

Complaint

IN THE MATTER OF

JAMES B. NUTTER & COMPANYCONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT AND THE
GRAMM-LEACH-BLILEY ACT SAFEGUARDS RULE

Docket No. C-4258; File No. 072 3108
Complaint, June 12, 2009 – Decision, June 12, 2009

This consent order addresses James B. Nutter & Company's ("JBN") failure to provide reasonable and appropriate security for sensitive information obtained from or about its consumers when making and servicing mortgage loans throughout the United States. According to the complaint JBN failed 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. Additionally, disseminated privacy notices that did not comply with the GLB Privacy Rule. The order requires JBN to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of sensitive consumer information (whether in paper or electronic format) and prohibits JBN from violating any provision of the GLB Safeguards Rule and Privacy Rule.

Participants

For the *Commission*: *Loretta H. Garrison and Alain Sheer.*

For the *Respondent*: *Jonathan Rosen, Shook, Hardy & Bacon, L.L.P.*

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that James B. Nutter & Company has violated the provisions of the Commission's Standards for Safeguarding

Complaint

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, and the Commission’s Privacy of Customer Financial Information Rule (“Privacy Rule”), 16 C.F.R. Part 313, issued pursuant to the GLB Act; and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent James B. Nutter & Company is a privately-held Missouri company with its principal office or place of business at 4153 Broadway, Kansas City, Missouri 64111.

2. The acts and practices of respondent alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act (“FTC Act”).

3. Respondent makes and services single-family residential mortgage loans throughout the United States.

4. Respondent routinely collects sensitive personal information from or about consumers. The information includes, among other things: name; street and email addresses; telephone number; Social Security number; driver’s license number; date of birth; bank and credit card account numbers; mortgage information; and income, debt, employment, and credit histories (collectively, “personal information”).

5. Respondent operates a computer network in conducting its lending business. Among other things, it uses the network to: (1) obtain personal information from consumers (through www.jamesbnutter.com) and others, such as credit reporting agencies; (2) maintain and store personal information; (3) prepare paper documents that contain personal information, such as loan applications; (4) approve and decline loan applications; (5) store electronic copies of closing documents for approved loans; (6) service loans and maintain loan servicing histories; and (7) prepare back-up tapes that contain the personal information of borrowers.

Complaint

Further, respondent uses the network to provide email service and internet access.

6. Since at least September 1, 2004 until at least November 2008, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information. In particular, respondent:

- a. did not develop, implement, and maintain a comprehensive written information security program;
- b. did not implement reasonable policies and procedures in areas such as employee training in safeguarding personal information;
- c. stored personal information in clear readable text on its computer network, creating an unnecessary risk to the information;
- d. did not employ sufficient measures to prevent or detect unauthorized access to personal information on its computer network or to conduct security investigations, such as monitoring and controlling connections between the network and the internet or regularly reviewing activity on the network;
- e. did not assess risks to the personal information it collected and stored on its computer network and in paper files; and
- f. provided back-up tapes containing personal information in clear readable 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.

As a result, an intruder was able to direct respondent's computer network to send millions of outgoing spam emails without its knowledge, and could have accessed personal information without authorization.

Complaint

7. Respondent began providing privacy notices to customers in 2004. The notices it provided: (1) did not set out respondent's security practices; (2) did not accurately inform customers that respondent disclosed customer information to third parties, such as credit reporting agencies; and (3) informed customers that they had 30 days in which to exercise their opt-out rights, even though the Privacy Rule provides that they can opt out at any time during the course of their loans.

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. Respondent is a "financial institution," as that term is defined in Section 509(3)(A) of the GLB Act.

Complaint

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

- a. failing to develop, implement, and maintain a comprehensive written information security program;
- b. failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information;
- c. failing to design and implement safeguards to control the risks to personal information and failing to regularly test and monitor them;
- d. failing to investigate, evaluate, and adjust the information security program in light of known or identified risks; and
- e. failing to oversee service providers and to require them by contract to implement safeguards to protect personal information.

VIOLATIONS OF THE PRIVACY RULE

11. 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 notice that, among other things, sets out the institution's security practices, accurately describes its disclosures of customer information to third parties, and accurately informs customers of their opt-out rights. 16 C.F.R. Part 313.

