Analysis of Proposed Consent Order
to Aid Public Comment
Nations Title Agency, Inc. File No. 0523117

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Nations Title Agency, Inc ("Nations Title"), Nations Holding Company ("Nations Holding"), and Christopher M. Likens ("Likens").

The 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.

According to the Commission's proposed complaint, Nations Holding, Nations Title, and Likens provide services in connection with financing home purchases and refinancing existing home mortgages, including, but not limited to, real estate settlement services, residential closings, title abstracts, title commitments, appraisals, foreclosure management, asset disposition, and real estate management. Likens wholly owns Nations Holding, a subchapter "S" corporation, and has the authority to control the conduct of Nations Holding and its subsidiaries, including Nations Title. In providing these services, Nations Title, Nations Holding, and Likens ("respondents") routinely obtain sensitive consumer information from banks and other lenders, real estate brokers, consumers, public records, and others, including but not limited to consumer names, Social Security numbers, bank and credit card account numbers, mortgage information, loan applications, purchase contracts, refinancing agreements, income histories, and credit histories (collectively, "personal information").

The Commission's proposed complaint alleges that respondents failed to employ reasonable and appropriate security measures to protect personal information. In particular, the proposed complaint alleges that respondents have engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. Among other things, respondents failed to: (1) assess risks to the information they collected and stored both online and offline; (2) implement reasonable policies and procedures in key areas, such as employee screening and training and the collection, handling, and disposal of personal information; (3) implement simple, low-cost, and readily available defenses to common website attacks, or implement reasonable access controls, such as strong passwords, to prevent a hacker from gaining access to personal information stored on respondents' computer network; (4) employ reasonable measures to detect and respond to unauthorized access to personal information or to conduct security investigations; and (5) provide reasonable oversight for the handling of personal information by service providers, such as third parties employed to process the information and assist in real estate closings.

The proposed complaint alleges that in April 2004, a hacker exploited these failures by using a common website attack to obtain unauthorized access to Nations Holding's computer network. In addition, in February 2005, a Kansas City television station found documents containing sensitive personal information discarded in a dumpster used by respondents located in an unsecured area adjacent to their building.

According to the complaint, respondents' practices violated the Gramm-Leach-Bliley ("GLB") Safeguards Rule because respondents failed to: (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; (2) design and implement information safeguards to control the risks to customer information and regularly test and monitor them; (3) investigate, evaluate, and adjust the information security program in light of known or identified risks; (4) develop, implement, and maintain a comprehensive written information security program; 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 respondents misrepresented that they implemented reasonable and appropriate measures to protect consumers' personal information from unauthorized access, in violation of Section 5 of the Federal Trade Commission Act ("FTC Act"). Further, the proposed complaint alleges that respondents disseminated a privacy policy that does not accurately reflect their privacy policies and practices, in violation of the GLB Privacy Rule.

The proposed order applies to personal information from or about consumers that respondents collect in connection with their real estate-related services. The proposed order contains provisions designed to prevent them from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires that respondents not misrepresent the extent to which they maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers.

Part II of the proposed order requires respondents to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information they collect from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to their size and complexity, the nature and scope of their activities, and the sensitivity of the personal information collected. Specifically, the order requires respondents 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 consumer information that could result in 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.

- Evaluate and adjust their information security program in light of the results of testing and monitoring, any material changes to their operations or business arrangements, or any other circumstances that they know or have to reason to know may have a material impact on the effectiveness of their information security program.

Part III of the proposed order requires that respondents not violate any provision of the GLB Safeguards Rule and Privacy Rule, as well as the Fair and Accurate Credit Transactions Act's Disposal Rule.

Part IV of the proposed order requires that respondents obtain within 180 days, and on a biennial basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) they have in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order, and (2) their security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected.

Parts V through X of the proposed order are reporting and compliance provisions. Part V requires respondents to retain documents relating to their compliance with the order. Part VI requires dissemination of the order now and in the future to persons with supervisory responsibilities relating to the subject matter of the order. Part VII requires Likens to notify the Commission of changes in his business or employment in connection with providing financial products or services. Part VIII requires respondents to notify the Commission of changes in their corporate status. Part IX mandates that they submit compliance reports to the FTC. Part X 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.