Comments of the World Privacy Forum

March 27, 2009

Via https://secure.commentworks.com/ftc-CVSCaremark and www.regulations.gov

Federal Trade Commission
Office of the Secretary
Room H-135
600 Pennsylvania Avenue, NW
Washington DC 20580

Re: CVS Caremark, File No. 072 3119, 74 Federal Register 12870-12871

The World Privacy Forum offers comments on the proposed consent order in *FTC File No. 072 3119, In the Matter of CVS Caremark Corporation*. The notice appeared on March 25, 2009, 74 Federal Register 12870-12871.

The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, including issues related to health care. See <http://www.worldprivacyforum.org>.

We appreciate that the FTC has taken this action; consumer privacy breaches in the area of sensitive medical records can bring much harm to impacted individuals. Regarding the consent order, we have several basic objections to the consent order as it stands in its current form. We are hopeful that the FTC will consider our comments and the potential for harm, and as a result make adjustments in the final consent order.

I. Fundamental Facts Missing

Neither the complaint nor the consent order contains sufficient facts to permit any member of the public to assess whether the Commission's proposed consent order is reasonable. The only facts in the consent order about CVS's conduct that gave rise to the complaint are these:

> 8. As a result of the failures set forth in Paragraph 7, CVS pharmacies discarded materials containing personal information in clear readable text (such as prescriptions, prescription bottles, pharmacy labels, computer printouts, prescription purchase refunds, credit card receipts, and employee records) in unsecured, publicly-accessible trash dumpsters on numerous occasions. For example, in July 2006 and continuing into 2007, television stations and other media outlets reported finding personal information in unsecured dumpsters used

> by CVS pharmacies in at least 15 cities throughout the United States. The personal information found in the dumpsters included information about both CVS's customers and its employees. When discarded in publicly-accessible dumpsters, such information can be obtained by individuals for purposes of identity theft or the theft of prescription medicines.

http://www.ftc.gov/os/caselist/0723119/090218cvscmpt.pdf.

The analysis released by the Commission essentially repeats the same summary of the facts. http://www.ftc.gov/os/caselist/0723119/090218cvsanal.pdf.

The lack of facts is problematic. Did CVS's conduct result in the disclosure of records about one million patients? We do not know from the Commission's disclosures in this case. Did CVS's conduct result in the disclosure of records about one hundred patients? We would like to think that there might be a greater consequence for a violation that affected a large number of patients, but we have no way of being able to make a judgment here due to the lack of facts.

How many different CVS locations were guilty of the breach of security? How many different locations were accused of a breach of security? The public does not know according to these documents, and we do not know.

How long did CVS dispose of patient records using methods that violate the HIPAA privacy and security rules and the FTC Act? Did the conduct last for a week? A month? Four years? Where was this specifically happening? We do not know, and we do not know what the Commission found out beyond the media reporting. The only facts are a few sentences summarizing what unnamed television stations and other media outlets found. The Commission did not provide a link to any of the reporting.

Did CVS' breach of security result in any cases of medical identity theft or financial identity theft? There is no information in the consent order or in other Commission documents.

In order to learn more about this case, we searched for the "television stations and other media outlets" referred to in the Commission documents. In Appendix A we attach to these comments a small portion of the public information pertaining to the extensive investigative reporting WTHR-TV (Indianapolis, Indiana) did about CVS data breaches of medical information, which led to at least two state cases (Indiana, Texas). This information appears on the television station's website. We focused on information provided by this media outlet because WTHR-TV asserted on February 18, 2009, that its reporting led to a "record $2.25M HIPAA settlement," additionally quoting an HHS official who stated that the television station's 2006 investigative reporting "formed the basis of the settlement." (See <http://www.wthr.com/Global/story.asp?s=9868296>, WTHR investigation leads to record $2.25M HIPAA settlement, posted Feb. 18, 2009.) We cannot assert that all of the facts reported by the television station are correct.

Of course, CVS is welcome to respond to these comments and to the television station's reporting. We recognize that supplementing the public record in this manner is unusual, however, we are unable to determine or know what the facts are from the consent order alone.

