UNITED STATES OF AMERICA **0723013**
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Deborah Platt Majoras, Chairman**
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

In the Matter of)

GOAL FINANCIAL, LLC,)
a limited liability company.)

) **DOCKET NO. C-**

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

(1) failed to assess adequately risks to the information it collected and stored in its paper files and on its computer network;

(2) failed to restrict adequately access to personal information stored in its paper files and on its computer network to authorized employees;

(3) 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;

(4) failed to provide adequate training to employees about handling and protecting personal information and responding to security incidents; and

(5) 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, 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

   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 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 _______ day of ______________, 2008, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary