addition four recommendations from the Media Working Group regarding political advertising, spectrum, the Emergency Alert System, and privacy will also be considered. The Committee may also consider other recommendations from its working groups, and may also receive briefings from FCC staff and outside speakers on matters of interest to the Committee. A limited amount of time will be available on the agenda for questions and comments from the public.

Meetings of the Committee are also broadcast live with open captioning over the Internet from the FCC Live Web page at *www.fcc.gov/live/*.

Simultaneous with the webcast, the meeting will be available through Accessible Event, a service that works with a web browser to make presentations accessible to people with disabilities. Persons wishing to attend through Accessible Event can listen to the audio and use a screen reader to read displayed documents, and can watch the video with open captioning. The Web site to access Accessible Event is *http://accessibleevent.com*. The Web page prompts for an Event Code which is: 005202376. To learn about the features of Accessible Event, consult its User's Guide at: *http://accessibleevent.com/doc/user_guide/*.

The public may ask questions of presenters via email *livequestions@fcc.gov* or via Twitter using the hashtab #fcclive. In addition, the public may also follow the meeting on Twitter @fcc or via the Commission's Facebook page at *www.facebook.com/fcc*.

Alternatively, written comments to the Committee may be sent to: Scott Marshall, Designated Federal Officer of the Committee at the address provided above.

The meeting is open to the public and the site is fully accessible to people using wheelchairs or other mobility aids. Sign language interpreters, open captioning, assistive listening devices, and Braille copies of the agenda and handouts will be provided on site.

Other reasonable accommodations for people with disabilities are available upon request. The request should include a detailed description of the accommodation needed and contact information. Please provide as much advance notice as possible; last minute requests will be accepted, but may be impossible to fill. Send an email to *fcc504@fcc.gov* or call the Consumer and Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (TTY).

Federal Communications Commission.

Kris Anne Monteith,

Acting Chief, Consumer and Governmental Affairs Bureau.

[FR Doc. 2012–12956 Filed 5–25–12; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL MINE SAFETY AND HEALTH REVIEW COMMISSION

Sunshine Act Meeting Notice

May 22, 2012.

TIME AND DATE: 10:00 a.m., Thursday, May 31, 2012.

PLACE: The Richard V. Backley Hearing Room, 9th Floor, 601 New Jersey Avenue NW., Washington, DC.

STATUS: Open.

MATTERS TO BE CONSIDERED: The Commission will consider and act upon the following in open session: *Secretary of Labor* v. *Shamokin Filler Co.,* Docket Nos. PENN 2009–775, et al. (Issues include whether the Mine Safety and Health Administration has regulatory jurisdiction over the company's facility.)

Any person attending this meeting who requires special accessibility features and/or auxiliary aids, such as sign language interpreters, must inform the Commission in advance of those needs. Subject to 29 CFR 2706.150(a)(3) and 2706.160(d).

CONTACT PERSON FOR MORE INFO: Jean Ellen (202) 434–9950/(202) 708–9300 for TDD Relay/1–800–877–8339 for toll free.

Emogene Johnson,

Administrative Assistant.

[FR Doc. 2012–13024 Filed 5–24–12; 4:15 pm]

BILLING CODE 6735–01–P

FEDERAL RESERVE SYSTEM

Change in Bank Control Notices; Acquisitions of Shares of a Bank or Bank Holding Company

The notificants listed below have applied under the Change in Bank Control Act (12 U.S.C. 1817(j)) and § 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire shares of a bank or bank holding company. The factors that are considered in acting on the notices are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The notices are available for immediate inspection at the Federal Reserve Bank indicated. The notices also will be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received not later than June 12, 2012.

A. Federal Reserve Bank of St. Louis (Glenda Wilson, Community Affairs Officer) P.O. Box 442, St. Louis, Missouri 63166–2034:

1. *Eddie D. Franklin,* Columbia, Kentucky; to retain control of United Citizens Bancorp, Inc., and thereby indirectly retain control of United Citizens Bank of Southern Kentucky, both in Columbia, Kentucky.

Board of Governors of the Federal Reserve System, May 23, 2012.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. 2012–12915 Filed 5–25–12; 8:45 am]

BILLING CODE 6210–01–P

FEDERAL TRADE COMMISSION

Agency Information Collection Activities; Proposed Collection; Comment Request; Extension

AGENCY: Federal Trade Commission (''FTC'' or ''Commission'').

ACTION: Notice.

SUMMARY: The FTC intends to ask the Office of Management and Budget (''OMB'') to extend through September 30, 2015, the current Paperwork Reduction Act (''PRA'') clearance for the information collection requirements in the Health Breach Notification Rule. That clearance expires on September 30, 2012.