II. No Public Assessment Made Available

There is no requirement in the consent order that CVS or the Commission make any information public about the required Assessment. As a result, the public will not have the opportunity in the future to determine if CVS is complying with the requirements of the consent order to have an Assessment or if CVS is meeting its security obligations as set forth in the consent order. We recognize that some of the information in the Assessment may be proprietary or unsuited for public release.

However, the public deserves increased transparency in this matter, and is entitled to know who is conducting the Assessment and to know the broad conclusions reflected in the Assessment. We additionally think it would be very helpful if the staff would make public its own summary of the Assessment so that the public can have some additional way of reviewing and analyzing the Assessment.

III. No Penalty in the FTC's First Health Provider Case

The Commission seeks no civil penalty. We recognize that there is value to the required Assessment, but the Assessment requires little more than a conscientious company would undertake otherwise. The Commission's Assessment may contain a few additional bells and whistles.

Based on the facts as reported by the television station – and there may be additional facts that reveal even greater lapses of security – the World Privacy Forum believes that the Commission should have sought an additional monetary penalty. At a minimum, the Commission should have explained why it did not seek a monetary penalty.

The World Privacy Forum previously objected to a settlement without a penalty in two cases: In the Matter of Milliman, Inc., FTC File No. 062-3189, Docket No. C-4213, and In the Matter of Ingenix, Inc., FTC File No. 062-3190, Docket No. C-4214. In its response, the Commission said:

> Among other remedies, the Commission may seek civil penalties in the event of a "knowing violation which constitutes a pattern or practice of violations." To that end, and as specified by the FCRA, the Commission considered whether the alleged violations were knowing and constituted a pattern or practice of violations. The Commission also considered the factors set forth in sections 621(A)(2)(A) and (B) of the FCRA for determining the amount of a civil penalty, including the respondent's degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.
> http://www.ftc.gov/os/caselist/0623189/080212letter.pdf

Were any of these factors considered in this case? We do not know. The Commission did not explain why it did not seek a civil penalty in this case. If we had a better statement of facts, we could probably assert with greater assurance that there was a knowing violation and a pattern or practice of violations. However, it appears highly likely that both are present in this case.

How will the public be able to assess the Commission's decision to settle the next case? The Commission has an obligation to inform the public why it takes a particular action or fails to do so in each case. The public (and those subject to the Commission's jurisdiction) are entitled to know how the Commission reaches a particular result. We need a scale to assess the Commission's actions, and the Commission needs to provide that scale. We do not seek mathematic evaluation here, but an evaluation of the factors that the Commission itself identified in the above quote would be helpful.

We are aware that the Department of Health and Human Services has negotiated a $2.25 million settlement with CVS. However, we do not see the settlement that HHS reached as particularly relevant to the issue of the proper civil penalty for violation of the law that the Commission enforces. It is a separate law, and the conduct of CVS apparently violated both laws. Two separate penalties would be appropriate.

We are especially concerned that as the FTC is being given greater responsibilities in policing the Personal Health Record data breach area through the newly enacted ARRA, that the FTC be seen as strong and as an agency that will take substantive action in the case of breaches in this most sensitive of information areas.

Because this case inadvertently becomes the first case of this kind, we are concerned that in the next case – one where the conduct violated only the FTC Act and not HIPAA – the defendant will argue forcefully that the Commission sought no penalty on CVS, and will use this case to successfully argue that the new defendant should be treated similarly.

IV. No Remedies For Patients Provided

We find nothing in the consent order that offers any remedy, relief, assistance, or support to a patient who may have been injured because of CVS's security breach. We have no explanation from Commission documents why the settlement in this case does not impose upon CVS an obligation to notify patients, provide assistance to those who may have been injured, and to compensate those who were injured. The television reports suggest that there were patients who suffered direct consequences as a result of CVS's lapses. Why is there nothing in the consent order for them?

Again, we urge the Commission to take another look at this consent order. It will set a long precedent in an area of critical importance to consumers, one which carries great potential for harm, and one which has become now much more officially a part of the Commission's purview.

We note that the Federal Register notice for this case was published March 25, 2009, with comments due March 27, 2009. We find this to be an unusually short comment period.

Thank you for considering our comments, and thank you for the opportunity to comment.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum
www.worldprivacyforum.org
760-268-0094

Appendix A.

