

Complaint

IN THE MATTER OF

GOAL FINANCIAL, LLCCONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF THE GRAMM-LEACH-BLILEY SAFEGUARDS RULE AND PRIVACY
RULE AND SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4216; File No. 072 3013
Complaint, April 9, 2008 – Decision, April 9, 2008

This consent order applies to practices of Goal Financial, LLC, in regard to personal information it collects from or about consumers in connection with its student loan and related services. The respondent's practices in storing the information failed to provide reasonable and appropriate security for consumers' sensitive personal information, leading to the transfer of consumer files to third parties and the potential exposure of personal information through sale of the company's hard drives. The order requires that Goal Financial not misrepresent the extent to which it maintains and protects the privacy, confidentiality, or integrity of any personal information collected from or about consumers. The order requires Goal Financial 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 it collects from or about consumers. In addition, Goal Financial must obtain, on a biennial basis for 10 years, an assessment and report from a qualified, objective, independent third-party professional, certifying that Goal Financial has in place a security program that provides protections that meet or exceed the protections required by the order; and that its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information has been protected. The respondent is required to retain documents relating to its compliance and to disseminate the order now and in the future to persons with responsibilities relating to the subject matter. 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: *Loretta Garrison, Marc Groman, Jamie Hine, Jessica Rich, Alain Sheer, and Joel Winston.*

For the Respondent: *Alysa Z. Hutnik and Lewis Rose, Kelley Drye Collier Shannon.*

Complaint

COMPLAINT

The Federal Trade Commission (“Commission”), having reason to believe that Goal Financial, LLC has violated the provisions of the Commission’s Standards for Safeguarding Customer Information Rule (“Safeguards Rule”), 16 C.F.R. Part 314, issued pursuant to Title V, Subtitle A of the Gramm-Leach-Bliley Act (“GLB Act”), 15 U.S.C. § 6801-6809; the Commission’s Privacy of Customer Financial Information Rule (“Privacy Rule”), 16 C.F.R. Part 313, issued pursuant to the GLB Act; and 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 Goal Financial, LLC, (“Goal Financial”) is a California limited liability company with its principal office or place of business at 9477 Waples Street, Suite 100, San Diego, California 92121.
2. The acts and practices of respondent alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act.
3. Respondent markets and originates a variety of student loans, and provides loan related services.
4. In the course of its business, respondent collects personal information from consumer loan applications and other sources. The information includes name; address; telephone number; driver’s license number; Social Security number; date of birth; and income, debt, and employment information. Respondent retains the personal information in paper documents and also stores and maintains the information in an electronic database.
5. Since at least September 1, 2004, respondent has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers’ sensitive personal information, including Social Security numbers, dates of

Complaint

birth, and income and employment information. In particular, respondent has:

A. failed to assess adequately risks to the information it collected and stored in its paper files and on its computer network;

B. failed to restrict adequately access to personal information stored in its paper files and on its computer network to authorized employees;

C. failed to implement a comprehensive information security program, including reasonable policies and procedures in key areas such as the collection, handling, and disposal of personal information;

D. failed to provide adequate training to employees about handling and protecting personal information and responding to security incidents; and

E. failed in a number of instances to require third-party service providers by contract to protect the security and confidentiality of personal information.

6. In 2005 and 2006, respondent's employees exploited the failures enumerated in paragraph 5 and were able to remove without authorization more than 7000 consumer files containing sensitive information and transfer them to third parties. Further, in 2006, an employee sold to the public hard drives that had not been processed to remove the data on the drives, thus exposing in clear text the sensitive personal information of approximately 34,000 consumers.

VIOLATIONS OF THE SAFEGUARDS RULE

7. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 23, 2002, and became effective on May 23, 2003. The Rule requires financial institutions to protect the security,

Complaint

confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through the risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers, and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

8. Respondent is a "financial institution," as that term is defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).

9. As set forth in Paragraph 5, respondent has failed to implement reasonable security policies and procedures, and has thereby engaged in violations of the Safeguards Rule, by, among other things:

A. Failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;

B. Failing to design and implement information safeguards to control the risks to customer information or to regularly test or monitor their effectiveness;

C. Failing to develop, implement, and maintain a comprehensive written information security program; and

Complaint

D. Failing to require service providers by contract to implement safeguards to protect the security and confidentiality of customer information.

VIOLATIONS OF THE FTC ACT

10. Since at least November 9, 2005, respondent has disseminated or caused to be disseminated to consumers privacy policies and statements, including, but not limited to the following:

Our Security Policies and Practices

Access to nonpublic personal information about you is limited to those employees who need to know such information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

(Goal Financial, LLC Privacy Policy, attached as Exhibit A.)

11. Through the means set forth in Paragraph 10, respondent represented, expressly or by implication, that it implements reasonable and appropriate measures to protect personal information from unauthorized access.

12. In truth and in fact, as set forth in Paragraph 5, respondent did not implement reasonable and appropriate measures to protect personal information from unauthorized access. Therefore, the representation set forth in Paragraph 11 was, and is, false or misleading.

VIOLATION OF THE PRIVACY RULE

13. The Privacy Rule, which implements Sections 501-509 of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 24, 2000, and became effective on July 1, 2001. The Rule

Complaint

requires financial institutions to provide customers, no later than when a customer relationship arises and annually for the duration of that relationship, “a clear and conspicuous notice that accurately reflects [the financial institution’s] privacy policies and practices” including its security policies and practices. 16 C.F.R. §§ 313.4(a); 313.5(a)(1); § 313.6(a)(8).

14. As set forth in Paragraphs 10 through 12, respondent disseminated a privacy policy that contained false or misleading statements regarding the measures implemented to protect consumers’ personal information. Therefore, respondent disseminated a privacy policy that does not accurately reflect its privacy policy, including its security policies and practices, in violation of the Privacy Rule.

15. The acts and practices of respondent as alleged in this complaint constitute unfair or 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 ninth day of April, 2008, has issued this complaint against respondent.

By the Commission.

FEDERAL TRADE COMMISSION DECISIONS
VOLUME 145

Complaint

EXHIBIT A

PRIVACY NOTICE

We, Goal Financial, LLC*, are sending this Privacy Notice to individuals who apply for or obtain products or receive services from us ("you") to provide you with information concerning each of our privacy policies and to help you understand how we handle personal information about you which we may collect and disclose. This Privacy Notice applies to our current customers, former customers and applicants.

Our Privacy Policies and Practices

This notice uses the term "nonpublic personal information." This means personal information about you which identifies you, and that is not available from public sources. We may collect nonpublic personal information about you from various sources, including:

- Information provided by you such as, for example, information provided on loan applications or other forms;
- Information about your transactions with us, our affiliate or others;
- Information we receive from third parties, such as a consumer reporting agency or a list vendor; and
- Information we receive when you visit our website, such as cookies.

We do not disclose any nonpublic personal information about our applicants, customers or former customers to anyone, except as permitted or required by law. For example, nonpublic personal information about you may be shared with nonaffiliated third parties as necessary to certify, process, make, guarantee, administer or service your loan. We may also provide nonpublic personal information about you to our affiliated companies for any of these purposes. We also share nonpublic personal information about you whenever you consent (or "opt in") to our sharing of your information.

Our Security Policies and Practices

Access to nonpublic personal information about you is limited to those employees who need to know such information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

Important Information About Credit Reporting

We may report information about your account to credit bureaus. Late payments, missed payments or other defaults on your account may be reflected in your credit report.

If you have any questions regarding our privacy and security policies and practices, please email us at privacy@goalfinancial.net or write us at:

THE ABOVE IS A COPY OF THE
PRIVACY NOTICE

GOAL FINANCIAL, LLC

Complaint

Goal Financial, LLC
9477 Waspius Street, Suite 100
San Diego, CA 92121

Date last revised: November 9, 2005.

