



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

April 4, 2008

Garret Rasmussen, Esq.
Orrick, Herrington & Sutcliffe LLP
Washington Harbour
3050 K Street, NW
Washington, DC 20007-5135

Re: NovaStar Financial, Inc., and NovaStar Mortgage, Inc.

Dear Mr. Rasmussen:

As you know, the Division of Privacy and Identity Protection staff has conducted an investigation into possible violations of the Fair Credit Reporting Act ("FCRA") and the Federal Trade Commission's Safeguards Rule, promulgated under the Gramm-Leach-Bliley Act, by your clients, mortgage companies NovaStar Financial, Inc., and NovaStar Mortgage, Inc. (collectively, "NovaStar"). The FTC's investigation arose from a data breach that Novastar reported to consumers in a July 2006 letter. The letter advised consumers that "an incident ha[d] occurred that may have exposed [them] to identity theft" and that their credit information "may have been accessed without [their] authorization."¹

Our investigation considered, among other things, whether NovaStar failed to implement reasonable procedures to monitor or review its employees' access to consumer reports, in violation of the FCRA or the Safeguards Rule. Section 604(f) of the FCRA prohibits a person from using or obtaining a consumer report for any purpose other than a purpose for which the report is authorized to be furnished under the Act. Further, the Safeguards Rule requires financial institutions, including mortgage companies such as NovaStar, to develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security and confidentiality of customer information. Under the Rule, companies must identify and address the reasonably foreseeable internal and external risks of disclosure or misuse of customer information, including risks in the area of employee training and management.² An employer could violate both the FCRA and the Safeguards Rule if it failed to implement reasonable procedures to monitor or review its employees' access, or to limit their unauthorized access, to consumer reports.

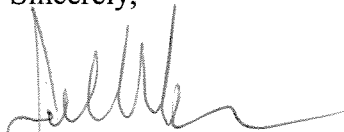
¹ It does not appear that this incident has resulted in any instances of identity theft or other fraud.

² 16 C.F.R. Part 314.

Based on all of the circumstances, staff has determined to close the investigation. In particular, staff took into account NovaStar's overall data security practices, its response to the data breach, and specific information that NovaStar provided as to its procedures to detect and prevent similar incidents. We continue to emphasize, however, that data security is an ongoing process, and that as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly. A significant number of data breaches are the result of rogue employees who take advantage of the easy access to consumers' personal information provided by their employers. Thus, we expect companies that collect or maintain such information to take appropriate steps to protect it from this risk. For companies that allow employees access to highly sensitive data, such as the data contained in consumer reports, such steps may include, depending on the circumstances: tailored access limitations based on an employee's position, functions, and workload; periodic supervisory review of an employee's activity; employee training and clear warnings regarding wrongful access to or disclosure of data; and/or the use of software or other means to monitor employee access to consumer data, place restrictions on such access, or flag suspicious activity.

The closing of this investigation is not to be construed as a determination that a violation may not have occurred, just as the pendency of an investigation should not be construed as a determination that a violation has occurred. The Commission reserves the right to take such further action as the public interest may require.

Sincerely,



Joel Winston
Associate Director
Division of Privacy and Identity Protection