I. Partial List of Drugstores from WTHR Investigation

This is a partial list of drugstores where "13 Investigates" found customers' personal information in unsecured dumpsters. See: <http://wthr.images.worldnow.com/images/incoming/html/wherewefoundit.htm> for the complete article and list.

DRUGSTORES WHERE 13 INVESTIGATES FOUND CUSTOMERS' PERSONAL INFORMATION IN UNSECURED DUMPSTERS (BY PHARMACY)

CVS / OSCO

City	Location	Date
Boston	587 Boylston	10/12
Chicago Metro	5158 N. Lincoln Ave.	10/10
	1539 Clavey Rd. (Highland Park)	9/1
	101 Asbury (Evanston)	9/6
Cleveland Metro	6301 Harvard	8/7
	2160 Lee Rd. (Cleveland Heights)	8/7
	1331 Youngstown-Warren Rd (Niles)	8/9
Detroit Metro	Michigan & Martin	8/5
	13th & Woodward (Royal Oak)	8/5
	13250 Ford Rd. (Dearborn)	8/5
Dallas Metro	5111 Greenville Ave.	8/30
	3012 Mockingbird Ave.	8/30
	Preston-Forest Shopping Center	8/30
	3401 W Walnut Hill Lane (Irving)	8/30

Indianapolis Metro	5502 W 38th St.	6/28
	5611 Georgetown Rd.	6/28
	5472 Georgetown Rd. (former Osco)	6/28
	1225 W 86th St.	6/30
	8330 Crawfordsville Rd.	6/30
	8935 E 21st St.	6/30
	9500 Allisonville Rd.	6/27
	1233 North State St. (Greenfield)	9/26
	13050 Publishers Dr. (Fishers)	6/30
	1825 Albany St. (Beech Grove)	6/30
	1390 Rangeline Rd. (Carmel) (Osco)	6/27
Louisville	7th & Dixie Hwy	8/24
	5330 S. 3rd St.	8/24
Miami	8765 S. Dixie Hwy	8/31
	6780 SW 40th	8/31
	306 Lincoln Rd. (Miami Beach)	8/31
New Haven, Conn.	215 Whalley	10/11
Philadelphia Metro	3300 S. Broad St.	9/27
	119 Baltimore Ave. (Lansdowne)	9/27
	1937 McDade (Folsum)	9/27
	Oak & McDade (Glenolden)	9/27
Phoenix	4742 E Indian School Rd.	9/3
	3141 E Indian School Rd	9/4
Woonsocket, RI	1450 Park Ave.	10/12
	166 Cass Ave.	10/12

[No personal information found in CVS dumpsters in Washington, DC. CVS does not operate pharmacies in the Denver area.]

II. November 2006 WTHR article about prescription privacy investigation

This is an article describing the WTHR investigation into pharmacies' practices. For the complete article, which included images related to the investigation, see <http://www.wthr.com/Global/story.asp?S=5693471>.

WTHR finds prescription privacy problems nationwide
Nov 22, 2006 12:22 PM

Bob Segall/13 Investigates

The nation's largest pharmacies said the problem was a regional one and they'd fix it.

But a nationwide WTHR investigation shows privacy violations at CVS and Walgreens drugstores are still taking place and stretch far beyond the borders of Indiana. The investigation has prompted pharmacies to announce new policies to protect the privacy of millions of customers at drugstores across the United States.

Over the past six months, 13 Investigates inspected pharmacy dumpsters in more than a dozen cities. The nationwide prescription privacy test found in nearly every city checked, pharmacies failed to protect customers' personal health information by discarding it in unsecured outdoor dumpsters.

13 Investigates found legally-protected patient information on prescription labels, patient information sheets, pill bottles, prescription forms and customer refill lists in dumpsters in and around Boston, Chicago, Cleveland, Dallas, Denver, Detroit, Louisville, Miami, New Haven (Conn.), Philadelphia, and Phoenix.

Washington, D.C., was the only exception. We checked 14 drugstore dumpsters around the nation's capitol and found no patient records.

Woonsocket, RI, proved to be one of the worst towns for prescription privacy. 13 Investigates found 460 patient records in CVS dumpsters in Woonsocket, which is home to CVS world headquarters.

