Supporting Statement for the Proposed Health Breach Notification Rulemaking
16 C.F.R. Part 318
(OMB Control No. 3084-NEW)

On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009 (the "Recovery Act" or "the Act") into law. The Act includes provisions to advance the use of health information technology and, at the same time, strengthen privacy and security protections for health information**.**

(1) & (2) Necessity for and Use of the Information Collection

Among other things, the Recovery Act recognizes that there are new types of web-based entities that collect consumers' health information. These entities include vendors of personal health records and other entities that offer online applications that interact with such personal health records ("PHR related entities"). Some of these entities are not subject to the privacy and security requirements of the Health Insurance Portability and Accountability Act ("HIPAA"). For such entities, the Recovery Act requires the Department of Health and Human Services ("HHS") to study, in consultation with the FTC, potential privacy, security, and breach notification requirements and submit a report to Congress containing recommendations within one year of enactment of the Recovery Act. Until Congress enacts new legislation implementing any recommendations contained in the HHS/FTC report, the Recovery Act contains temporary requirements, to be enforced by the FTC, that such entities notify customers in the event of a security breach. The proposed rule ("Rule") implements these requirements.

These requirements are subject to the provisions of the Paperwork Reduction Act, 44 U.S.C. Chapter 35 ("PRA"). The Rule requires vendors of personal health records and PHR related entities to provide: (1) notice to consumers whose unsecured personally identifiable health information has been breached; and (2) notice to the Commission. The Rule requires third party service providers (i.e., those companies that provide services such as billing or data storage) to vendors of personal health records and PHR related entities to provide notification to such vendors and PHR related entities following the discovery of a breach. The Rule does not include recordkeeping requirements.

(3) Information Technology

The Rule gives explicit examples of electronic options that covered entities may use to provide notice to consumers and the Commission. These electronic options help minimize the burden and cost of the Rule's information collection requirements for entities subject to the Rule. Likewise, the Rule is consistent with the Government Paperwork Elimination Act, which, in relevant part, requires that OMB ensure that Executive agencies, by October 23, 2003, provide for the option of electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper. See 44 U.S.C. § 3504 note.

(4) Efforts to Identify Duplication

The FTC has not identified any other federal statutes, rules, or policies currently in effect that would conflict with the Rule. There is a potential for overlap with forthcoming rules to be promulgated by HHS governing breach notification for entities covered by HIPAA. The FTC is consulting with HHS on this potential overlap.

(5) Efforts to Minimize Small Organization Burden

In drafting the Rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. In particular, the Commission believes that the alternative of providing notice to consumers electronically will assist small entities by significantly reducing the cost of sending breach notices.

(6) Consequences of Conducting Collection Less Frequently

A less frequent "collection" would violate both the express statutory language and intent of the Recovery Act.

(7) Circumstances Requiring Collection Inconsistent with Guidelines

The collection of information in the Rule is consistent with all applicable guidelines contained in 5 C.F.R. § 1320.5(d)(2).

(8) Public Comments/Consultation Outside the Agency

The Commission is seeking through its notice of proposed rulemaking public comment on the various aspects of the Rule, including the Rule's PRA implications. See [NPRM citation to be inserted before submission to OMB]

(9) Payments or Gifts to Respondents

Not applicable.

(10) & (11) Assurances of Confidentiality/Matters of a Sensitive Nature

The Rule's breach notification requirements do not involve disclosure of confidential or sensitive information.

(12) Estimated Annual Hours Burden and Labor Costs[1]

In the event of a data breach, the Rule would require covered firms to investigate and, if certain conditions are met, notify consumers and the Commission. The annual hours burden and labor costs associated with these requirements will depend on a variety of factors, including the number of covered firms that will experience a breach requiring further investigation and the number of breach notices sent.

Based on input from industry sources, staff estimates that approximately 200 vendors of personal health records and 500 PHR related entities will be covered by the Rule. Thus, a total of 700 entities may be required to notify consumers and the Commission in the event that they experience a breach. Approximately 200 third party service providers also will be subject to the Rule, and thus required to notify vendors of personal health records or PHR related entities in the event of a breach. Thus, a total of approximately 900 entities will be subject to the Rule's breach notification requirements.

Staff estimates that these entities, cumulatively, will experience 11 breaches per year for which notification may be required. Because there is insufficient data at this time about the number and incidence of breaches in the personal health record industry, staff used available data relating to breaches incurred by private sector businesses in order to calculate a breach incidence rate. Staff then applied this rate to the estimated total number of entities that will be subject to the Rule. According to one recent research paper, private sector businesses across multiple industries experienced a total of approximately 50 breaches per year during the years 2002 through 2007.[2] Dividing 50 breaches by the estimated number of firms that would be subject to a breach (4,187)[3]

---

[1] Staff notes that its estimate of the annual hours burden and labor costs likely overstates the costs imposed by the Rule because: (1) it assumes that all breaches will require notification, whereas many breaches will not require notification (e.g., those involving data that is not "unsecured"); (2) it assumes that all entities subject to the Rule's notification requirements will be required to take all of the steps described below; and (3) staff made conservative assumptions in developing many of the underlying estimates.

