UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

June 18, 2009

Mr. Christopher Chafe
Executive Director
Change to Win
1900 L Street, NW
Suite 900
Washington, DC 20036

Re: In the Matter of CVS Caremark Corporation, File No. 072-3119, Docket No. C-4259

Dear Mr. Chafe:

Thank you for your letter commenting on the Federal Trade Commission's consent agreement in the above-entitled proceeding. Your letter was placed on the public record pursuant to Rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii), and was given serious consideration by the Commission.

Your letter commends the Commission for its action, and also presents comments and recommendations which the Commission addresses below.

You express concern that the proposed order may not lead to the timely correction of order violations that may occur while the order is in effect. You therefore ask the Commission to: require CVS Caremark Corporation ("CVS Caremark") to obtain assessments annually for at least the first three years of the order and to produce all assessments to the Commission; report to the Commission the actions the company has taken to correct deficiencies identified in assessments; and report order violations and any resulting corrective actions to the Commission within 30 days after a violation occurs. The Commission believes that the order and available remedies for order violations appropriately address this concern, for the following reasons.

First, the order requires the company to implement appropriate practices to identify and promptly correct security deficiencies that may violate the order. Second, the order requires CVS Caremark to obtain assessments of its information security program from qualified, independent, and objective assessors. To provide assurances that, among other things, CVS Caremark identifies and corrects deficiencies appropriately, the assessor must certify that the program operated effectively throughout the reporting period. Third, the Commission may review CVS Caremark's compliance with the order at any time by requesting and examining any plans, audits, policies, and other materials related to compliance. Finally, should CVS Caremark's information security program fail to operate effectively during the assessment period – because, for example, the company failed to appropriately correct security deficiencies that

arose during that period – the company could be in violation of the order and subject to civil monetary penalties of up to $16,000 per violation. In sum, these provisions, which are consistent with numerous FTC data security orders, provide strong incentives for the company to take appropriate steps to correct security deficiencies during an assessment period.

You also ask the Commission to provide assessments, reports of order violations, and reports of corrective actions taken by CVS Caremark to all state Attorneys General. Commission procedures permit it to share information obtained in monitoring CVS Caremark's compliance with the order with federal and state law enforcement agencies. Further, pursuant to law, compliance reports the company submits under the order will (subject to appropriate redaction) be entered onto the public record.

Finally, you ask the Commission to require CVS Caremark to notify consumers whose information has been, or in the future is, disposed of improperly. The Commission considers various factors in deciding whether notice to consumers is an appropriate remedy in a particular case, such as whether consumer victims are reasonably identifiable, whether notice is already required under federal or state laws[1], and whether the notice would be likely to benefit consumers under the circumstances. Here, the Commission has determined that the remedies in the proposed order – including implementing and maintaining a comprehensive information security program and obtaining independent assessments of its effectiveness every other year for 20 years – will ensure appropriate protections for consumers.

After considering your comments, the Commission has determined that the public interest would be best served by accepting the consent order. Thank you again for your letter.

By direction of the Commission.

Donald S. Clark
Secretary

---

[1] Current Federal law (the recently enacted American Recovery and Reinvestment Act of 2009) requires all health-related entities, including pharmacies, to notify customers of breaches of personal health information. In addition, 44 states have enacted laws requiring breach notification, some of which make public the fact that notifications have been made, and private entities routinely compile and publish information about breaches.