

Complaint

IN THE MATTER OF

**LIFE IS GOOD, INC.,
AND
LIFE IS GOOD RETAIL, INC.**CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

*Docket C-4218; File No. 072 3046
Complaint, April 16, 2008 – Decision, April 16, 2008*

This consent order addresses false or misleading representations Life is good made about the security it provided for personal information collected from consumers in connection with the sale of apparel and accessories through a retail website. Life is good engaged in a number of practices that failed to provide reasonable and appropriate security for the sensitive consumer information stored on its computer network. In fact, a hacker was able to export consumer information for thousands of customers. The order prohibits Life is good from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or integrity of personally identifiable information collected from or about consumers. The 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. In addition, Life is good must obtain, on a biennial basis for 20 years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that it has in place a security program that provides protections that meet or exceed the protections required by the order; and its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected. Additional provisions of the order relate to notifying the Commission of changes in corporate status and submitting compliance reports to the Commission.

Participants

For the Commission: *Laura Berger, Kristin Krause Cohen,
Marc Groman, Michael Ostheimer, Jessica Rich, and Joel Winston.*

For the Respondents: *John Banse, in-house counsel.*

Complaint

COMPLAINT

The Federal Trade Commission, having reason to believe that Life is good, Inc., and Life is good Retail, Inc. (“respondents”), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Life is good, Inc., is a Massachusetts corporation with its principal office or place of business at 283-285 Newbury Street, Boston, Massachusetts 02115.

2. Respondent Life is good Retail, Inc., is a Delaware corporation with its principal office or place of business at 283-285 Newbury Street, Boston, Massachusetts 02115. Life is good Retail, Inc., is a wholly-owned subsidiary of Life is good, Inc.

3. The acts and practices of respondents as alleged in this complaint are in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

4. Respondents design and distribute retail apparel and accessories and operate a retail website at *www.lifeisgood.com*.

5. Respondents operate a computer network that consumers use, in conjunction with respondents’ website (*www.lifeisgood.com*) and web application, to obtain information and to buy respondents’ products.

6. In selling their products, respondents routinely have 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”). Respondents have collected this consumer information through their website and telephone orders and stored it on a network computer accessible through the website.

Complaint

7. Since at least October 2005, respondents have disseminated or caused to be disseminated privacy policies and statements on their website, including, but not necessarily limited to, the following statements regarding the privacy and confidentiality of the consumer information they collect:

We are committed to maintaining our customers' privacy. We collect and store information you share with us – name, address, credit card and phone numbers – along with information about products and services you request. All information is kept in a secure file and is used to tailor our communications with you.

(Emphasis added).

8. Since at least October 2005, respondents have engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the consumer information stored on their network, including credit card numbers, expiration dates, and security codes. In particular, respondents: (1) stored the consumer information in clear, readable text; (2) created unnecessary risks to consumer information by storing it indefinitely on their network, without a business need, and by storing credit card security codes; (3) did not adequately assess the vulnerability of their web application and network to commonly known or reasonably foreseeable attacks, such as “Structured Query Language” (“SQL”) injection attacks; (4) did not implement simple, free or low-cost, and readily available defenses to such attacks; (5) did not use readily available security measures to monitor and control connections from the network to the internet; and (6) failed to employ reasonable measures to detect unauthorized access to consumer information.

9. Between June and August 2006, a hacker exploited the failures set forth in Paragraph 8 by using SQL injection attacks on respondents' 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.

Decision and Order

After learning of the breach from their customers, respondents took steps to prevent further unauthorized access, notified law enforcement, and sent breach notification letters to affected customers.

10. Through the means described in Paragraph 7, respondents represented, expressly or by implication, that they implemented reasonable and appropriate measures to protect consumer information against unauthorized access.

11. In truth and in fact, respondents did not implement reasonable and appropriate measures to protect consumer information against unauthorized access. Therefore, the representation set forth in Paragraph 7 was, and is, false or misleading.

12. The acts and practices of respondents as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this sixteenth day of April, 2008, has issued this complaint against respondents.

By the Commission.