© Copyright Goal Financial, LLC 11/09/05. All rights reserved.

[illegible]

Decision and Order

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violations of the Commission's Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314, and Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313, both issued pursuant to Title V, Subtitle A of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 -6809, and the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq*;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that 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 has reason to believe that the Respondent has violated the said Acts, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

Decision and Order

1. Respondent Goal Financial, LLC, (“Goal Financial”) is a California limited liability company with its principal office or place of business at 9477 Waples Street, Suite 100, San Diego, California, 92121.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

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

1. “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) a bank, loan, or credit card account number; (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, “respondent” shall mean Goal Financial and its successors and assigns, officers, agents, representatives, and employees.
3. All other terms are synonymous in meaning and equal in scope to the usage of such terms in the Gramm-Leach-Bliley

Decision and Order

Act, 15 U.S.C. § 6801 *et seq.*, attached hereto as Appendix A or as may hereafter be amended.

4. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the collection of personal information from or about consumers, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the privacy, confidentiality, or integrity of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondent, 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 respondent’s size and complexity, the nature and scope of respondent’s 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

Decision and Order

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 failures.

- 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 respondent, requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information.
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that respondent shall not, directly or through any corporation, subsidiary, division, website, or other device, violate any provision of:

Decision and Order

- A. the Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314, as attached or as may be amended; or
- B. the Privacy of Customer Financial Information Rule, 16 C.F.R. Part 313, as attached or as may be amended.

In the event that any of these Rules is hereafter amended or modified, respondent's compliance with that Rule as so amended or modified shall not be a violation of this order.

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Parts II, and III.A. of this order, respondent 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 ten (10) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's 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 the Parts II and III A. of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that

Decision and Order

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.

Respondent 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 respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

V.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission 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 respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part IV of this order, all

Decision and Order

materials relied upon to prepare the Assessment, whether prepared by or on behalf of the 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 respondent's compliance with Parts II and III.A. 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.

VI.

IT IS FURTHER ORDERED that respondent 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. Respondent 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.

VII.

IT IS FURTHER ORDERED that respondent and its successors and assigns shall notify the Commission at least thirty (30) days prior to any change in the limited liability company that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; 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 company name or address. *Provided, however*, that, with respect to any proposed change in the company about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent 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,

Decision and Order

Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

IT IS FURTHER ORDERED that respondent and its successors and assigns shall, within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

IX.

This order will terminate on April 9, 2028, or twenty (20) years from the most recent date that the United States or the Federal Trade 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 less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- 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 did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order 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

Analysis to Aid Public Comment

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 Goal Financial, LLC (“Goal Financial”).

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.

Goal Financial markets and originates a variety of student loans and provides loan-related services. In conducting its business, Goal Financial routinely obtains personal information from loan applications and other sources, including name, address, telephone number, driver’s license number, Social Security number, date of birth, and income, debt, and employment information. Goal Financial, therefore, is a “financial institution” subject to the requirements of the Gramm-Leach-Bliley (“GLB”) Safeguards Rule and Privacy Rule. This matter concerns Goal Financial’s alleged violations of the GLB Safeguards Rule, the GLB Privacy Rule, and Section 5 of the Federal Trade Commission (“FTC”) Act.

Analysis to Aid Public Comment

The Commission's proposed complaint alleges that Goal Financial engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security measures to protect personal information. In particular, Goal Financial failed: (1) to assess adequately risks to the information it collected and stored in its paper files and on its computer network; (2) to restrict adequately access to personal information stored in its paper files and on its computer network to authorized employees; (3) to implement a comprehensive information security program, including reasonable policies and procedures in key areas such as the collection, handling, and disposal of personal information; (4) to provide adequate training to employees about handling and protecting personal information and responding to security incidents; and (5) in a number of instances to require third-party service providers by contract to protect the security and confidentiality of personal information. As a result of these alleged failures, Goal Financial put at risk the sensitive information of more than 41,000 consumers.