DATES: Comments must be filed by July 30, 2012.

ADDRESSES: Interested parties may file a comment online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write ''Health Breach Notification Rule, PRA Comments, P–125402'' on your comment and file your comment online at *https://ftcpublic.commentworks.com/ftc/healthbreachnotificationPRA* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Room H–113 (Annex J), 600 Pennsylvania Avenue NW, Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Amanda Koulousias, Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania

Avenue NW., Washington, DC 20580, (202) 326–2252.

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 includes 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,'' [1] 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, 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 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. 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 PRA, 44 U.S.C. Chapter 35. Under the PRA, Federal agencies must get OMB approval for each collection of information they conduct or sponsor. ''Collection of information'' includes 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). On September 22, 2009, OMB granted the FTC clearance (under Control Number 3084–0150) for these notification requirements through September 30, 2012. As required by the PRA, the FTC is providing this opportunity for public comment before requesting that OMB extend the existing paperwork clearance for the Rule. 44 U.S.C. 3506(c)(2)(A).

The FTC invites comments on: (1) Whether the notification requirements in the Rule and associated form are necessary, including whether the information will be practically useful; (2) the accuracy of our burden estimates, including whether the methodology and assumptions used are valid; (3) how to improve the quality, utility, and clarity of the required notifications; and (4) how to minimize the burden of providing the required information to consumers and to the agency. All comments should be filed as prescribed in the **ADDRESSES** section above, and must be received on or before July 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.

The form entities must use to inform the Commission of a security breach requests minimal information, mostly in the form of replies to check boxes; thus, entities do not require extensive time to complete it. The Commission inputs the information it receives from entities into a database that the Commission updates periodically and makes available to the public. The publicly-available 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.

Burden Statement:

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 breaches subject to the Rule's notification requirements will be required to take all of the steps described below.

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 private sector breaches across multiple industries. Staff estimated that there would be 11 breaches per year requiring notification of 232,000 consumers.[2]

As described above, the Rule requires covered entities that have suffered a breach to notify the Commission. Since the Rule has now been in effect for over two years,[3] staff is now able to base the burden estimate on the actual notifications received from covered entities, which include the number of consumers notified. Accordingly, staff has used this information to update its burden estimate.

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 (conveying similar information as in its 2010 notices) in 2011.

This information indicates that an average of about 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. Among other things, staff believes that this lower incidence rate may be due to a reported low utilization by consumers of PHR vendors.[4] Among the barriers cited to adoption of PHRs are consumer resistance due to concerns about privacy and the lack of consumer

[1] ''PHR related entity'' means an entity, other than a 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 Web site of a vendor of personal health records; (2) offers products or services through the Web sites 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 CFR 318.2(f).

[2] 74 FR at 42977.

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

[4] For example, the New York Times reported in June 2011 that Google was ending its PHR service after failing to attract sufficient users. Steve Lohr, ''Google to End Health Records Service After It Fails to Attract Users,'' New York Times, June 24, 2011, available at *http://www.nytimes.com/2011/06/25/technology/25health.html?_r=1&emc=eta1.* The article reported that according to a survey performed by the research firm IDC Health Insights, ''7 percent of consumers had tried online personal health records, and fewer than half of those continued to use them.''

motivation to manage their own health data.[5]

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.

Estimated Annual Labor Costs: $13,379.

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 under ''Estimated Annual Non-Labor Costs'' below). Based on an estimated 2 breaches per year, the annual employee labor cost burden for affected entities to perform these tasks is $10,536.[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 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.

Estimated Annual Non-Labor Costs: $7,918.

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

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

2. Notification of consumers via email, mail, web posting, or media.[9]

Staff estimates that covered firms (breached entities) will require 30 hours of a forensic expert's time, at a cumulative cost of $3,534 for each breach. This 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 personal health records and PHR related entities, most notifications will be made by email and the cost of such notifications will be minimal.[10]

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.[11] Assuming that vendors of personal health records and PHR related entities will need to notify by postal mail 10 percent of the 2,500 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 Web site posting to be 6 cents per breached record, and the cost of providing notice via published media to be 3 cents per breached record.[12] Applied to the above-stated estimate of 2,500 affected consumers, the estimated total annual cost of Web site 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).

Request for Comment: You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before July 30, 2012. Write ''Health Breach Notification Rule, PRA Comments, P–125402'' on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including to the extent practicable, on the public Commission

---

[5] *Id.; see also,* Wes Richsel and Robert H. Booz, ''Google Health Shutdown Underscores Uncertain Future of PHRs,'' Gartner, July 1, 2011, available at *http://www.gartner.com/id=1736829.*

[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—May 2011,'' 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 manager 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, staff estimates that covered firms will require per breach, on average, 1 hour of employee labor at an approximate 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, *supra.* 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 is $124.

