



Office of the Secretary

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

September 5, 2006

Mr. Richard A. Painter, P.E.
8470 Swan Road
Black Forest, Colorado 80908

Re: *In the Matter of CardSystems Solutions, Inc., et al., File No. 052 3148*

Dear Mr. Painter:

This acknowledges 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 comment expresses concern that the proposed order does not qualify explicitly Professional Engineers ("PEs") to perform the security assessments ("Assessments") required under Paragraph II. The proposed order requires CardSystems Solutions, Inc. and its successor to obtain Assessments on a biennial basis from a person qualified as a Certified Information System Security Professional or as a Certified Information Systems Auditor or holding Global Information Assurance Certification from the SANS Institute. Individuals with these credentials necessarily will have been trained in the technical skills required to perform Assessments. As you note, some persons holding PE credentials may possess these same specific technical skills, but others may not. Thus, the proposed order provides that persons who do not have the credentials specified in the order, but who, such as certain PEs, are similarly qualified, may perform Assessments if approved by the Associate Director for Enforcement of the Commission's Bureau of Consumer Protection.

Your comment also states that the proposed order should require CardSystems to notify affected consumers of the data compromise described in the Commission's complaint, and inform the Commission and notify consumers of future security failures and breaches. Under the circumstances of this case, the Commission has determined that the relief in the proposed order is adequate and appropriate. It is important to note that the law violation alleged in the complaint is not the data compromise that CardSystems experienced, but the failure to maintain reasonable and appropriate security for personal information stored on its computer network. To remedy that alleged violation, the proposed order requires CardSystems to establish and maintain a comprehensive information security program and to obtain Assessments of its program from an independent professional, on a biennial basis, for twenty years. Further, the Commission notes that notice to consumers of data compromises may not be appropriate in all cases, but should be used when necessary to address a significant risk of identity theft. After considering the

circumstances of this case, the Commission determined not to seek notice to consumers. As for notice to the Commission, the proposed order requires CardSystems to make available to the Commission each Assessment and its underlying information as well as all information that calls into question CardSystems' compliance with the order.

After reviewing your comment, and the other submitted comments, the Commission has determined that the public interest would be best served by according final approval to the consent order. Thank you again for your comment.

By direction of the Commission, Commissioner Harbour recused.

Donald S. Clark
Secretary