

March 19, 2009

Leadership Council

Anna Burger
Chair
Change to Win
International
Secretary-Treasurer
Service Employees
International Union (SEIU)

Edgar Romney
Secretary-Treasurer
Change to Win
Executive Vice President
UNITE HERE

Joseph Hansen
International President
United Food and
Commercial Workers
International Union (UFCW)

James P. Hoffa
General President
International Brotherhood
of Teamsters (IBT)

Gerilyn Luty
International Vice President
United Food and
Commercial Workers
International Union (UFCW)

Douglas J. McCarron
General President
United Brotherhood
of Carpenters
and Joiners
of America (UBC)

Terence M. O'Sullivan
General President
Laborers' International Union
of North America (LIUNA)

Bruce Raynor
General President
UNITE HERE

Arturo S. Rodriguez
President
United Farm Workers
of America (UFW)

Andrew L. Stern
International President
Service Employees
International Union (SEIU)

Federal Trade Commission
Office of the Secretary
Room H-135
600 Pennsylvania Avenue N.W.
Washington, D.C. 20580

Re: Comments regarding Proposed Consent Order *In the Matter of CVS Caremark Corporation*, FTC File No. 072 3119

To the Secretary:

Change to Win submits these comments regarding the Proposed Consent Order *In the Matter of CVS Caremark Corporation*, File No. 0723119. As explained below, we believe the proposed Consent Order should be modified in four respects to adequately protect the public from the potential disclosure of highly confidential patient and other information.

Change to Win is a federation of seven of the country's most active labor unions, including the Service Employees International Union, United Food and Commercial Workers, and the International Brotherhood of Teamsters. Health care issues, including the day to day accessibility, cost and safety of obtaining medications, are extremely important to our members – and to all Americans. Promoting a health system that is secure as well as effective and affordable is high on our agenda for working families.

We have been concerned for some time that CVS Caremark Corporation has failed to take adequate steps to protect consumer and patient privacy by dumping personal information unprotected in publicly accessible trash containers. Moreover, CVS has repeatedly promised to reform its practices when confronted with public reports of its breaches, but has failed to do so. We commend the Federal Trade Commission ("FTC" or "Commission") for investigating and taking action on this important issue. However, in light of the seriousness of CVS Caremark's breaches, and its failed promises to reform in response to prior violations, we believe that the order should impose stronger accountability measures on the company.

Reports of CVS Caremark privacy breaches

CVS Caremark encompasses the country's largest chain of retail pharmacies – more than 6,800 – and also the country's second largest pharmacy benefit management company. As such the company, by its own estimates, has "more

*Federal Trade Commission
Comments regarding Proposed Consent Order in FTC File No. 072 3119
March 19, 2009
Page 2 of 7*

information on the consumer and their behavior than anyone else,”¹ and possesses data on 30 percent of all prescriptions in the U.S. – over 1.2 billion prescriptions per year. Its retail drugstore chain also operates the largest customer loyalty program in history, ExtraCare, with at least 50 million members. Through the ExtraCare program, CVS collects detailed and extensive personal information on its customers.

In spite of its unprecedented access to patient and consumer information, CVS Caremark has been the subject of a number of news reports and state-level enforcement actions concerning the improper disposal of patient and consumer information. Moreover, it has promised in response to these public reports and actions that it would reform its privacy practices, but it is unclear that it has adhered to these promises.

In November 2006, three news stations in different parts of the country announced that they had found patient and consumer information in unsecured trash cans at multiple CVS stores. The areas covered by the investigations included Houston, Boston, Indianapolis, New Haven, Philadelphia, and much of Ohio, among others. The news stations each investigated other drugstore chains, but CVS appeared to have by far the most severe problems with improperly disposing of sensitive information:

- The Houston investigation found 20 CVS stores dumping private information, and only three Walgreens.
- The Ohio investigation found one-third of CVS stores investigated had personal information in unsecured trash cans. In contrast, it found all Walgreens dumpsters were secured and inaccessible.
- A multi-city investigation reported by an Indianapolis television station found private information dumped at 39 CVS stores, but only 22 Walgreens stores and only nine Rite Aid stores, despite looking in cities, such as Chicago, where CVS was not necessarily the dominant chain.

CVS repeatedly promised to strengthen or improve its privacy practices in response to news reports or regulatory action showing violations, but reports of further violations – even after these promises were made – suggest CVS has not taken the issue of consumer and patient privacy seriously, and has not kept its promises to implement effective policies against such violations:

¹ Statement of Thomas Ryan, CVS – CVS Caremark Corporation 2008 Analyst/Investor Meeting Transcript, May 21, 2008, at 7.

