

Complaint

IN THE MATTER OF
NATIONS TITLE AGENCY, INC.

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4160; File No. 0523117
Complaint, June 19, 2006--Decision, June 19, 2006

This consent order relates to personal information on consumers collected by Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens. The respondents provide services in connection with financing home purchases and refinancing existing home mortgages and routinely obtain sensitive consumer information from banks and other sources. The respondents failed to employ reasonable and appropriate security measures to protect such information. The 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. It 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 order also requires that respondents not violate any provision of the Gramm-Leach-Bliley Safeguards Rule and Privacy Rule, as well as the Fair and Accurate Credit Transactions Act's Disposal Rule. In addition, the respondents must obtain periodic assessments and reports from a qualified, objective, independent third-party professional, certifying, among other things, that they have in place a security program that provides protections that meet or exceed the protections required by this order, and their security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information have been protected. Additional provisions relate to reporting and compliance.

Participants

For the Commission: *Molly Crawford, Loretta Garrison,*
Jessica Rich, Alain Sheen, and Joel Winston.

For the Respondents: *David H. Cox, Jackson & Campbell, P.C.*

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that Nations Title Agency, Inc., Nations Holding

Complaint

Company, and Christopher M. Likens have 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, Subtitle A of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801-6809; the Commission's Privacy of Customer Financial Information Rule ("Privacy Rule"), 16 C.F.R. Part 313, issued pursuant to the GLB Act; 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 Nations Title Agency, Inc. ("NTA") is a Kansas corporation with its principal office or place of business at 9415 Nall Avenue, Prairie Village, Kansas 66207. Respondent NTA is a wholly-owned subsidiary of respondent Nations Holding Company.

2. Respondent Nations Holding Company ("NHC") is a Kansas corporation with its principal office or place of business at 5370 West 95th Street, Prairie Village, Kansas 66207. NHC conducts business through its 57 wholly-owned subsidiaries, including NTA, in twenty states. During all relevant time, NHC controlled the practices at issue in this complaint.

3. Respondent Christopher M. Likens ("Likens") is president and sole owner of NHC, a Subchapter "S" corporation, and NHC's wholly-owned subsidiaries. He has the authority to control the conduct of NHC and its subsidiaries, including NTA. Individually or in concert with others he formulates, directs, or controls the policies, acts, or practices of the respondent corporations, including the acts or practices alleged in this complaint. His principal office or place of business is the same as NHC.

4. Respondents 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. In providing these services, respondents routinely

Complaint

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”).

5. Since at least 2003, 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.

6. In April 2004, a hacker exploited the failures set forth in Paragraph 5 by using a common website attack to obtain unauthorized access to NHC’s computer network. In addition, in February 2005, a Kansas City television station found intact documents containing sensitive personal information discarded in respondents’ dumpster in an unsecured area adjacent to respondents’ building.

7. The acts and practices of respondents 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.

Complaint

VIOLATIONS OF THE SAFEGUARDS RULE

8. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), 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: (1) designating one or more employees to coordinate the information security program; (2) 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; (3) 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; (4) overseeing service providers, and requiring them by contract to protect the security and confidentiality of customer information; and (5) 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.

9. Respondents NHC and NTA are “financial institutions,” as that term is defined in Section 509(3)(A) of the GLB Act.

10. As set forth in Paragraphs 5 and 6, respondents have failed to implement reasonable security policies and procedures, and have thereby engaged in violations of the Safeguards Rule, by, among other things:

- a. Failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;

Complaint

- b. Failing to design and implement information safeguards to control the risks to customer information and failing to regularly test and monitor them;
- c. Failing to investigate, evaluate, and adjust the information security program in light of known or identified risks;
- d. Failing to develop, implement, and maintain a comprehensive written information security program; and
- e. Failing to oversee service providers and to require them by contract to implement safeguards to protect respondent's customer information.