The complaint alleges that these security failures violated the GLB Safeguards Rule. In addition, the complaint alleges that Goal Financial misrepresented that it implemented reasonable and appropriate security measures to protect personal information from unauthorized access, in violation of Section 5 of the FTC Act. Further, the proposed complaint alleges that Goal Financial disseminated a privacy policy that does not accurately reflect its privacy practices, including its security policies and practices, in violation of the GLB Privacy Rule.

The proposed order applies to personal information Goal Financial collects from or about consumers in connection with its student loan and related services and contains provisions designed to prevent Goal Financial from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires that Goal Financial not misrepresent the extent to which it maintains and protects the

Analysis to Aid Public Comment

privacy, confidentiality, or integrity of any personal information collected from or about consumers.

Part II of the proposed order requires Goal Financial 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 it collects from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected. Specifically, the order requires Goal Financial 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 consumer information that could result in 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 Goal Financial, 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 testing and monitoring, any material changes to its operations or business arrangements, or any other

Analysis to Aid Public Comment

circumstances that it knows or has reason to know may have a material impact on the effectiveness of its information security program.

Part III of the proposed order requires that Goal Financial not violate any provision of the GLB Safeguards Rule and Privacy Rule.

Part IV of the proposed order requires that Goal Financial obtain, within 180 days after being served with the final order approved by the Commission, and on a biennial basis thereafter for ten (10) years, an assessment and report from a qualified, objective, independent third-party professional, certifying that: (1) Goal Financial has in place a security program that provides protections that meet or exceed the protections required by Parts II and IIIA 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 nonpublic personal information has been protected. This provision is substantially similar to comparable provisions obtained in prior Commission orders under the Safeguards Rule and Section 5 of the FTC Act.

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

Analysis to Aid Public Comment

The purpose of this analysis is to facilitate 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

**THE CONNECTICUT CHIROPRACTIC
ASSOCIATION,
THE CONNECTICUT CHIROPRACTIC
COUNCIL,
AND
ROBERT L. HIRTLE, ESQ.**

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

*Docket C-4217; File No. 071 0074
Complaint, April 14, 2008 – Decision, April 14, 2008*

This consent order concerns a series of agreements among competing chiropractors to boycott American Specialty Health (ASH), to preclude ASH from administering a chiropractic cost-savings benefits administration program on behalf of payors offering coverage for health care services in the State of Connecticut. The chiropractors engaged in this conduct with and through their respective trade associations, the Connecticut Chiropractic Association and the Connecticut Chiropractic Council. Respondent Robert L. Hirtle was legal counsel for the former association. The conduct in question had the purpose and effect of unreasonably restraining prices and other forms of competition among hundreds of otherwise independent chiropractors in Connecticut. The order prohibits the respondents from entering into or facilitating any agreement between or among any chiropractors to negotiate with payors on any chiropractor's behalf; to deal, not to deal, or threaten not to deal with payors; or on what terms to deal with any payor. More specifically, the order prohibits the respondents from engaging in, attempting to engage in, or inducing anyone to engage in the following actions: persuading a chiropractor to deal or not deal with a payor, or to accept or not accept the terms or conditions on which the chiropractor is willing to deal with a payor; facilitating exchanges of information between chiropractors concerning whether, or on what terms, to contract with a payor; or continuing a meeting of chiropractors after any person makes any statements regarding any chiropractor's intentions that if agreed to would violate the order, unless that person is ejected from the meeting. Certain kinds of agreements are excluded from the general bar on joint negotiations, and the associations are not prevented from exercising rights permitted under the First Amendment to the United States Constitution to petition the government. Other provisions relate to distributing the complaint and order to current and future members of the two associations and to certain payors, and impose various obligations on the respondents to report or provide access to