Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Life is good, Inc., and Life is good Retail, Inc., File No. 072 3046

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Life is good, Inc. and Life is good Retail, Inc. (collectively, "Life is good").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Life is good designs and distributes retail apparel and accessories and operates a retail website at www.lifeisgood.com. In selling its products, Life is good routinely has collected sensitive information from consumers, including name, address, e-mail address, phone number, credit card number, credit card expiration date, and credit card security code (hereinafter "consumer information"). Life is good has collected this consumer information through its website and telephone orders and stored it on a network computer accessible through the website. This matter concerns alleged false or misleading representations Life is good made about the security it provided for this information.

The Commission's proposed complaint alleges that Life is good represented that it implemented reasonable and appropriate security measures to protect the privacy and confidentiality of sensitive consumer information. The complaint alleges this representation was false because Life is good engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the sensitive consumer information stored on its computer network. In particular, Life is good: (1) created unnecessary risks to credit card information by storing it indefinitely in clear, readable text on its network without a business need, and by storing credit card security codes; (2) failed to assess adequately the vulnerability of its web application and corporate computer network to certain commonly known or reasonably foreseeable attacks, such SQL injection attacks; (3) failed to implement simple, free or low-cost, and readily available defenses to SQL and related types of attacks; (4) failed to use readily available security measures to monitor and control connections from the network to the internet; and (5) failed to employ sufficient measures to detect unauthorized access to credit card information.

The complaint further alleges that between June and August 2006, a hacker exploited Life is good's failures by using SQL injection attacks on Life is good's website and web application and exporting to the hacker's browser consumer information for thousands of customers, including credit card numbers, expiration dates, and security codes.

The proposed order applies to personal information Life is good collects from or about consumers. It contains provisions designed to prevent Life is good from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits Life is good, in connection with the collection of personally identifiable information from or about consumers, in or affecting commerce, from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or integrity of such information.

Part II of the proposed order requires Life is good to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Life is good's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires Life is good to:

- Designate an employee or employees to coordinate and be accountable for the information security program.

- Identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.

- Develop and use reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondents, require service providers by contract to implement and maintain appropriate safeguards, and monitor their safeguarding of personal information.

- Evaluate and adjust its information security program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of their information security program.

Part III of the proposed order requires that Life is good obtain, covering the first 180 days after the order is served, and on a biennial basis thereafter for twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that (1) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its security program is

operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected.

Parts IV through VII of the proposed order are reporting and compliance provisions. Part IV requires Life is good to retain documents relating to their compliance with the order. For most records, the order required that the documents be retained for a five-year period. For the third-party assessments and supporting documents, Life is good must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Life is good submit an initial compliance report to the FTC, and make available to the FTC subsequent reports. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.