052 3136

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of **SUPERIOR MORTGAGE CORPORATION, a corporation**.	**Docket C-4153**

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that Superior Mortgage Corp. 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 of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. ' 6801 *et seq*., 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 Superior Mortgage Corp. ("Superior Mortgage") is a New Jersey corporation with its principal office or place of business at 1395 Route 539, Tuckerton, New Jersey 08087. In addition to conducting business from its headquarters location in Tuckerton, Superior Mortgage conducts business through forty (40) branch offices located in ten different states, as well as through six separate websites.

2. Respondent is a direct lender that specializes in residential mortgage loans. As such, it is a "financial institution," as that term is defined in Section 509(3)(A) of the GLB Act, and is therefore subject to the requirements of the Safeguards Rule.

3. 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, 15 U.S.C. ' 44.

SAFEGUARDS RULE

4. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 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:

A. Designating one or more employees to coordinate the information security program;

B. 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;

C. Designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures;

D. Overseeing service providers, and requiring them by contract to protect the security and confidentiality of customer information; and

E. 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.

VIOLATIONS OF THE SAFEGUARDS RULE

5. Through its offices and websites, respondent has collected sensitive customer information in connection with the mortgage application process, including customer names, Social Security numbers, credit histories, and bank and credit card account numbers. Since the Rule's effective date until at least May 2005, respondent failed to implement reasonable policies and procedures to protect the security and confidentiality of the information it collects.

6. For example, respondent failed to (a) assess risks to its customer information until more than a year after the Rule's effective date; (b) institute appropriate password policies to control access to company systems and documents containing sensitive customer information; and (c) encrypt or otherwise protect sensitive customer information emailed by respondent and its service providers using networks outside of respondent's computer network. Respondent also failed to take reasonable steps to ensure that its service providers were providing appropriate security for customer information and addressing known security risks in a timely fashion.

7. By failing to implement reasonable security policies and procedures, respondent engaged in violations of the Safeguards Rule, including but not limited to:

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 and failing to regularly test and monitor them; and

C. Failing to oversee service providers to ensure that they implement safeguards to protect respondent's customer information.

8. A violation of the Safeguards Rule constitutes an unfair or deceptive act or practice in violation of Section 5(a)(1) of the FTC Act.

VIOLATIONS OF THE FTC ACT

9. Since at least 2002, respondent has collected personal information from consumers through its Online Application Form at www.supmort.com. Since at least 2003, respondent has operated five additional websites that collect personal information from consumers by linking them to the Online Application Form. This online form serves as an initial step for many consumers seeking a loan through respondent.

10. The Online Application Form collects from consumers personal information, including, but not limited to, name, address, date of birth, Social Security number, credit history, and bank and credit card account numbers.

11. Since at least 2002, respondent has disseminated or caused to be disseminated on www.supmort.com the following statement regarding the privacy and confidentiality of personal information collected through respondent's website:

> All information submitted is handled by SSL encryption -
> see the yellow padlock at the bottom of your browser.

Exhibit A (Superior Mortgage webpage dated October 25, 2004).

12. Through the means described in paragraph 11, respondent has represented, expressly or by implication, that the personal information it obtained from consumers through www.supmort.com was encrypted using SSL from the time of submission until receipt by respondent.

13. In truth and in fact, the personal information obtained from consumers through www.supmort.com was not encrypted using SSL from the time of submission until it was received by respondent. Instead, respondent encrypted sensitive personal information only while it was being transmitted between a visitor's web browser and the website's server (using SSL); once the information reached the server, which was operated by a service provider outside of respondent's computer network, it was decrypted and emailed

to respondent's headquarters and branch offices in clear, readable text. Therefore, the representation set forth in paragraph 12 was false or misleading.

14. 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 fourteenth day of December, 2005, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary