Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Goal Financial, LLC, File No. 0723013

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.

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 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 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.

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.