

Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Nationwide Mortgage Group, Inc., and John D. Eubank, Docket No. 9319

The Federal Trade Commission (“Commission”) has accepted a consent agreement, subject to final approval, from Nationwide Mortgage Group, Inc., and John D. Eubank (collectively “Nationwide”). Nationwide is a mortgage broker with headquarters in Fairfax, Virginia. Nationwide collects sensitive customer information, including customer names, social security numbers, credit histories, bank account numbers, and income tax returns, and is a “financial institution” subject to the Gramm-Leach-Bliley Act’s Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314 (“Safeguards Rule”) and Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313 (“Privacy Rule”).

The proposed consent agreement 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.

This matter concerns Nationwide’s alleged violations of the Safeguards and Privacy Rules. The Safeguards Rule, which became effective on May 23, 2003, requires financial institutions to implement reasonable policies and procedures to ensure the security and confidentiality of customer information, including:

- Designating one or more employees to coordinate the information security program;
- 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;
- 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;
- Overseeing service providers, and requiring them by contract to protect the security and confidentiality of customer information; and
- 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.

The Privacy Rule, which became effective on July 1, 2001, requires financial institutions to provide customers with clear and conspicuous notices that explain the financial institution’s information collection and sharing practices and allow customers to opt out of having their information shared with certain non-affiliated third parties.

The Commission’s administrative complaint, issued on November 9, 2004, charges that Nationwide engaged in violations of the Safeguards Rule, specifically by: (1) failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of

customer information; (2) failing to implement information safeguards to control the risks to customer information and failing to regularly test or monitor them; (3) failing to develop, implement, and maintain a comprehensive written information security program; and (4) failing to designate one or more employees to coordinate the information security program. The complaint also alleges that Nationwide failed to provide its customers with the notice required by the Privacy Rule.

The proposed order contains provisions designed to prevent Nationwide from engaging in future practices similar to those alleged in the complaint. Specifically, Part I of the proposed order prohibits Nationwide from violating the Safeguards Rule or the Privacy Rule. Part II of the proposed order requires that Nationwide obtain, within 180 days after being served with the final order approved by the Commission, 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 that: (1) Nationwide has in place a security program that provides protections that meet or exceed the protections required by the Safeguards Rule, and (2) Nationwide's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected. This provision is substantially similar to comparable provisions obtained in prior Commission orders under Section 5 of the FTC Act. *See In the Matter of Petco Animal Supplies Inc.*, FTC File No. 032-3221 (consent order) (Placed on the public record on Nov. 17, 2004); *In the Matter of MTS, Inc., doing business as Tower Records/Books/Video, et al.*, FTC Docket No. C-4110 (consent order) (Issued May 28, 2004); *In the Matter of Guess?, Inc., and Guess.com, Inc.*, FTC Docket No. C-4091 (consent order) (Issued July 30, 2003); and *In the Matter of Microsoft Corporation*, FTC Docket No. C-4069 (consent order) (Issued Dec. 20, 2002).

Part II of the proposed order also requires Nationwide to retain documents relating to compliance. For the assessments and supporting documents, Nationwide must retain the documents for three years after the date that each assessment is prepared.

Parts III through VI of the proposed order are reporting and compliance provisions. Part III requires dissemination of the order now and in the future to all employees and other persons having responsibilities with respect to the subject matter of the order. Part IV requires Mr. Eubank to notify the FTC, for a period of ten years, if he discontinues his current business or becomes affiliated with a new one. Part V ensures notification to the FTC of changes in corporate status. Part VI mandates that Nationwide submit compliance reports to the FTC. Part VII 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.