Analysis of Proposed Consent Order to Aid Public Comment

In the Matter of MTS, Inc., d/b/a Tower Records/Books/Video, and Tower Direct, LLC, d/b/a TowerRecords.com
File No. 032-3209

The Federal Trade Commission has accepted a consent agreement, subject to final approval, from MTS, Inc., and Tower Direct, LLC ("Tower"). Tower sells music and video recordings, books, and other entertainment products through retail stores and its Web site, TowerRecords.com.

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 other appropriate action or make final the agreement's proposed order.

This matter concerns alleged representations about the security of personal information collected online through TowerRecords.com, Tower's online store. According to the Commission's complaint, Tower offers its online customers an order status page that allows customers to confirm their orders and view their order information. In December 2002, Tower redesigned the "check out" portion of its Web site, including the order status page. As alleged in the Commission's complaint, the redesigned version of the order status page contained a security flaw that allowed any user of the site that entered a valid order number to view the personal identifying information and order history of the Tower customer who placed the order, including name, email address, billing address, shipping address, telephone number, and items ordered since 1996.

The complaint charges that Tower falsely represented that it implemented reasonable and appropriate measures to protect the privacy and confidentiality of personal information. In particular, the complaint alleges that Tower failed to implement procedures that were reasonable and appropriate to detect and prevent vulnerabilities in its Web site, including reasonable and appropriate procedures for writing and revising Web-application code.

The proposed order applies to Tower's collection and storage of personal information from or about consumers in connection with its online business. It contains provisions designed to prevent Tower from future engagement in practices similar to those alleged in the complaint. The proposed order is substantially similar to the orders obtained by the Commission in the cases of *Eli Lilly, Inc*., FTC Docket No. C-4047 (May 8, 2002); *Microsoft Corp*., FTC Docket No. C-4069 (Dec. 20, 2002); and *Guess, Inc*., FTC Docket No. C-4091 (July 30, 2003).

Part I of the proposed order prohibits Tower, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service, from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or security of any

personal information collected from or about consumers.

Part II of the proposed order requires Tower 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 collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Tower's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires Tower 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. At a minimum, this risk assessment must include consideration of risks in each area of relevant operation.
- 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 its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Tower knows or has reason to know may have material impact on its information security program.

Part III of the proposed order requires that Tower obtain within one year, and on a biannual basis thereafter for ten (10) years, an assessment and report from a qualified, objective, independent third-party professional, certifying that: (1) Tower has in place a security program that provides protections that meet or exceed the protections required by Part II of this order; and (2) Tower'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.

Parts IV through VII of the proposed order are reporting and compliance provisions. Part IV requires Tower to retain documents relating to compliance. For most records, the order requires that the documents be retained for a five-year period. For the assessments and supporting documents, Tower must retain the documents for 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 corporate status. Part VII mandates that Tower submit

compliance reports to the FTC. Part VIII 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.