BILLING CODE: 6750-01-S

FEDERAL TRADE COMMISSION

Agency Information Collection Activities;

Proposed Collection; Comment Request

AGENCY: Federal Trade Commission (FTC or Commission).

ACTION: Notice.

SUMMARY: The information collection requirements described below will be submitted to the Office of Management and Budget (OMB) for review, as required by the Paperwork Reduction Act (PRA). The FTC seeks public comment on its proposal to extend, for three years, the current PRA clearance for information collection requirements contained in the Health Breach Notification Rule. That clearance expires on March 31, 2019.

DATES: Comments must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Interested parties may file a comment online or on paper by following the instructions in the Request for Comments part of the SUPPLEMENTARY INFORMATION section below. Write "Paperwork Reduction Act: FTC File No. P072108" on your comment, and file your comment online at https://www.regulations.gov by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania

Avenue, NW, Suite CC-5610 (Annex J), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610 (Annex J), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Robin Wetherill, 202-326-2220, Attorney, Privacy & Identity Protection, Bureau of Consumer Protection, 600 Pennsylvania Ave., NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION:

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 included provisions to advance the use of health information technology and, at the same time, strengthen privacy and security protections for health information. The Act required the FTC to adopt a rule implementing the breach notification requirements applicable to vendors of personal health records, "PHR related entities," and third-party service providers, and the Commission issued a final rule on August 25, 2009. 74 FR 42962.

The Health Breach Notification Rule (Rule), 16 CFR Part 318 (OMB Control Number 3084-0150), 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. Under the Rule, consumers whose information has been affected by a breach receive notice "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. To notify the FTC of a breach, the Commission developed a simple, two-page form requesting minimal information and consisting mainly of check boxes, which is posted at www.ftc.gov/healthbreach. For breaches involving the health information of 500 or more individuals, entities must notify the Commission as soon as possible, and in any event no later than ten business days after discovering the breach. Entities may report all breaches involving the information of fewer than 500 individuals in an annual submission for the calendar year. The Commission uses entities' notifications to compile a list of breaches affecting 500 or more individuals that is publicly available on the FTC's website. The list provides businesses with information about potential sources of data breaches, which is helpful to those developing data security procedures. It also provides the public with information about the extent of data breaches.

The Rule also 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 only applies to electronic health records and does not include recordkeeping requirements.

These notification requirements are subject to the provisions of the PRA, 44 U.S.C. Chapter 35. Under the PRA, federal agencies must get OMB approval for each collection of information they conduct, sponsor, or require. "Collection of information" means agency requests or requirements to submit reports, keep records, or provide information to a third party. 44 U.S.C. 3502(3); 5 CFR 1320.3(c). As required by Section 3506(c)(2)(A) of the PRA, the FTC

is providing this opportunity for public comment before requesting that OMB extend the existing PRA clearance for the information collection requirements associated with the Rule.

The FTC invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (2) the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on those who are to respond. All comments must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Burden Estimates

The PRA burden of the Rule's requirements depends 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. The annual hours and cost estimates below likely overstate the burden because, among other things, they assume, though it is not necessarily so, that all covered firms experiencing breaches subject to the Rule's notification requirements will be required to take all of the steps described below.

The analysis may also overstate the burden of the Rule's requirements because it assumes that covered firms would not take any of the steps described were it not for the requirements of the Rule. For example, the analysis incorporates labor costs associated with understanding what

information has been breached. It seems likely that some firms would incur such costs even in the absence of the Rule's requirements because the firms are independently interested in identifying, understanding, and remediating security risks. A company that investigates, for its own purposes, what information has been breached is unlikely to fully duplicate the costs of that investigation in complying with the Rule. Therefore, it may not be correct in all cases that complying with the Rule results in added labor costs for this activity. Nevertheless, in order to allow for a complete understanding of all the potential costs associated with compliance, these costs are included in this analysis.

At the time the Rule was issued in 2009, insufficient data was available about the incidence of breaches in the PHR industry. Accordingly, staff based its burden estimate on data pertaining to private sector breaches across multiple industries. Staff estimated that there would be 11 breaches per year requiring notification of 232,000 consumers.

In 2016, based on available data from the years 2010 through 2014, staff arrived at new estimates, projecting an average of two breaches per year affecting a total of 40,000 individual consumers.