[2] Sasha Romanosky, Rahul Telang & Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" Seventh Workshop on the Economics of Information Security, June 2008. The authors tallied the breaches reported to the website Attrition.org during the time period 2002 to 2007 and counted a total of 773 breaches for a range of entities, including businesses, governments, health providers, and educational institutions. Staff used the volume of breaches reported for businesses (246 over a 5 year period, or approximately 50 per year) because that class of data is most compatible with other data staff used to calculate the incidence of breaches.

[3] Staff focused on firms that routinely collect information on a sizeable number of consumers, thereby rendering them attractive targets for data thieves. To do so, staff focused first on retail businesses and eliminated retailers with annual revenue under $1,000,000. The

yields an estimated breach incidence rate of 1.2% per year. Applying this incidence rate to the estimated 900 vendors of personal health records, PHR related entities, and third party service providers yields an estimate of 11 breaches per year that may require notification of consumers and the Commission.

Staff estimates that covered firms will require per breach, on average, 100 hours of employee labor at a cost of $4,652[4] to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required report to the Commission. Based on the estimate that there will be 11 breaches per year, the annual hours burden for all covered entities is 1,100 and the annual labor cost associated with these tasks is $51,172.

In addition, covered entities will incur labor costs associated with processing calls that come in through the toll-free number they may set up in the event of a data breach.[5] Staff estimates that processing per breach an estimated 5,000 calls for the first month will require an average of 1,917 hours of employee labor at a cost of $27,468.[6] Staff estimates that affected entities will need to offer the toll-free number for an additional five months, during which time staff projects that entities will receive an additional 5,000 calls,[7] yielding an estimated annual labor cost of $54,936 for processing calls. Based on the above rate of 11 breaches per year, the annual

---

2002 Economic Census reports that, in that year, there were 418,713 retailers with revenue of $1,000,000 or more. To apply 50 breaches to such a large population, however, would yield a very small incidence rate. In an abundance of caution, to estimate more conservatively the incidence of breach, staff then assumed that only one percent of these firms had security vulnerabilities that would render them breach targets, thus yielding the total of 4,187.

[4] Hourly wages throughout this supporting statement are based on http://www.bls.gov/ncs/ncswage2007.htm (National Compensation Survey: Occupational Earnings in the United States 2007, U.S. Department of Labor released August 2008, Bulletin 2704, Table 3 ("Full-time civilian workers," mean and median hourly wages).

[5] The cost of a toll-free number will depend on the cost associated with T1 lines sufficient to handle the projected call volume, the cost of obtaining a toll-free telephone number and queue messaging (a service that provides rudimentary call routing), the cost of processing each call, and the telecommunication charges associated with each call. Because the Rule may require entities to notify consumers by posting a message on their homepage for a period of six months, staff estimated the cost of a toll-free line for a six-month period. The labor costs associated with the toll-free number are those associated with the processing costs.

[6] The breakdown of labor hours and costs is as follows: 667 hours of telephone operator time (8 minutes per call x 5,000 calls) at $14.87 per hour and 1,250 hours of information processor time (15 minutes per call x 5,000 calls) at $14.04 per hour.

[7] Staff anticipates that the greatest influx of calls will be in the first month, and that it will be equivalent to the volume of calls over the remaining five months.

hours burden is 42,174 ((1,917 hours x 2) x 11 breaches) and the annual labor cost is $604,296.

In sum, the total annual estimated hours burden associated with the Rule would be 43,274 (1,100 + (1,917 x 2 x 11)), and the annual estimated labor cost would be $655,468.

(13) Estimated Capital/Other Non-Labor Costs Burden[8]

Staff estimates that the capital and other non-labor costs associated with the Rule would consist of the following:

1. the services of a forensic expert in investigating the breach;
2. notification of consumers via e-mail, mail, web posting, or media; and
3. other costs associated with setting up a toll-free number, if needed (i.e., costs associated with T1 lines sufficient to handle the projected call volume, the cost of obtaining a toll-free telephone number and queue messaging, and the telecommunication charges associated with each call)

First, staff estimates that covered firms will require the services of a forensic expert at a cost of $2,930.[9] Based on the estimate that there will be 11 breaches per year, the annual cost associated with the services of a forensic expert are $32,230.