12. As set forth in Paragraph 7, respondent violated the Privacy Rule by failing to provide privacy notices for several years after the Rule became effective, and thereafter by providing notices that failed to set out respondent's security practices; did not accurately

Decision and Order

describe to customers that customer information would be disclosed to third parties, such as credit reporting agencies; and informed customers that they had 30 days in which to exercise their opt-out rights even though the Rule provides that they can opt out at any time during the course of their loans.

13. Pursuant to the GLB Act, violations of the Safeguards Rule and the Privacy Rule are enforced through the FTC Act.

THEREFORE, the Federal Trade Commission this twelfth day of June, 2009, has issued this complaint against respondent James B. Nutter & Company.

By the Commission.

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent 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 Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq*;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent 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 Respondent that the law has been violated as alleged in such

Decision and Order

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 Respondent has violated the said Act, 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, 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. Respondent James B. Nutter & Company is a Missouri corporation with its principal office or place of business at 4153 Broadway, Kansas City, Missouri 64111.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

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

1. "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; (d) a telephone number; (e) a Social Security number; (f) a driver's license number; (g) a bank, loan, mortgage, credit card, or debit card account number; (h) a persistent identifier, such as a customer number held in a

Decision and Order

“cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information that is combined with any of (a) through (h) above.

2. Unless otherwise specified, “respondent” shall mean James B. Nutter & Company and its subsidiaries, divisions, and affiliates, and successors and assigns.
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.*, or as may hereafter be amended.
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 respondent, and its officers, agents, representatives, and employees, 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 the size and complexity of respondent’s operations, the nature and scope of respondent’s 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;

Decision and Order

- 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 development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of respondent's information security program.

Decision and Order

II.

IT IS FURTHER ORDERED that respondent, and its officers, agents, representatives, and employees, shall not, directly or through any corporation, subsidiary, division, or other device, violate any provision of:

- A. the Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314; or
- B. the Privacy of Customer Financial Information Rule, 16 C.F.R. Part 313.

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

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Parts I and IIA of this order, respondent, and its officers, agents, representatives, and employees, shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses 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 ten (10) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to the size and complexity of respondent’s operations, the nature and scope

Decision and Order

of respondent's 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 Parts I and IIA of this order; and
- D. certify that respondent's 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.

Respondent shall provide the initial 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 respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request, make available to the Federal Trade Commission for inspection and copying:

Decision and Order

- A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including but not limited to documents, prepared by or on behalf of respondent that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and IIA of this order, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent 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 responsibilities relating to the subject matter of this order. Respondent 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.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the company 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 company; 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 company name or address. *Provided, however,* that, with

Decision and Order

respect to any proposed change in the company about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent 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.

VII.

IT IS FURTHER ORDERED that respondent shall, within sixty (60) 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.

VIII.

This order will terminate on June 12, 2029, 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 respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though

Analysis to Aid Public Comment

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 OF CONSENT ORDER TO AID PUBLIC
COMMENT**

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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

CVS CAREMARK CORPORATIONCONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT*Docket No. C-4259; File No. 072 3119**Complaint, June 18, 2009 – Decision, June 18, 2009*

This consent order addresses CVS Caremark Corporation's failure to provide reasonable and appropriate security for sensitive information routinely obtained from consumers and employees. The complaint alleges that CVS failed to: (1) implement policies and procedures to dispose securely of such information, including, but not limited to, policies and procedures to render the information unreadable in the course of disposal; (2) adequately train employees to dispose securely of such information; (3) use reasonable measures to assess compliance with its established policies and procedures for the disposal of such information; or (4) employ a reasonable process for discovering and remedying risks to such information. Additionally, CVS pharmacies discarded materials containing sensitive information in clear readable text in unsecured, publicly-accessible trash dumpsters on numerous occasions. The order prohibits misrepresentations about the security, confidentiality, and integrity of sensitive information and requires CVS to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of sensitive personal information (whether in paper or electronic format) about consumers, employees, and those seeking to become employees.

Participants

For the *Commission*: *Loretta Garson and Alain Sheer.*

For the *Respondent*: *Anthony E. DiResta and Mark S. Melodia, ReedSmith LLP.*

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that CVS Caremark Corporation ("respondent" or "CVS") has violated the provisions of the Federal Trade Commission Act,