The Rule has now been in effect for over eight years, and new data regarding the number and scale of reported breaches from 2015 through 2017 allow staff to update its burden estimates. A review of the breach reports received by the FTC from 2010 through 2017 reveals that there are two primary categories of breaches reported: (1) "single-person breaches," incidents in which a single individual's information is potentially compromised; and (2) what are hereafter described as "major breaches," in which multiple—and typically, many—individuals are

affected. These two categories of breaches are addressed separately in this analysis because the frequency and costs of the categories differ significantly.

Nearly all of the submissions received between 2010 and 2017—over 99.99% of them—reported single-person breaches related to an individual's loss of control over his or her login credentials. The rate of such breaches has increased significantly since the Rule went into effect; the year-to-year average rate of increase during this period was nearly 70%. Whereas from 2011 to 2014 the average annual number of single-person breaches was 7,502, from 2014 to 2017 the average was almost 15,000. Assuming that this rate of increase continues, staff estimates that between 2019 and 2022 the agency will receive, on average, about 25,000 single-person breach reports per year.

By contrast, major breach reports are quite infrequent. On average, the FTC receives one major breach report approximately every two and a half years, with an average of approximately 200,000 persons affected. Given the low frequency at which major breaches occur, FTC staff are unable to identify any meaningful trends in the frequency of major breach reports. FTC staff has not identified any existing research allowing us to make specific projections about future variation in the frequency of major breaches. Consequently, FTC staff has assumed that the average frequency and scale of major breaches will remain more or less static. Staff's calculations are based on the estimate that a major breach will occur approximately every two and a half years and that 200,000 people will be affected by each major breach, for an annual average of 80,000 individuals affected per year.

Estimated Annual Burden Hours: 4,779

As explained in more detail within the next section, FTC staff projects that the employee time required for each single-person breach is quite minimal because the processes for notifying consumers are largely automated and single-person breaches can be reported to the FTC in an aggregate annual notification using the FTC's two-page form. On average, staff estimates that covered firms will require approximately 20 seconds of employee labor per single-person breach. With an estimated 25,000 single-person breaches per year, the total estimated burden hours for single-person breaches is approximately 139 hours.

For each major breach, covered firms will require on average 100 hours of employee labor to determine what information has been breached, the identification of affected customers, preparation of the breach notice, and submission of the required report to the Commission. Based on staff's estimate that one major breach occurs every two and a half years, the average annual burden of major breaches amounts to 40 hours per year.

Additionally, covered firms will incur labor costs associated with processing calls they may receive in the event of a major breach. The Rule requires that covered firms that fail to contact 10 or more consumers because of insufficient or out-of-date contact information must 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 200,000 consumers affected by a major breach, staff estimates that 20,000 may call

the companies over the 90 days they are required to provide such access. Staff additionally projects that 10,000 additional consumers who are not affected by the breach will also call the companies during this period. Staff estimates that processing all 30,000 calls will require an average of 11,500 hours of employee labor resulting in an average annual burden of 4,600 labor hours.

Given the low frequency of major breaches, the annual average requirement for major breaches is 4,640 hours.

The combined annual hours burden for both single-person and major breaches therefore is 4,779 (4,640 + 139).

Estimated Annual Labor Costs: $91,836

For each single-person breach, FTC staff estimates that the average 20 seconds of employee labor to provide (likely automated) notification to affected individuals and produce an annual breach notification for submission to the FTC will cost approximately $0.27 per breach. With an estimated 25,000 single-person breaches per year, the annual labor costs associated with all single-person breaches come to $6,570.

For major breaches, FTC staff projects that the average 100 hours of employee labor costs (excluding outside forensic services, discussed below as estimated non-labor costs) to determine what information has been breached, identify the affected customers, prepare the breach notice, and report to the Commission will cost an average of $61.66 per hour for a total of $6,166.[1]

[1] Hourly wages throughout this document are based on mean hourly wages found at http://www.bls.gov/news.release/ocwage.htm ("Occupational Employment and Wages–May 2017," U.S.

Based on an estimated one breach every two and a half years, the annual employee labor cost burden for affected entities to perform these tasks is $2,466.

Additionally, staff expects covered firms will require, for each major breach, 11,500 hours of labor associated with answering consumer telephone calls at a cost of $207,000.[2] Since a major breach occurs approximately every two and a half years, the average annual burden of 4,600 labor hours results in annualized labor cost of approximately $82,800.

Accordingly, estimated cumulative annual labor costs, excluding outside forensic services, for both single-person and major breaches, is $91,836 ($82,800 + $2,466 + $6,570).

