Supporting Statement for the Health Breach Notification Rule and Form
16 C.F.R. Part 318
(OMB Control No. 3084-0150)

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

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. The Recovery Act required the Federal Trade Commission ("FTC" or "Commission") to adopt a rule implementing the breach notification requirements applicable to vendors of personal health records, "PHR related entities,"[1] and third party service providers. The Commission issued a final rule on August 25, 2009. 74 Fed. Reg. 42,962.

The Health Breach Notification Rule ("Rule"), 16 C.F.R. Part 318, 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 only applies to electronic health records and does not include recordkeeping requirements. The Rule requires third party service providers (i.e., those companies that provide services such as billing or data storage) to notify vendors of personal health records and PHR related entities following the discovery of a breach; those entities in turn must provide notification to consumers and the Commission. To notify the FTC of a breach, the Commission developed a form, which is posted at www.ftc.gov/healthbreach, for entities subject to the Rule to complete and return to the agency.

These notification requirements are subject to the provisions of the Paperwork Reduction Act ("PRA"), 44 U.S.C. Chapter 35. On September 22, 2009, the Office of Management and Budget ("OMB") granted the FTC clearance for these notification requirements through September 30, 2012.

In the Commission's view, it has maximized the practical utility of the breach notification requirements in the Rule, consistent with the requirements of the Recovery Act. Under the Rule, consumers whose information has been affected by a breach of security receive notice of it "without unreasonable delay and in no case later than 60 calendar days" after discovery of the breach. Among other information, the notices must provide consumers with steps they can take to protect themselves from harm. Moreover, the breach notice requirements encourage entities to safeguard the information of their customers, thereby potentially reducing the incidence of harm.

---

[1] "PHR related entity" means an entity, other than a Health Insurance Portability and Accountability Act ("HIPAA")-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that: (1) offers products or services through the website of a vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals personal health records; or (3) accesses information in a personal health record or sends information to a personal health record. 16 C.F.R. § 318.2(f).

The form entities must use to notify the Commission of a security breach requests minimal information, mostly in the manner of replies to check boxes; FTC staff believes that entities would require no more than ten minutes to complete the form, excluding information merely pertaining to an entity's identification and address.[2] The Commission inputs the information it receives from entities into a database that the Commission updates periodically and makes available to the public. The database serves businesses, the public, and policymakers. It provides businesses with information about potential sources of data breaches, which is particularly helpful to those setting up data security procedures. It provides the public with information about the extent of data breaches. Finally, it helps policymakers in developing breach notification requirements in non-health-related areas. Thus, in the Commission's view, the Rule and form have significant practical utility.

(3) Information Technology

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

As noted above, the Commission makes available online the form entities will use to notify the Commission of a breach. Entities can complete it online and then print and send it to a designated FTC official by courier or overnight mail. The form's simplicity and availability at the FTC's website help minimize the burden and cost of its information collection. Although it cannot be filed electronically at present,[3] the form's availability online is consistent with GPEA objectives.

(4) Efforts to Identify Duplication

The FTC has not identified any other federal statutes, rules, or policies currently in effect that conflicts with the Rule or its requirement that affected entities use the form to notify the Commission of a breach. Due to the potential for overlap with the Department of Health and Human Service's ("HHS") Interim Final Rule on "Breach Notification for Unsecured Protected Health Information," which governs breach notification for entities covered by HIPAA, the FTC consulted with HHS to harmonize the two rules, within the constraints of the statutory language. Moreover, for some entities subject to both the HHS and FTC rules, compliance with certain HHS rule requirements shall be deemed compliance with the corresponding provisions of the FTC's rule.

---

[2] Under OMB regulations that implement the PRA, "burden" generally excludes disclosures that require persons to provide or display facts necessary to identify themselves, e.g., identification of the respondent and the respondent's address.

[3] The Commission does not currently accept forms via electronic submission due to technical reasons.

(5) Efforts to Minimize Small Organization Burden

In drafting the Rule, the Commission 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. And, the Commission's creation of a user-friendly form relieves entities of the separate need to design their own to notify the Commission of a breach. The form requests minimal information, mostly in the nature of replies to check boxes. Moreover, the Commission makes the form available on its website, so that entities can fill it out online, print it out, and send it to a designated FTC official.