*Federal Trade Commission
Comments regarding Proposed Consent Order in FTC File No. 072 3119
March 19, 2009
Page 3 of 7*

- An Indianapolis television station first reported privacy violations by CVS and other area drugstores in July 2006, at which time CVS promised to address the problem quickly, stating “We have reinforced our strict procedures for the disposal of confidential information at our stores. Our field management team will also work to ensure our disposal policies are being followed and that these incidences do not occur again.”² These promises – and CVS’s claims in July 2006 that the problem was a localized one – were refuted by the multiple news reports of personal information dumping by CVS nationwide in November 2006, discussed above.
- In response to the November 2006 reports, CVS again promised to address the problem, stating that it was “implementing new policies and procedures for the disposal of confidential information ... at all of our pharmacies in order to strengthen compliance.”³ However, in December 2006, an Evansville news station reported that it had found patient information in CVS drugstore trash bins. The Indiana Attorney General ultimately brought complaints against ten CVS stores in Indiana, filed in August and September 2007, for dumping patient information in violation of state licensing regulations.

Even several months after CVS’s information-disposal problems were reported by multiple news stations, and CVS promised to strengthen its disposal and privacy protection practices, state regulators continued to find violations of consumer and patient privacy by CVS:

- In March 2007, the Texas Attorney General discovered more than one thousand unprotected patient and consumer financial records in a trash bin outside a CVS store. The Attorney General brought suit in April 2007. In March 2008, a settlement was announced under which CVS promised, again, to adopt reforms of its privacy practices that would protect sensitive patient and consumer information in Texas.
- In June 2008, in response to consumer complaints indicating CVS was improperly disposing of private patient information in California, Attorney General Brown called on the company to “comply with California laws requiring proper storage and disposal” of consumer and medical information.⁴

The improper disposal of sensitive patient and consumer information poses serious risks to consumers. The most obvious is identity theft. In addition, however, patients may be

² “CVS/pharmacy Statement for WTHR,” July 2006, available at: <http://wthr.images.worldnow.com/images/incoming/pdfs/CVS%20Response.pdf>.

³ “Protecting your prescription information,” Ted Hart, WBNS-10TV, Nov. 7, 2006.

⁴ “Brown Calls On CVS Pharmacy To End Expired Product Sales, Protect Confidential Information,” News Release, Office of the California Attorney General, June 19, 2008.

*Federal Trade Commission
Comments regarding Proposed Consent Order in FTC File No. 072 3119
March 19, 2009
Page 4 of 7*

exposed to other serious risks from having their prescription information disposed of in publicly accessible trash containers. For example, the Ohio television report on patient records found in the trash at drug stores recounted that a patient who had filled a prescription for oxycontin was visited at her home by a man who claimed to work for the pharmacy that had filled her prescription, and said he needed the pills back because there was a problem with the prescription. In fact the man had simply found her prescription information and home address in the trash, identified her as having a prescription for narcotics, and hunted her down to try to obtain the drugs from her illicitly. Thus the risks attendant to drug store privacy practices go beyond identity theft.

CVS Caremark has repeatedly promised it would reform its privacy practices in response to these public reports of privacy breaches, but these promises have failed to prevent further violations. Because of this, we urge the Commission to require additional steps to ensure CVS Caremark implements policies and procedures that effectively protect private patient information from damaging public disclosure.

Additional Steps

We have four recommendations that we believe would strengthen accountability under the proposed consent order:

1) Require annual, rather than biennial, third party assessments of CVS Caremark's policies and procedures for protecting privacy, for at least the first three years the order is in effect, and require CVS Caremark to provide these reports, along with responsive steps taken regarding any deficiencies, to the Commission.

The proposed Consent Order requires CVS Caremark to adopt a comprehensive system for safeguarding patient and consumer privacy. It also requires the company to retain a third-party monitor to evaluate the policy and its implementation.

However, the proposed Consent Order requires a third-party evaluation only once every two years while the separate but parallel agreement with the Department of Health and Human Services (HHS) requires a third-party evaluation annually during the first three years of that agreement. The evaluations required by the HHS agreement are limited to personal health information (PHI) and apply only to CVS pharmacies. The evaluations required by the proposed Consent Order apply to both medical and consumer information and to both pharmacy and non-pharmacy pharmacy benefit management operations, which also handle vast amounts of patient and consumer information.

*Federal Trade Commission
Comments regarding Proposed Consent Order in FTC File No. 072 3119
March 19, 2009
Page 5 of 7*

Moreover, the proposed Consent Decree does not require CVS to respond in any way to deficiencies identified by the third-party evaluations and requires only the first evaluation to be provided to the Commission.

