

February 23, 2009

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



RE: CVS Caremark Corporation

Ms. Harbour and Gentlemen:

Thank you for the opportunity to comment upon the Commission's proposed Consent Order in this matter. I suggest that the Order is insufficient and should be amended to (1) define "reasonable" to assure that any cost/benefit analysis will value consumer protection ahead of cost; (2) require that CVS notify and make whole customers potentially affected by the underlying security breaches; (3) require an immediate assessment of CVS's new information security program, and (4) provide that the third party professional be in turn hired through an independent third party, and not directly by CVS.

1. The Several Requirements of "Reasonability" Render the Order Vague and Difficult to Enforce

At several points, the Order sets forth a standard of reasonability. For example, the Order requires CVS to implement an information security program that is "reasonably designed" to protect the security, etc. of customers' personal information.

Any assessment of reasonability involves a balancing test. Here the predominant balancing will be between the level of security of customer personal information and the cost to obtain that level of security. Yet the Order fails to specify who shall conduct the balancing or the context of the cost/benefit analysis. This requirement of undefined reasonableness invites a battle of experts in any attempt to enforce the Order.

The Commission should modify the Order to provide that any judgment of reasonableness shall be made by the security professional (see below) and shall be based upon the core information security and assurance tenets: confidentiality,

integrity, and availability,¹ with the security of customer personal information the predominant consideration.

2. The Order Fails to Correct the Damage to Affected Customers

The Complaint, the Order, and the Commission's press release do not provide sufficient information for any particular customer of CVS to decide whether the security of his/her personal information may have been breached. For example, I cannot tell from these documents whether the security of my personal information at CVS Store #1989 may have been compromised. Thus, the Order overlooks the primary purpose of this enforcement action: the protection of the personal information of customers of CVS.

The Commission should modify the Order to require that CVS notify affected customers by mail where possible and in any event by posting of conspicuous notice and inclusion of notice in future prescription paperwork at those stores where CVS has breached the security of its customers' personal information. The Order should further require that CVS provide any affected customer a free credit watch and full compensation for any identity theft or other credit impairment that occurred after CVS's breach of security of that customer's personal information.

3. The Order Requires Only a Belated Assessment of CVS's New Information Security Program

The Order requires that CVS implement its new information security program no later than the date of service of the Order. Yet the Order does not require any assessment of the adequacy of that program for a year. The Order should be modified to require an immediate assessment.

4. The Order Fails to Assure the Independence of the Third Party Professional

Recent experience confirms the potential for an unnaturally cozy relationship between a professional and the entity that pays the professional. Examples include Enron and its accountants as well as Wall Street and the bond rating agencies.

¹ See Tipton & Henry, *Official (ISC)² Guide to the CISSP CBK*, Auerbach Publications, p. xv, ISBN 0-8493-8231-9

Federal Trade Commission
February 23, 2009
Page 3

The Commission should modify the Order to provide that the third party professional be hired and paid by an independent third party such as Consumers Union and that CVS reimburse that third party for the fees of the professional and the cost of managing the professional's activities.

5. Conclusion

The Commission has accused CVS of severe breaches of the security of its customers' personal information. The vague language of the Order, the delayed assessment, the lack of controls over the assessment, and the failure to make affected customers whole render the Order toothless and inappropriate. The Commission should direct its staff to negotiate a strong enforcement order to correct the defects of this inadequate proposal.

With renewed thanks for this opportunity to comment and with kindest regards, I am

Sincerely,

John R. Butcher