032-3209

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Timothy J. Muris, Chairman**
Mozelle W. Thompson
Orson Swindle
Thomas B. Leary
Pamela Jones Harbour

In the Matter of	)	
MTS, INC., d/b/a TOWER RECORDS/BOOKS/VIDEO, a corporation,	)	**DOCKET NO. C-4110**
and	)	
TOWER DIRECT, LLC, d/b/a TOWERRECORDS.COM, a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that MTS, Inc., and Tower Direct, LLC, corporations ("Respondents") have violated 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 MTS, Inc., is a California corporation doing business as Tower Records/Books/Video with its principal office or place of business at 2500 Del Monte, West Sacramento, California 95691.

2. Respondent Tower Direct, LLC, is a Delaware limited liability company doing business as TowerRecords.com and is a subsidiary of Respondent MTS, Inc. Its principal office or place of business is also at 2500 Del Monte, West Sacramento, California 95691.

3. On February 9, 2004, Respondents and related entities filed voluntary petitions for relief under the reorganization provisions of Chapter 11 of the Bankruptcy Code, Title 11 U.S.C. 101 et seq., in the United States Bankruptcy Court for the District of Delaware, Case Nos. 04-10393-PJW through 04-10398-PJW, 04-10400-PJW, and 04-10403-PJW

through 04-10410-PJW. On February 10, 2004, the bankruptcy cases were consolidated for administration, and a confirmation hearing was set for March 15, 2004. Pursuant to 11 U.S.C. §§ 1106 and 1107, the Respondents remain in possession of their business and property as debtors-in-possession.

4. The acts and practices of respondents as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

5. Respondents have marketed and sold music and video recordings, books, and other entertainment products through the Internet at their Web site, www.TowerRecords.com (the "Tower Web site") since at least 1996. Respondents collect personal information from consumers who visit the Tower Web site and purchase Tower products online. This personal information includes name, billing address, shipping address, email address, telephone number, and all Tower products purchased online – such as music and video recordings, books, and other entertainment products – since 1996.

6. Consumers who purchase products on the Tower Web site are assigned an order number and interact with Respondents' Web site using a software program called an "application." One of these applications is the Order Status application, which allows consumers to use their order number to view their purchase history.

7. Since at least 1997, Respondents have disseminated or have caused to be disseminated various privacy policies on the Tower Web site, including but not necessarily limited to the attached Exhibit A, containing the following statements regarding the privacy and confidentiality of personal information collected through Respondents' Web site:

> **Security & Privacy Information**
>
> * * *
>
> Your privacy is important to us. TowerRecords.com is committed to safeguarding your privacy online. We will never share your personal information with anyone for any reason without your explicit permission.
>
> * * *
>
> **How does TowerRecords.com protect my personal information?**
> We use state-of-the-art technology to safeguard your personal information. All TowerRecords.com employees are required to acknowledge that they understand and will comply with this privacy policy. Employees who violate this policy will be subjected to disciplinary action, up to and including termination.

* * *

> **What security precautions are in place to protect the loss, misuse, or alteration of my information?**
> Your TowerRecords.com Account information is password-protected. You and only you have access to this information . . . TowerRecords.com takes steps to ensure that your information is treated securely and in accordance with the relevant Terms of Service and this Privacy Policy. Unfortunately, no data transmission over the Internet can be guaranteed 100% secure. While we strive to protect your personal information, TowerRecords.com cannot ensure or warrant the security or services, and you do so at your own risk. Once we receive your transmission, we make our best effort to ensure its security on our systems.

Exhibit A, Tower Web Site Privacy Policy, December 2002 (emphasis in original).

8. In November and December 2002, Respondents redesigned the "check out" portion of their Web site and rewrote the software code for the Order Status application. In rewriting the code, Respondents failed to ensure that all of the code from the original version had been rewritten and included, as appropriate, in the new version. As a result, the rewritten version of the Order Status application failed to include any "authentication code" to ensure that the consumer viewing purchase history information was the consumer to whom such information related. The rewritten code generated an email to consumers confirming their order and providing a URL that they could use to check the status of their order online (the "Order Status URL"). The Order Status URL contained the order number in clear text.

9. The omission of authentication code and the inclusion of the order number in the Order Status URL created a commonly known and reasonably foreseeable vulnerability in the Order Status application often referred to as "broken account and session management." Any visitor to the Tower Web site who entered a valid order number in the Order Status URL could view certain personal information relating to other Tower consumers, specifically, the consumer's name, billing and shipping addresses, email address, phone number, whether the product purchased was a gift, and all Tower products purchased online. The vulnerability lasted for eight days and was exploited by a number of visitors to the site. In December 2002, personal information relating to approximately 5,225 consumers was accessed by unauthorized users, and at least two Internet chat rooms contained postings about the vulnerability as well as comments about some consumers' purchases.

10. Respondents created this vulnerability by failing to implement procedures that were reasonable and appropriate to detect and prevent vulnerabilities in their Web site and applications, including reasonable and appropriate procedures for writing and revising

Web-application code. Among other things, Respondents failed to: implement appropriate checks and controls on the process of writing and revising Web applications; adopt and implement policies and procedures regarding security tests for its Web applications; and provide appropriate training and oversight for their employees regarding Web application vulnerabilities and security testing.

11. The security risks associated with broken account and session management are widely known in the information technology industry, as are simple, publicly available measures to prevent such vulnerabilities. Security experts have been warning the industry about these vulnerabilities since at least 2000, when at least one security organization also developed and made freely available security education materials which could alert industry about how to prevent such vulnerabilities.

12. Through the means described in Paragraph 7, Respondents have represented, expressly or by implication, that they implemented measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers through the Tower Web site.

13. In truth and in fact, Respondents did not implement measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers through the Tower Web site. In particular, as set forth in Paragraph 10, Respondents failed to implement procedures that were reasonable and appropriate to detect and prevent vulnerabilities in their Web site and applications, including reasonable and appropriate procedures for writing and revising Web-application code. Therefore, the representation set forth in Paragraph 12 was false or misleading.

14. 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, on this twenty-eighth day of May, 2004, has issued this complaint against Respondents.

By the Commission.

Donald S. Clark
Secretary