[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 × 500 calls) at $16.48 per hour, and 125 hours of information processor time (15 minutes per call × 500 calls) at $13.95 per hour.

[9] Staff's earlier estimate also included 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. Since 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.

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

[11] 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.

[12] 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.

Web site, at *http://www.ftc.gov/os/publiccomments.shtm.* As a matter of discretion, the Commission tries to remove individuals' home contact information from comments before placing them on the Commission Web site.

Because your comment will be made public, you are solely responsible for making sure that your comment does not include any sensitive personal information, like anyone'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, like medical records or other individually identifiable health information. In addition, do not include any ''[t]rade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential'' as provided in 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). In particular, do not include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you have to follow the procedure explained in FTC Rule 4.9(c).[13] Your comment will be kept confidential only if the FTC General Counsel, in his or her sole discretion, grants your request in accordance with the law and the public interest.

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 at *https://ftcpublic.commentworks.com/ftc/healthbreachnotificationPRA,* by following the instructions on the web-based form. If this Notice appears at *http://www.regulations.gov/#!home,* you also may file a comment through that Web site.

If you file your comment on paper, write ''Health Breach Notification Rule, PRA comments, P–125402'' on your comment and on the envelope, and mail or deliver it to the following address: Federal Trade Commission, Office of the Secretary, Room H–113 (Annex J), 600 Pennsylvania Avenue NW., Washington, DC 20580. If possible, submit your paper comment to the Commission by courier or overnight service.

Visit the Commission Web site at to read this Notice and the news release describing it. 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 July 30, 2012. You can find more information, including routine uses permitted by the Privacy Act, in the Commission's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm.*

Christian S. White,

Acting General Counsel.

[FR Doc. 2012–12863 Filed 5–25–12; 8:45 am]

BILLING CODE 6750–01–P

[13] 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), 16 CFR 4.9(c).

GENERAL SERVICES ADMINISTRATION

[Notice–FMR–2012–G–03; Docket No. 2012–0004, Sequence 3]

Improving Mail Management Policies, Procedures, and Activities

AGENCY: Office of Governmentwide Policy, General Services Administration (GSA).

ACTION: Notice of FMR Bulletin G–03.

SUMMARY: The General Services Administration (GSA) has issued Federal Management Regulation (FMR) Bulletin G–03 which provides guidance to Executive Branch agencies for improving mail management policies, procedures, and activities. FMR Bulletin G–03 and all other FMR Bulletins may be found at *http://www.gsa.gov/portal/content/102955#MailManagement.*

DATES: *Effective Date:* This notice is effective May 29, 2012.

Applicability Date: This notice applies to Mail Management Policy performed on or after May 2, 2012.

FOR FURTHER INFORMATION CONTACT: Mr. Derrick Miliner, Office of Governmentwide Policy (MAF), Office of Asset and Transportation Management, General Services Administration at (202) 273–3564 or via email at *derrick.miliner@gsa.gov.* Please cite FMR Bulletin G–03.

SUPPLEMENTARY INFORMATION: In an effort to cut waste, increase sustainable practices, remain in compliance with Executive Orders and the Federal Management Regulation, Federal agencies, internal policies should address the four requirements described in this bulletin. These include: (1) Consolidation of mail including presorting; (2) reductions of hard copy agency-to-agency mailings; (3) sustainable mail practices; and (4) secure mail for teleworkers.

Dated: May 16, 2012.

Carolyn Austin Diggs,

Assistant Deputy Associate Administrator, Office of Asset and Transportation Management, Office of Governmentwide Policy.

[FR Doc. 2012–12985 Filed 5–25–12; 8:45 am]

BILLING CODE 6860–14–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

[Document Identifier CMS–1500 (08/05) and CMS–1500 (2/12)]

Agency Information Collection Activities: Proposed Collection; Comment Request

AGENCY: Centers for Medicare & Medicaid Services, HHS.

In compliance with the requirement of section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995, the Centers for Medicare & Medicaid Services (CMS) is publishing the following summary of proposed collections for public comment. Interested persons are invited to send comments regarding this burden estimate or any other aspect of this collection of information, including any of the following subjects: (1) The necessity and utility of the proposed information collection for the proper performance of the agency's functions; (2) the accuracy of the estimated burden; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) the use of automated collection techniques or other forms of information technology to minimize the information collection burden.

1. *Type of Information Collection Request:* Reinstatement without change of a previously approved collection; *Title of Information Collection:* Health Insurance Common Claims Form and Supporting Regulations at 42 CFR part 424, Subpart C; *Use:* The Form CMS–1500 answers the needs of many health insurers. It is the basic form prescribed by CMS for the Medicare program for