(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

As required by the PRA, the FTC provided opportunity for public comment before requesting that OMB extend the existing paperwork clearance for the Rule. 44 U.S.C. 3506(c)(2)(A). See 77 Fed. Reg. 31,612 (May 29, 2012). The Commission received no comments in response to the notice.

(9) Payments or Gifts to Respondents

Not applicable.

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

Neither the Rule's breach notification requirements nor the associated form involve disclosure of confidential or sensitive information.

(12) Estimated Annual Hours Burden and Associated Labor Costs

In the event of a data breach, the Rule requires 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; the percentage of such firms that will experience a breach requiring further investigation and, if necessary, the sending of breach notices; and the number of

consumers notified.[4]

The Rule has now been in effect for almost three years,[5] and FTC staff bases its burden estimate on the notifications received from covered entities, which include the number of consumers notified. During 2010 and 2011, two firms informed the Commission of events that resulted in notices to consumers. In 2010, one firm sent notices to 2,094 consumers, and another firm sent notices to 3 consumers. This second firm sent an additional 2,899 notices in 2011 (conveying similar information as in its 2010 notices). This information indicates that an average of about 2,500 consumers per year received notifications over the years 2010 and 2011.

Given the information it has received to date from covered entities, staff bases its current burden estimate on an assumed two breach incidents per year that, together, require the notification of approximately 2,500 consumers.

FTC staff projects that covered firms will require on average, per breach, 100 hours of employee labor to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required report to the Commission, at an estimated cost of $5,268[6] (staff assumes that outside services of a forensic expert will also be required and those services are separately accounted for in the "Estimated Capital/Other Non-Labor Costs Burden" discussion under item (13) below). Based on the estimate that there will be two breaches per year, the annual employee labor cost burden for affected entities to perform these tasks is estimated to be $10,536 (2 breaches x $5,268 each).[7]

Additionally, covered entities will incur labor costs associated with processing calls they may receive in the event of a data breach. The rule requires that covered entities that fail to contact 10 or more consumers because of insufficient or out-of-date contact information must

---

[4] FTC staff's estimates of the annual hours burden and labor costs likely overstate the costs imposed by the Rule because, among other things, they assume, though it is not necessarily so, that all entities subject to the Rule's notification requirements will be required to take all of the steps described below.

[5] The Rule became effective on September 24, 2009. Full compliance was required by February 22, 2010.

[6] Hourly wages throughout this document are based on mean hourly wages found at http://www.bls.gov/news.release/archives/ocwage_03272012.pdf ("Occupational Employment and Wages–May2011," U.S. Department of Labor, released March 2012, Table 1) ("National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2011").

The breakdown of labor hours and costs is as follows: 50 hours of computer and information systems managerial time at $60.41 per hour; 12 hours of marketing managerial time at $60.67 per hour; 33 hours of computer programmer time at $36.54 per hour; and 5 hours of legal staff time at $62.74 per hour.

[7] Labor hours and costs pertaining to reporting to the Commission are subsumed within this total. Specifically, however, staff estimates that covered firms will require per breach, on average, 1 hour of employee labor at a cost of $62 to complete the required form. This is composed of 30 minutes of marketing managerial time at $60.67 per hour, and 30 minutes of legal staff time at $62.74 per hour, with the hourly rates based on the above-referenced Department of Labor table. See note 6 above. Thus, based on 2 breaches per year for which notification may be required, the cumulative annual hours burden for covered entities to complete the notification to the Commission is 2 hours and the annual labor cost would total $124.

provide substitute notice through either a clear and conspicuous posting on their web site or media notice. Such substitute notice must include a toll-free number for the purpose of allowing a consumer to learn whether or not his/her information was affected by the breach.