"It's not supposed to work like this," said Mitch Betses, CVS Director of Pharmacy Operations. "It's very upsetting and we're going to have to correct these errors... customers have an expectation of privacy and we cannot allow these things to happen."

13 Investigates' prescription privacy test netted 2,394 patient records from 74 drugstore dumpsters nationwide. Most of those dumpsters belong to CVS, Walgreens and RiteAid pharmacies, although several smaller, locally-owned drugstores also failed the test. CVS, Walgreens and RiteAid are the country's three largest pharmacy chains with more than 15,000 drugstores nationwide.

A total of 296 dumpsters were checked during the investigation. Of those:

* 103 dumpsters were inaccessible to the public because they were either locked, accessible only from inside the drugstore or located behind a closed gate (WTHR did not open closed gates to inspect dumpsters even if they were not locked)

* 56 dumpsters were empty at the time of inspection

* 64 dumpsters contained trash bags with no personal information

* 74 dumpsters contained trash bags with personal information.

Of the 138 pharmacy dumpsters where Eyewitness News was able to inspect trash, more than half (54%) contained customer information that pharmacies say should not have been in there.

While about one-third of the dumpsters checked offered little or no public access, most were unlocked and wide open. In several cities, 13 Investigates watched as other people rummaged through unsecured dumpsters.

"I'm looking to make money," said Ted, a homeless man in Cleveland who was looking inside a Walgreens dumpster. Ted told 13 Investigates he checks pharmacy dumpsters because he often finds beer, soda, cigarettes and other items he can sell on the street. He said he sees a lot of prescription labels in the dumpsters, as well.

WTHR began its investigation this summer, following up on the story of a Bloomington grandmother who was robbed at her front door. The Monroe County Sheriff's Department says a thief found the woman's address and prescription information in an unsecured CVS dumpster, then went to her home and posed as a pharmacy employee to successfully steal the woman's prescription for Oxycontin. The drug is a powerful, highly-addictive pain medication.

During the initial investigation, 13 Investigates found hundreds of patient records in drugstore dumpsters around Indianapolis. In July, CVS and Walgreens told WTHR the problem was a result of pharmacy staff failing to adhere to strict policies designed to protect customers' personal information. At that point, both companies issued statements assuring customers the problem would be fixed.

"We apologize," said Marla Barger, a Walgreens regional manager. "We'll address the procedures and ensure they are followed in the future."

Industry watchdogs now say that did not happen, and they believe the pharmacies are violating state and federal law.

"For pharmacies to still be engaged in the activity or to allow it to occur is not only a violation of state laws but it's a disgrace," said Carmen Catizone. He is president of the National Association of Boards of Pharmacy, an organization that helps regulate the nation's roughly 87,000 pharmacies.

Catizone says pharmacy boards in every state have rules to prevent pharmacies from jeopardizing customers' private information. "For this to be happening to this extent means somebody is not doing what they're supposed to be doing. This is a national issue," he added.

Federal law requires doctors, nurses, pharmacists and other healthcare professionals to

take reasonable measures to protect patients' personal and healthcare-related information. Failing to do so can result in fines levied against violators, although that rarely happens.

A corporate official at CVS admitted the nation's largest drugstore chain is falling short of federal requirements.

"We are not safeguarding customer privacy as we are required to do," said CVS corporate privacy officer Kristine Egan. "It's sad and intolerable ... and we need to do better. We will do better."

A Walgreens spokesman said his company has not broken the law by placing patients' personal information in unsecured dumpsters. Walgreens corporate communications manager Michael Polzin told 13 Investigates that federal law "doesn't prohibit disposing of information in dumpsters."

The federal government's top legal advisor on heath privacy disagreed.

"Putting protected health information in a dumpster that is accessible to anyone ... is clearly not an example of a reasonable safegaurd," said Susan McAndrew, senior advisor with the U.S. Department of Health and Human Services' Office of Civil Rights. Her advice to pharmacies looking to follow the law: "Don't do that!"

A spokesman for the Office of Civil Rights said the agency has launched its own investigation following WTHR's reports. The investigation will determine whether pharmacies will face any fines for improperly disposing of patient information. The Indiana Attorney General's office has also opened an investigation after the Indiana Board of Pharmacy filed 30 consumer complaints resulting from reports on Eyewitness News.