Estimated Annual Capital and other Non-Labor Costs: $29,446

Commission staff estimates that capital and other non-labor costs associated with single-person breaches will be negligible. Companies generally use automated notification systems to notify consumers of single-person breaches. Automated notifications are typically delivered by email or other electronic methods. The costs of providing such electronic notifications are minimal.

Commission staff anticipates that capital and other non-labor costs associated with major breaches will consist of the following:

Department of Labor, released March 2018, Table 1 ("National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2017").

The breakdown of labor hours and costs is as follows: 50 hours of computer and information systems managerial time at approximately $72 per hour; 12 hours of marketing manager time at $70 per hour; 33 hours of computer programmer time at $42 per hour; and 5 hours of legal staff time at $68 per hour.

[2] The cost of telephone operators is estimated at $18/hour.

1. services of a forensic expert in investigating the breach;

2. notification of consumers via e-mail, mail, web posting, or media; and

3. the cost of setting up a toll-free number, if needed.

Staff estimates that, for each major breach, covered firms will require 240 hours of a forensic expert's time, at a cumulative cost of $34,560 for each breach. This estimate is based on a projection that an average major breach will affect approximately 20 machines and that a forensic analyst will require about 12 hours per machine to conduct his or her analysis. The projected cost of retaining the forensic analyst consists of the hourly wages of an information security analyst ($48), tripled to reflect profits and overhead for an outside consultant ($144), and multiplied by 240 hours. Based on the estimate that there will be one major breach every two and a half years, the annual cost associated with the services of an outside forensic expert is $13,824.

As explained above, staff estimates that an average of 200,000 consumers will be entitled to notification of each major breach. 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 minimal.

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 a mailed notice is $0.11 for the paper and envelope, and $0.55 for a first class stamp. Assuming that vendors of personal health records and PHR related entities will need to notify by postal mail 10 percent of the 200,000 customers whose information is

breached, the estimated cost of this notification will be $13,200 per breach. The annual cost will be around $5,280.

In addition, vendors of personal health records and PHR related entities may need to notify consumers by posting a message on their home page, or by providing media notice. Staff estimates the cost of providing notice via website posting to be $0.08 per breached record, and the cost of providing notice via published media to be $0.04 per breached record. Applied to the above-stated estimate of 200,000 affected consumers, the estimated total cost of website notice will be $16,000, and the estimated total cost of media notice will be $8,000, yielding an estimated total per-breach cost for both forms of notice to consumers of $24,000. Annualized, this number is approximately $9,600 per year.

Finally, staff estimates that the cost of providing a toll-free number will depend on the costs associated with T1 lines sufficient to handle the projected call volume and the cost of obtaining a toll-free telephone number. Based on industry research, staff projects that affected entities may need two T1 lines at a cost of $1,800 for the 90-day period. In addition, staff estimates the cost of obtaining a dedicated toll-free line to be $100 per month. Accordingly, staff projects that the cost of obtaining two toll-free lines for 90 days will be $2,400. The total annualized cost for providing a toll-free number will be $960.

In sum, the total annual estimate for non-labor costs associated with major breaches is $29,664: $13,824 (services of a forensic expert) + $5,280 (cost of mail notifications) + $9,600 (cost of website and media notice) + $960 (cost of providing a toll-free number). Negligible non-labor costs are associated with single-person breaches.

The total estimated PRA annual cost burden is $91,836 for labor costs and $29,446 for non-labor costs, totaling approximately $121,500.

Request for Comments

You can file a comment online or on paper. [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Write "Paperwork Reduction Act: FTC File No. P072108" on your comment. Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it through the https://www.regulations.gov website by following the instructions on the web-based form provided. Your comment -- including your name and your state -- will be placed on the public record of this proceeding, including at the https://www.regulations.gov website.

If you file your comment on paper, write "Paperwork Reduction Act: FTC File No. P072108" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC–5610 (Annex C), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610, Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at www.regulations.gov, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include

any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . . is privileged or confidential" – as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. See FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at www.regulations.gov, we cannot redact or remove your comment, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. You can find more information, including routine uses permitted by the Privacy Act, in the Commission's privacy policy, at https://www.ftc.gov/site-information/privacy-policy.

Heather Hippsley,
Deputy General Counsel.
[FR Doc. 2019-01530 Filed: 2/7/2019 8:45 am; Publication Date: 2/8/2019]