In these respects, the proposed Consent Order fails to adequately protect the public, particularly in light of the past history of CVS promises followed by repeated violations. Accordingly, we urge the Commission to revise the proposed Consent Order to require more frequent third-party evaluations – at least once each year during the first three years, the same schedule as that imposed by the separate HHS agreement. This would significantly strengthen protection for the public because, unlike the HHS agreement, the proposed Consent Order applies to both medical and non-medical information and to both pharmacy and non-pharmacy operations. We also urge the Commission to require CVS to report its actions to remedy any deficiencies identified in the third-party evaluations and to provide all evaluation reports and CVS responses to the Commission.

2) Require CVS Caremark to report any violation of the revised policies and procedure for safeguarding sensitive patient and consumer information, along with a report on corrective action taken, within 30 days of the violation.

In order to provide accountability for implementing a privacy protection system that is effective at protecting privacy, we recommend that the consent order adopt the same violations-reporting measures that are contained in the HHS agreement, requiring CVS Caremark to report any failure to comply with, or violation of, its privacy measures to its third-party monitor and the FTC. The company should also be required to report the corrective action it has taken to remedy the violation. Reports of violations and corrective action taken should be submitted within 30 days of the violation (or an explanation why corrective action could not be completed within 30 days). Because the HHS agreement already requires reporting of violations with respect to PHI, and the company should put procedures in place to detect, evaluate and correct any violations, this provision also would impose little additional burden on CVS.

3) Require CVS Caremark to provide copies of all reports, including assessment reports and reports of violations and corrective action, to state Attorneys General.

States have done much to compliment the FTC's groundbreaking work in past years on protecting consumer privacy. An overwhelming number of states have recently adopted laws protecting individuals from identity theft or the misuse of medical information or both. State Attorneys General are generally responsible for enforcing these laws, and have been at the forefront of working to protect consumer and medical privacy. With respect to CVS Caremark specifically, Attorneys General in Texas and Indiana were the first to take legal action on the dumping of patient and consumer information by CVS.

*Federal Trade Commission
Comments regarding Proposed Consent Order in FTC File No. 072 3119
March 19, 2009
Page 6 of 7*

In addition, pharmacies are licensed at the state level. Pharmacies' failure to protect patient or consumer information, in ways that violate either state or federal law, is relevant to states' decision whether to review pharmacies' licenses to operate – and thus to continue collecting and using patient and consumer information.

Requiring information-sharing with state Attorneys General, rather than public publication or dissemination of compliance reports, would avoid confidentiality or trade secret issues, because the reports would only be shared with other law enforcement/investigatory bodies.

As partners in the effort to protect privacy, and with significant responsibilities for enforcement and licensing located at the state level, state Attorneys General should have access to information that will enable them to perform these tasks more effectively by receiving CVS Caremark reporting on privacy compliance under the consent order.

4) Require CVS Caremark to provide notice to customers and patients whose information was previously, or later is, disposed of improperly.

The violations that led to the FTC settlement created a significant risk of identity theft and the disclosure of sensitive personal and medical information. In these circumstances, it is standard practice to warn consumers and patients so that they can take whatever steps they believe necessary and appropriate to protect themselves. The proposed Consent Order should be modified to require CVS to notify individuals whose information was previously exposed or is exposed through improper disposal in the future.

We applaud the FTC for taking action on this important issue, against a company that, by its own account, handles data on almost one-third of all prescriptions filled in the United States. We urge the Commission to add the above provisions to the proposed consent order so that the public can be assured of meaningful reform by CVS Caremark.

Respectfully submitted,

Christopher Chafe
Executive Director, Change to Win

cc: Attorney General Dustin McDaniel
P.O. Box 251368

*Federal Trade Commission
Comments regarding Proposed Consent Order in FTC File No. 072 3119
March 19, 2009
Page 7 of 7*

Little Rock, AR 72225

Attorney General Jack Conway
700 Capitol Avenue
State Capitol Building, Suite 118
Frankfort, KY 40601

Attorney General Martha Coakley
One Ashburton Place, FL 20
Boston, MA 02180

Attorney General Doug Gansler
200 St. Paul Place
Baltimore, MD 21202

Attorney General Drew Edmonson
313 Ne 21st Street
Oklahoma City, OK 73105

Attorney General Patrick Lynch
Attn: Jeff Guimond
150 South Main Street
Providence, RI 02903

Attorney General Steve Bullock
P.O. Box 201401
Helena, MT 59620-1401

Attorney General Chris Koster
Supreme Court Building
207 W. High St.
P.O. Box 899
Jefferson City, MO 65102

Attorney General Roy Cooper
Attn: Stephen Bryant, Senior Advisor
P.O. Box 10587
Raleigh, NC 27605