VIOLATIONS OF THE FTC ACT

11. Since at least 2001, respondents NHC, NTA, and Likens have disseminated or caused to be disseminated to consumers privacy policies and statements, including, but not limited to the following:

NTA, at all times, strives to maintain the confidentiality and integrity of the personal information in its possession and has instituted measures to guard against its unauthorized access. We maintain physical, electronic and procedural safeguards in compliance with federal standards to protect the information. (Nations Title Agency Privacy Policy.)

12. Through the means set forth in Paragraph 11, respondents have represented, expressly or by implication, that they implement reasonable and appropriate measures to protect consumers' personal information from unauthorized access.

13. In truth and in fact, as set forth in Paragraphs 5 and 6, respondents did not implement reasonable and appropriate measures

Complaint

to protect consumers' personal information from unauthorized access. Therefore, the representation set forth in Paragraph 12 was, and is, false or misleading, in violation of Section 5(a) of the Federal Trade Commission Act.

VIOLATION OF THE PRIVACY RULE

14. The Privacy Rule, which implements Sections 501-509 of the GLB Act, 15 U.S.C. §§ 6801-6809, was promulgated by the Commission on May 24, 2000, and became effective on July 1, 2001. The Rule requires financial institutions to provide customers, no later than when a customer relationship arises and annually for the duration of that relationship, "a clear and conspicuous notice that accurately reflects [the financial institution's] privacy policies and practices" including its security policies and practices. 16 C.F.R. §§ 313.4(a); 313.5(a)(1); § 313.6(a)(8).

15. As set forth in Paragraphs 11 through 13, respondents disseminated a privacy policy that contained false or misleading statements regarding the measures implemented to protect consumers' personal information. Therefore, respondents have disseminated a privacy policy that does not accurately reflect their privacy policies and practices, including their security policies and practices, in violation of the Privacy Rule.

16. The acts and practices of respondents 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 nineteenth day of June, 2006, has issued this complaint against respondents.

By the Commission.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondents named in the caption hereof, and the Respondents, having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondents with violations of the Gramm-Leach Bliley Act, 15 U.S.C. 6801 *et seq.* and the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*

The Respondents, their attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondents of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondents that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondents have violated the said Acts, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Proposed respondent Nations Title Agency, Inc. (“Nations Title”) is a Kansas corporation with its principal office or place of business at 9415 Nall

Decision and Order

Avenue, Prairie Village, Kansas 66207. NTA is a wholly-owned subsidiary of Nations Holding Company.

2. Proposed respondent Nations Holding Company (“Nations Holding”) is a Kansas corporation with its principal office or place of business at 5370 West 95th Street, Prairie Village, Kansas 66207. Nations Holding is a Subchapter “S” corporation.
3. Proposed respondent Christopher M. Likens is president and sole owner of Nations Holding. Individually or in concert with others, he formulates, directs, or controls the policies, acts, or practices of the respondent corporations. His principal office or place of business is the same as that of Nations Holding.

ORDER**DEFINITIONS**

For purposes of this Order, the following definitions shall apply:

1. “Personally identifiable information” or “personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) a bank, loan, or credit card account number; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any information that is combined with any of (a) through (g) above.

Decision and Order

2. Unless otherwise specified, “respondents” shall mean Nations Holding and Nations Title and their successors and assigns, officers, agents, representatives, subsidiaries, affiliates, and employees, and Christopher M. Likens, individually and as an officer of Nations Holding.
3. All other terms are synonymous in meaning and equal in scope to the usage of such terms in the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*
4. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondents, directly or through any corporation, subsidiary, division, or other device, in connection with the collection of personally identifiable information from or about consumers, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondents, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to

Decision and Order

respondents' size and complexity, the nature and scope of respondents' activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. the evaluation and adjustment of respondents' information security program in light of the results of the testing and monitoring required by Part II.C., any material changes to respondents' operations or business arrangements, or any other circumstances that respondents know or have reason to know may have a material impact on the effectiveness of their information security program.

Decision and Order

III.

IT IS FURTHER ORDERED that respondents shall not, directly or through any corporation, subsidiary, division, website, or other device, violate any provision of:

- A. the Gramm-Leach-Bliley Act's Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314;
- B. the Gramm-Leach-Bliley Act's Privacy of Customer Financial Information Rule, 16 C.F.R. Part 313; or
- C. the Fair and Accurate Credit Transactions Act's Disposal of Consumer Report Information and Records Rule, 16 C.F.R. Part 682.

