPHERABLE

FOR PURPOSES OF THE BREACH NOTIFICATION REQUIREMENTS

UNDER SECTION 13402 OF TITLE XIII (HITECH ACT) OF THE

AMERICAN RECOVERY & REINVESTMENT ACT OF 2009

MAY 21, 2009

Intuit thanks the Federal Trade Commission for the opportunity to comment on the proposed rulemakings on Security Breach Notifications as part of their implementations of the American Recovery and Reinvestment Act (ARRA) and applauds the department for their thoughtful work in providing a platform for the privacy of Personal Health Record information.

Intuit, named by Fortune Magazine as America's most-admired software company for the fourth consecutive year, offers products and services to help people solve their important problems. Whether helping balance a checkbook, run a small business, or pay income taxes, our innovative solutions have simplified millions of people's lives. In a world where emerging technology and market trends are changing the way people live and work, we'll continue to develop new products that offer the same ease and delight that are a hallmark of Intuit's pursuit of customer-driven innovation.

Intuit also helps consumers manage their health and medical expenses. Among other offerings, Intuit cooperates with several health plans to provide *Quicken Health℠ Expense Tracker*; a service that gathers medical expense information in one place, enabling the consumer to find and correct errors, to make medical payments easily, and to transfer the information smoothly to their income tax returns.

Intuit urges that a single, Federal set of standards and guidelines be developed to provide protection for Personal Health Records. We believe that multiple standards and guidelines, whether by responsible agencies or state and local governments, will induce confusion among the holders of Personal Health Records and the consumers whose private information may be breached.

Intuit believes that technical guidelines are preferable to developing a list of approved products. American business is continually innovating – developing new and better technologies. Preparing a complete list of providers of a type of technology risks missing new and/or smaller products and companies and may spark attacks against those listed technologies. However, listing guidelines allows new solutions to be used as they become available and proven effective.

Intuit offers the following comments and questions.

- Definition of Security Breach: The definitions suggested by the FTC and HHS appear to be substantively the same. However, in the FTC proposed rulemaking there is the following: "*reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information*". We'd like to ask the FTC to provide clarification of what types of evidence would demonstrate that there was no unauthorized acquisition? It seems difficult to prove a negative.
- Definition of Personal Health Record: We'd like to receive further clarification on the phrase "*can be drawn from multiple sources*" We'd like to ask the FTC for clarification on what is a "*source*" and what constitutes "*multiple sources*"; including why that latter concept is key to the definition of PHR? Can the FTC explain what is meant by "*managed, shared, and controlled by*?" Our concern is that some customer records may be PHRs and some not, depending on the answer.
- Example PHR Identifiable Health Information: We'd like to ask the FTC for clarification around the statement: "*Thus, for example, the proposed rule would cover a security breach of a database containing names and credit card information, even if no other information was included.*" We are concerned that names and financial information are data points covered in other rulings, resulting in possible confusion and conflicting requirements. If name and credit card information are the only data in a record, the information would appear to be a financial transaction record and not a health record. There are hundreds of merchant credit card processors – is it the intent that records held by those processors are covered?
- Definitions of "*De-identification*": The HHS definition does not include the "*reasonable basis*" language. We'd like to see additional alignment of the two definitions. In addition, we ask the FTC to further explain and clarify the concept of "*no reasonable basis*", including the standards to use and burden of proof.
- Definition of "*PHR-related entity*": Some entities may be both Business Associates and neither Business Associates nor covered entities, particular to different sets of data or the same data at different times. To a certain extent Intuit's Quicken Health Expense Tracker offering may fall into this category. Can you clarify how organizations that might be, at different times or for different sets of data, both Business Associates covered under HIPAA and excluded entities not covered under HIPAA, should apply definitions and rules to the data in question? Can you clarify the extent/type of Web site relationship that is required in order for the definition to apply? Do simple links to free consumer products from covered entity sites meet the definition, for example?

- Requirement for notification and acknowledgement: The FTC requires 3rd parties to notify a "*senior official of the vendor or PHR related entity and to obtain acknowledgment from such official that he or she has received the notice*." We would like to ask what type of acknowledgement would be required.
- Definition of "*Discovered*": The date/time of a data breach "discovery" can be extremely difficult to discern. We'd like additional clarification of this definition– is it when a senior official learns of the possible event? Is it when something is suspected by staff members but not confirmed?
- Definition of "*Reasonably should have known*": We would like more explanation and/or examples of this phrase.
- Requirement "Breach Notification Timing": The FTC language cites that it is "*allowed*" to delay notification at the "*appropriate request of a law enforcement official*." The HHS language says it "*requires a delay* of *notification where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security*". We'd like to ask if these paragraphs are essentially the same.
- Example Breach Notification Timing: We'd like to point out that a 60 day outer limit requirement for notification may be a problem for organizations to meet in some cases. Sixty days may not be enough time to determine the complete list of affected individuals or to determine the courses of action recommended to the affected individuals.
- Questions for the Public:
  "*Alternate media notice language must be prominent, and run multiple times. The Commission requests further comment on the standards that should apply to substitute media notice*."
    - Intuit believes that it would be appropriate to consider geographic and demographic attributes in selecting substitute media – choosing media that would be appropriate for the affected parties.
- Ruling Effectiveness Timing: We'd like to point out that a 30 day implementation requirement may be difficult for some organizations to meet. Larger organizations may require more time to "turn the battleship" and smaller organizations may require more time to become aware of the requirement.