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondents named in the caption hereof, and the Respondents having been furnished thereafter with a copy of a draft complaint, which the Bureau of Consumer Protection

Decision and Order

proposed to present to the Commission, and which would charge the Respondents with violation of the Federal Trade Commission Act; and

The Respondents and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondents of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondents that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondents have violated the Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days, and having duly considered the comment filed thereafter by an interested party pursuant to Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Life is good, Inc., is a Massachusetts corporation with its principal office or place of business at 283-285 Newbury Street, Boston, Massachusetts 02115.
2. Respondent Life is good Retail, Inc., is a Delaware corporation with its principal office or place of business at 283-285 Newbury Street, Boston, Massachusetts 02115. Life is good Retail, Inc., is a wholly-owned subsidiary of Life is good, Inc.
3. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondents, and proceeding is in the public interest.

Decision and Order

ORDER**DEFINITIONS**

For purposes of this Order, the following definitions shall apply:

1. “Personally identifiable information” or “personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and security code; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any information that is combined with any of (a) through (g) above.
2. Unless otherwise specified, “respondents” shall mean Life is good, Inc., Life is good Retail, Inc., and their successors and assigns, officers, agents, representatives, subsidiaries, affiliates, and employees.
3. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondents, directly or through any corporation, subsidiary, division, or other device, in connection with the collection of personally identifiable information from or about consumers, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondents

Decision and Order

maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondents, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondents' size and complexity, the nature and scope of respondents' activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program;
- B. the identification of 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 assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems failure;

Decision and Order

- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondents, requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information; and
- E. the evaluation and adjustment of respondents' information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondents' operations or business arrangements, or any other circumstances that respondents know or have reason to know may have a material impact on the effectiveness of their information security program.

III.

IT IS FURTHER ORDERED that, in connection with their compliance with Part II of this order, respondents shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondents have implemented and maintained during the reporting period;

Decision and Order

- B. explain how such safeguards are appropriate to respondents' size and complexity, the nature and scope of respondents' activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and
- D. certify that respondents' security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondents shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondents until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

IV.

IT IS FURTHER ORDERED that respondents shall maintain, and upon request make available to the Federal Trade Commission

Decision and Order

for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

- A. for a period of five (5) years, any documents, whether prepared by or on behalf of either respondent, that contradict, qualify, or call into question respondents' compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of either respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondents' compliance with Part II of this order, for the compliance period covered by such Assessment. Respondent shall provide such documents to the Associate Director of Enforcement within ten (10) days of request.

V.

IT IS FURTHER ORDERED that respondents shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondents shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that respondents and their successors and assigns shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not

Decision and Order

limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation(s) about which respondents learn fewer than thirty (30) days prior to the date such action is to take place, respondents shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondents and their successors and assigns shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.

VIII.

This order will terminate on April 16, 2028, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and

Analysis to Aid Public Comment

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent(s) did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent(s) will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

**ANALYSIS OF CONSENT ORDER TO AID PUBLIC
COMMENT**

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

Analysis to Aid Public Comment

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 as 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.

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

- 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.

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

CASHPRO d/b/a/ MAKEPAYDAYTODAY.COMCONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 144 OF THE TRUTH IN LENDING ACT

Docket C-4220; File No. 072 3203
Complaint, June 3, 2008 – Decision, June 3, 2008

This consent order addresses payday loan advertisements disseminated by CashPro, d/b/a *MakePaydayToday.com*, that failed to disclose the annual percentage rate for these loans, undermining consumers' ability to compare them to loans offered by other payday lenders or to alternative forms of credit. The order prohibits the respondent, in connection with any advertisement of consumer credit, from stating the amount or percentage of any down payment, the number of payments or period of repayment, the amount of any payment, or the amount of any finance charge, without disclosing clearly and conspicuously all of the terms required by the Truth in Lending Act and its implementing Regulation Z, including the amount or percentage of the down payment, the terms of repayment, and the annual percentage rate. The order prohibits the respondent from stating a rate of finance charge without stating the rate as an annual percentage rate, and from failing to comply in any other respect with the Truth in Lending Act or Regulation Z. It requires that the respondent maintain all records that will demonstrate compliance with the order. The respondent must distribute copies of the order to various principals, officers, directors, and managers, and all current and future employees, agents and representatives having responsibilities with respect to the subject matter of the order. In addition, CashPro is required to notify the Commission of any changes in its corporate structure that might affect compliance with the order and to file with the Commission one or more reports detailing compliance with the order.

Participants

For the Commission: *Beverly Childs, Thomas Pahl, Cara Petersen, Patti Poss, Peggy L. Twohig, and Quisaira Whitney.*

For the Respondent: *Not represented by counsel.*