Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of James B. Nutter & Company, File No. 0723108

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from James B. Nutter & Company ("JBN").

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.

The Commission's proposed complaint alleges that JBN is in the business of making and servicing mortgage loans throughout the United states. In doing so, JBN routinely obtains information from or about its customers, including, but not limited to, name; address; Social Security number; financial information; employment history; credit scores; and information contained in credit reports.

The complaint further alleges that JBN engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive information from consumers and employees, in violation of the Gramm-Leach-Bliley ("GLB") Act Safeguards Rule. In particular, JBN: (1) did not develop, implement, and maintain a comprehensive written information security program; (2) did not implement reasonable policies and procedures in areas such as employee training; (3) stored personal information in clear text on its computer network; (4) did not employ sufficient measures to prevent or detect unauthorized access to personal information on its computer network or to conduct security investigations; (5) did not assess risks to personal information it collected and stored on its computer network and in paper files; and (6) provided back-up tapes containing personal information in clear text to a third party service provider but did not require the service provider by contract to protect the security and confidentiality of the information.

According to the complaint, JBN's practices violated the Safeguards Rule by, among other things, failing to: (1) develop, implement, and maintain a comprehensive written information security program; (2) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; (3) design and implement information safeguards to control the risks to customer information and regularly test and monitor them; (4) investigate, evaluate, and adjust the information security program in light of known or identified risks; and (5) oversee service providers and require them by contract to implement safeguards to protect respondent's customer information.

In addition, the proposed complaint alleges that JBN disseminated privacy notices that did not comply with the GLB Privacy Rule. In particular: (1) JBN began providing notices in 2004 even though under the Rule notices were to be provided starting on July 1, 2001; and (2) the notices it provided did not: set out its security practices; accurately describe that customer information

would be disclosed to third parties; or accurately inform customers that they could exercise their opt-out rights at any time during the course of their loans.

The proposed order applies to personal information from or about consumers that JBN collects in connection with its lending business. The proposed order contains provisions designed to prevent the company from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires JBN to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of such information (whether in paper or electronic format) from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to JBN's size and complexity, the nature and scope of its activities, and the sensitivity of the information collected from or about consumers and employees. Specifically, the order requires JBN 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 customer information that could result in the 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 select and retain service providers capable of appropriately safeguarding personal information they receive from JBN and require service providers by contract to implement and maintain appropriate safeguards.

- Evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, or any other circumstances that it knows or has reason to know may have material impact on its information security program.

Part II of the order prohibits JBN from violating any provision of the GLB Safeguards Rule and Privacy Rule.

Part III of the proposed order requires JBN to obtain within one year, and on a biennial basis thereafter for a period of ten (10) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part I 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 sensitive consumer and employee information has been protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires JBN 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, JBN must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in company status. Part VII mandates that JBN submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part VIII 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.