



Federal Trade Commission Protecting America's Consumers

For Release: March 4, 2008

Student Lender Settles FTC Charges That It Failed to Safeguard Sensitive Consumer Information and Misrepresented Its Security Practices

A student loan company has agreed to settle Federal Trade Commission charges that it failed to provide reasonable and appropriate security for consumers' sensitive personal information in violation of federal law. The proposed settlement will require the company to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 10 years.

According to the FTC's complaint, Goal Financial, LLC, collects personal information from applicants in the course of providing loans and related services. As a result of security failures, employees transferred more than 7,000 files with consumer information to third parties without authorization, and one employee sold to the public surplus hard drives that contained, in clear text, information about 34,000 consumers.

Goal Financial allegedly violated the FTC's Safeguards Rule by failing to: adequately assess the risks to consumers' personal information, adequately restrict access to this information to authorized employees, implement a comprehensive information security program, provide adequate employee training, and, in some instances, contractually require third-party service providers to protect the information. The San Diego-based company allegedly violated the FTC's Privacy Rule by providing customers with a privacy policy that contained false or misleading statements, and the FTC Act by falsely representing to consumers that it implements reasonable and appropriate measures to protect personal information.

The proposed consent order bars Goal Financial from future data security misrepresentations and requires the company to implement and maintain a comprehensive information-security program that includes administrative, technical, and physical safeguards. The settlement also requires the company to obtain, every two years for the next 10 years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order. The settlement also contains standard record-keeping provisions to allow the FTC to monitor compliance with its order.

This is the FTC's 17th case to challenge data security practices by a company handling sensitive consumer information.

The Commission vote to accept the complaint and proposed consent agreement was 5-0.

The FTC will publish an announcement regarding the agreement in the Federal Register shortly. The agreement will be subject to public comment for 30 days, until April 3, 2008, after which the Commission will decide whether to make it final. Comments should be addressed to the FTC, Office of the Secretary, Room H-159, 600 Pennsylvania Avenue, N.W., Washington, DC 20580. The FTC requests that any comment filed in paper form near the end of the public comment period be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions.

NOTE: The Commission issues a complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. The complaint is not a finding or ruling that the respondent has actually violated the law. The consent agreement is for settlement purposes only and does not constitute an admission by the respondent of a law violation.

Copies of the complaint, consent order, and an analysis to aid public comment are available from the FTC's Web site at <http://www.ftc.gov> and the FTC's Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, DC 20580. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, an avoid them. To file a complaint in English or Spanish, click <http://www.ftc.gov/ftc/complaint.shtm> or call 1-877-382-4357. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to more than 1,600 civil and criminal law enforcement agencies in the U.S. and abroad. For free information on a variety of consumer topics, click <http://ftc.gov/bcp/consumer.shtm>.

MEDIA CONTACT:

Frank Dorman
Office of Public Affairs
202-326-2674

STAFF CONTACT:

Jessica Rich
Bureau of Consumer Protection
202-326-2148

[E-mail this News Release](#)

If you send this link to someone else, the FTC will not collect any personal information about you or the recipient.

Related Documents:

[In the Matter of Goal Financial, LLC, a limited liability company.](#)

FTC File No. 072-3013

Consumer Information:

- [What To Do If Your Personal Information Has Been Compromised](#)

Business Information:

- [Protecting Personal Information Interactive Tutorial](#)
- [Protecting Personal Information: A Guide for Business](#)
- [Financial Institutions and Customer Information: Complying with the Safeguards Rule](#)
- [Fighting Back Against Identity Theft: Dealing with a Data Breach](#)

Last Modified: Tuesday, 04-Mar-2008 11:31:00 EST