Individuals contacted directly will have already received this information. Staff estimates that no more than 10 percent of affected consumers will utilize the offered toll-free number. Thus, of the 2,500 consumers affected by a breach annually, staff estimates that 250 may call the companies over the 90 days they are required to provide such access. Staff additionally projects that 250 additional consumers who are not affected by the breach will also call the companies during this period. Staff estimates that processing all 500 calls will require an average of 192 hours of employee labor at a cost of $2,843.[8]

Accordingly, estimated cumulative annual labor costs, excluding outside forensic services, is $13,379.

(13) **Estimated Capital/Other Non-Labor Costs Burden**[9]

Staff estimates that the capital and other non-labor costs associated with the Rule will consist of the following:[10]

1. the services of a forensic expert in investigating the breach; and
2. notification of consumers via e-mail, mail, web posting, or media.

Staff estimates that covered firms (breached entities) will require 30 hours of a forensic expert's time, at a cumulative cost of $3,534. This monetary sum is the product of hourly wages of an information security analyst ($39.27), tripled to reflect profits and overhead for an outside consultant ($117.81), and multiplied by 30 hours. Based on the estimate that there will be 2 breaches per year, the annual cost associated with the services of an outside forensic expert is $7,068.

As explained above, staff estimates that an average of 2,500 consumers per year will receive a breach notification. Given the online relationship between consumers and vendors of

[8] This assumes telephone operator time of 8 minutes per call and information processor time of 15 minutes per call. The cost estimate above is arrived at as follows: 66.7 hours of telephone operator time (8 minutes per call x 500 calls) at $16.48 per hour, and 125 hours of information processor time (15 minutes per call x 500 calls) at $13.95 per hour.

[9] As with its estimates of the annual hours burden and labor costs associated with the Rule, staff believes that its estimate of the Rule's associated capital and other non-labor costs is likely overstated for the same reasons stated in note 3 above.

[10] The instant burden estimate excludes the cost of equipment or other tangible assets of the breached firms, as those assets likely will be used, in any event, for ordinary business purposes.

personal health records and PHR related entities, most notifications will be made by email and the cost of such notifications will be minimal.[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 $2.50 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 $625 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 2,500 consumers per year receiving breach notification, the estimated total annual cost of website notice will be $150, and the estimated total annual cost of media notice will be $75, yielding an estimated total annual cost for all forms of notice to consumers of $225.

In sum, the total estimate for non-labor costs is $7,918: $7,068 (services of a forensic expert) + $850 (costs of notifying consumers).

(14) Estimate of Cost to Federal Government

Staff estimates that the cost to the FTC Bureau of Consumer Protection of enforcing the Rule's notification requirements will be approximately $75,000 per year. This estimate is based on the assumption that 50% of one attorney work year will be expended to enforce the Rule's requirements related to notification. Employee benefits, as well as clerical and other support services are also included in this estimate.

(15) Program Changes or Adjustments

At the time the Rule was issued, insufficient data was available about the incidence of breaches in the PHR industry. Accordingly, staff based its burden estimate on data pertaining to

---

[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 $2.50 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. In studies conducted for subsequent years, the Ponemon Institute does not report this level of detail, but it notes that overall notification costs have not increased.

private sector breaches across multiple industries. Staff estimated that there would be 11 breaches per year requiring notification of 232,000 consumers. As discussed above, because the Rule has now been in effect for almost three years, staff is now able to base the burden estimate on the actual notifications received from covered entities, which include the number of consumers notified.

As discussed above, the notifications received indicate that an average of 2,500 consumers per year received notifications over the years 2010 and 2011. This number is about one percent of the figure staff had previously projected would require notification. Staff has updated the burden estimate based on these new figures.

Further, staff's previous burden estimate included in the cost of a toll-free number, the costs associated with obtaining a T1 line (a specific type of telephone line that can carry more data than traditional telephone lines) and services such as queue messaging that are necessary when handling large call volumes. Because staff's current estimate does not include large projected call volumes, staff believes that affected entities will not need these additional services and equipment and did not include those cost estimates here.

(16) Plans for Tabulation and Publication

There are no plans to publish for statistical use any information required by the Rule, but the Commission intends to input the information it receives from entities that have completed the associated form into a database, which it will update periodically and make publicly available.

(17) Display of Expiration Date for OMB Approval

Not applicable.

(18) Exceptions to Certification

Not applicable.