



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](http://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. 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:
  - (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 in safeguarding personal information;
  - (3) stored personal information in clear readable text on its computer network, creating an unnecessary risk to the information;
  - (4) 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;
  - (5) did not assess risks to the 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 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.

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.
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:
  - (1) failing to develop, implement, and maintain a comprehensive written information security program;
  - (2) failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information;
  - (3) failing to design and implement safeguards to control the risks to personal information and failing to regularly test and monitor them;
  - (4) failing to investigate, evaluate, and adjust the information security program in light of known or identified risks; and
  - (5) 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 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 \_\_\_\_\_ day of \_\_\_\_\_, 2009, has issued this complaint against respondent James B. Nutter & Company.

By the Commission.

Donald S. Clark  
Secretary