Second, the cost of breach notifications will depend on the number of consumers contacted. Based on a recent survey, 11.6 percent of adult consumers reported receiving a breach notification during a one-year period.[10] Staff estimates that for the prospective 3-year PRA clearance, the average customer base of all vendors of personal health records and PHR related entities will be approximately two million per year. Accordingly, staff estimates that an average of 232,000

---

[8] As with its estimates of the annual hours burden and labor costs, staff notes that its estimate of the capital and other non-labor costs likely overstates the costs imposed by the Rule because: (1) it assumes that all breaches will require notification, whereas many breaches (e.g., those involving data that is not “unsecured") will not require notification; (2) it assumes that all entities subject to the Rule’s notification requirements will be required to take all of the steps described below; and (3) staff made conservative assumptions in developing many of the underlying estimates.

[9] Staff estimates that breached entities will use 30 hours of a forensic expert's time. Staff applied the wages of a network systems and data communications analyst ($32.56), tripled it to reflect profits and overhead for an outside consultant ($97.68), and multiplied it by 30 hours to yield $2,930.

[10] Ponemon Institute, "National Survey on Data Security Breach Notification," 2005. Staff believes that this estimate is likely high given the importance of data security to the personal health record industry and the likelihood that data encryption will be a strong selling point to consumers.

consumers per year will receive a breach notification.

Given the online relationship between consumers and vendors of personal health records and PHR related entities, most notifications will be made by email and the cost of such notifications will be de minimis.[11]

In some cases, however, vendors of personal health records and PHR related entities will need to notify individuals by postal mail, either because these individuals have asked for such notification, or because the email addresses of these individuals are not current or not working. Staff estimates that the cost of notifying an individual by postal mail is approximately $2.30 per letter.[12] Assuming that vendors of personal health records and PHR related entities will need to notify by postal mail 10 percent of their customers whose information is breached, the estimated cost of this notification will be $53,360 per year.

In addition, vendors of personal health records and PHR related entities sometimes may need to notify consumers by posting a message on their home page, or by providing media notice. Based on a recent study on data breach costs, staff estimates the cost of providing notice via website posting to be 6 cents per breached record, and the cost of providing notice via published media to be 3 cents per breached record.[13] Applied to the above-stated estimate of 232,000 consumers per year receiving breach notification, the estimated total annual cost of website notice will be $13,920, and the estimated total annual cost of media notice will be $6,960, yielding an estimated total annual cost for all forms of notice to consumers of $74,240.

Third, based on industry research, staff projects that in order to accommodate a sufficient number of incoming calls for that period, affected entities may need two T1 lines at a cost of $18,000.[14] Staff further estimates that the cost of obtaining a dedicated toll-free line and queue messaging will be $3,017.[15] In addition, according to industry research, the telecommunication

---

[11] See National Do Not Email Registry, A Report to Congress, June 2004 n.93, available at www.ftc.gov/reports/dneregistry/report.pdf.

[12] Robin Sidel and Mitchell Pacelle, "Credit-Card Breach Tests Banking Industry's Defenses," Wall Street Journal, June 21, 2005, p.C1. Sidel and Pacelle reported that industry sources estimated the cost per letter to be about $2.00 in 2005. Allowing for inflation, staff estimates the cost to average about $2.30 per letter over the next three years of prospective PRA clearance sought from OMB.

[13] Ponemon Institute, 2006 Annual Study: Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, Table 2.

[14] According to industry research, the cost of a single T1 line is $1,500 per month.

[15] Staff estimates that installation of a toll-free number and queue messaging will require 40 hours of a technician's time. Staff applied the wages of a telecommunications technician

charges associated with the toll-free line will be approximately $2,500.[16] Adding these costs together, staff estimates that the capital and other non-labor costs per breach for setting up a toll-free line will be $23,517. Based on the above rate of 11 breaches per year, the annual cost burden for affected entities will be $258,687 (11 x $23,517).

In sum, the total estimate for capital and other non-labor costs is $365,157: $32,230 (services of a forensic expert) + $74,240 (costs of notifying consumers) + $258,687 (capital and other non-labor costs associated with a toll-free line).

(14) Estimate of Cost to Federal Government

Staff estimates that the fiscal year cost to the FTC Bureau of Consumer Protection of enforcing the Rule's notification requirements will be approximately $270,000 per year. This estimate is based on the assumption that 3 full attorney work years will be expended to enforce the Rule's requirements related to notification. Clerical and other support services are also included in this estimate.

(15) Program Changes or Adjustments

Not applicable. This is a new information collection.

(16) Statistical Use of Information

Not applicable. There are no plans to publish for statistical use any information required by the Rule.

(17) Display of Expiration Date for OMB Approval

Not applicable.

(18) Exceptions to Certification

Not applicable.

($25.14), tripled it to reflect profits and overhead of a telecommunications firm ($75.42), and multiplied it by 40 hours to yield $3,017.

[16] Staff estimates a cost per call of 25¢ (.05 per minute/per call x 5 minutes per call). Assuming 10,000 calls for each breach, the total estimated telecommunications charges are $2,500.