In the event that any of these Rules is hereafter amended or modified, respondents' compliance with that Rule as so amended or modified shall not be a violation of this order.

IV.

IT IS FURTHER ORDERED that, in connection with their compliance with Parts II, III.A., and III.C. of this order, respondents shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondents have implemented and maintained during the reporting period;

Decision and Order

- B. explain how such safeguards are appropriate to respondents' size and complexity, the nature and scope of respondents' activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by the Parts II, III.A., and III.C. of this order; and
- D. certify that respondents' security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondents shall provide the initial Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of either respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondents until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

Decision and Order

V.

IT IS FURTHER ORDERED that respondents shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

- A. for a period of five (5) years: any documents, whether prepared by or on behalf of either respondent, that contradict, qualify, or call into question respondents' compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Part IV of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of either respondent, relating to respondents' compliance with Parts II, III.A., and III.C. of this order for the compliance period covered by such biennial Assessment.

VI.

IT IS FURTHER ORDERED that respondents shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondents shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent Christopher M. Likens, for a period of ten (10) years, after the date of issuance of this order, shall notify the Commission of the discontinuance of his current business or employment, or of his affiliation with any new

Decision and Order

business or employment that provides financial products or services. The notice shall include respondent Christopher M. Likens's new business address and telephone number and a description of the nature of the business or employment and his duties and responsibilities. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

IT IS FURTHER ORDERED that respondents and their successors and assigns shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondents learn less than thirty (30) days prior to the date such action is to take place, respondents shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

IX.

IT IS FURTHER ORDERED that respondents and their successors and assigns shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

Decision and Order

X.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that one or both of the respondents did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to that respondent(s) will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis to Aid Public Comment

Analysis of Proposed Consent Order to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

FRESENIUS AG

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 7 OF THE CLAYTON ACT AND SEC. 5 OF THE FEDERAL TRADE
COMMISSION ACT

Docket C-4161; File No. 0510154
Complaint, March 13, 2006--Decision, June 19, 2006

This consent order addresses the acquisition by respondent Fresenius AG of Renal Care Group, Inc. The combined firm would be the largest provider of outpatient dialysis services in the United States and would likely be able to exercise unilateral market power. The order requires Fresenius to divest 91 outpatient dialysis clinics, and Renal Care Group's joint venture equity interests in 12 additional clinics, to National Renal Institutes, Inc. (NRI). To ensure that NRI will have the assets necessary to operate the divested clinics in a competitive manner, Fresenius is required to obtain the agreement of the medical directors affiliated with the divested clinics to continue providing physician services after the transfer of ownership, to obtain the consent of all lessors necessary to assign the leases for the real property associated with the divested clinics to NRI, and to provide NRI with the opportunity to interview and hire employees affiliated with the divested clinics. The order prevents Fresenius from contracting with the medical directors (or their practice groups) affiliated with the divested clinics for three years. The order requires Fresenius to provide NRI with a license to Fresenius's policies and procedures, as well as the option to obtain Fresenius's medical protocols. In addition, Fresenius will provide transition services to NRI for a period of 12 months to ensure continuity of patient care and records. The order also requires Fresenius to provide prior notice to the Commission of its planned acquisitions of dialysis clinics located in the 66 markets addressed by the order to ensure that subsequent acquisitions do not adversely impact competition in the markets at issue and undermine the remedial goals of this order.

Participants

For the Commission: *Linda B. Blumenreich, Robert S. Canterman, Mary Connelly-Draper, Richard Cunningham, Jeffrey Dahnke, Daniel P. Ducore, Erin Dwyer-Frazier, Melea E. Greenfeld, Stephen F. Krebs, John Lambright, William Layher, Martha H. Oppenheim, David R. Pender, Eric Rohlck, Elizabeth Schneirov, Gary H. Schorr, and Karan R. Singh.*