

Complaint

IN THE MATTER OF

**MTS, INC., d/b/a TOWER RECORDS/BOOKS/VIDEO, ET
AL.**CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT*Docket C-4110; File No. 0323209
Complaint, May 28, 2004--Decision, May 28, 2004*

This consent order addresses the manner in which Respondents MTS, Inc., doing business as Tower Records/Books/Video, and Tower Direct, LLC – (“Tower”) – which together sell music and video recordings, books, and other entertainment products through retail stores and their Web site, TowerRecords.com.– handle the security of personal information collected online through their online store. The order, among other things, 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. The order also 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. In addition, the order requires Tower to 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 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.

Participants

For the Commission: *Laura Mazzarella, James Silver, Jessica L. Rich, and Joel Winston.*

For the Respondents: *Alan R. Malasky, Porter Wright Morris & Arthur LLP.*

Complaint

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

Complaint

“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

Complaint

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 of 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

Complaint

“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

Complaint

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.

Exhibit A

Welcome to TowerRecords.com! Already a customer? [Sign In.](#)

[TowerRecords.co.uk](#)

TOWER RECORDS.COM™



home



bag



account



order status



wish list



help

Search:

In:

All Music

GO!

[Advanced Search](#)

[MUSIC](#)

[CLASSICAL](#)

[DVD/VHS](#)

[DISCOVER](#)

[TOYS](#)

[ACCESSORIES](#)

[SALE!](#)

[GIFTS](#)

Security & Privacy Information

[Return to Main Help Page](#)

TowerRecords.com Commitment to Safe Internet Shopping

We guarantee that every order you place with TowerRecords.com will be safe and secure. We offer 128-bit SSL encryption, which encrypts your personal and credit card information as it is transferred over the Internet.

We electronically verify each order with the credit company at the moment it is placed, returning an order confirmed message **only** if the issuing bank authorizes it. Our experienced staff then manually checks all orders which still appear unusual, canceling any we feel are not valid.

In the event of unauthorized use of your credit card, federal law states that you will not be liable for more than \$50 of fraudulent charges. TowerRecords.com will cover this liability, up to \$50, as long as the following is true:

1. You have reported the fraudulent use to the issuing bank of your credit card according to their reporting rules and procedures.
2. The unauthorized use of your credit card resulted through no fault of your own.
3. The credit card number was obtained from purchases made at TowerRecords.com while using our secure server.

Shopping online with TowerRecords.com is perfectly safe. Give it a try!

[Return To the Top](#)

Cookies

Cookies are small files containing alphanumeric identifiers that we transfer through your web browser to your computer's hard drive in order for our systems to recognize your browser. We use cookies to enhance your browsing and shopping experience on the TowerRecords.com site. The

information captured makes it possible for us to:

- Keep track of items in your shopping bag during current and future visits to TowerRecords.com
- Remember information so you don't have to re-enter it each time you visit the TowerRecords.com site
- Speed navigation
- Provide you with custom tailored content
- Monitor the effectiveness of our marketing email campaigns
- Monitor total number of visitors, pages viewed, and other aggregate metrics
- Track your entries, submissions, and status in some of our promotions, sweepstakes and contests

Most browsers automatically accept cookies, but you can choose to have your browser warn you every time a cookie is being sent to you, or you can disable cookies altogether. It is possible to shop our site without enabling cookies on your browser. The "help" portion of the toolbar on most browsers will tell you how to modify your cookie settings. Please note: If you turn off the cookies feature, you will not be able to take advantage of all the special features that TowerRecords.com offers.

[Return To the Top](#)

Your Personal Information

- [What personal information do we collect?](#)
- [How is your personal information used?](#)
- [Who is collecting your personal information?](#)
- [With whom is your personal information shared?](#)
- [What choices do I have on the collection, use and distribution of my personal information?](#)
- [How can I access, update or delete my personal information?](#)
- [How does TowerRecords.com protect your personal information?](#)
- [What kind of security precautions are in place to protect the loss, misuse, or alteration of your personal information?](#)
- [What else you should know about your online privacy?](#)

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.

Please read the following policy to understand how your personal information will be treated as you make full use of our many offerings.

What personal information do we collect?

You will be asked to provide your email, billing and shipping addresses during

registration.

In addition to registration we may ask you for personal information at other times, including (but not limited to) when you enter a sweepstakes, contest or promotion sponsored by TowerRecords.com and/or our many partners; and when you report a problem with one of our sites or services.

If you contact TowerRecords.com, we may keep a record of that correspondence. Occasionally we ask users to complete surveys used for research purposes to improve and enhance TowerRecords.com. Wherever TowerRecords.com collects personal information, we make an effort to include a link our Privacy Policy.

[Return To Questions](#)

How does TowerRecords.com use my information?

The primary goal in collecting personal information is to provide you with personalized services and interactive communications.

Who is collecting information?

When asked for personal information at TowerRecords.com, you are sharing that information with TowerRecords.com alone. However, some data collected during a promotion may be shared with the sponsor. If data will be shared, you will be notified prior to the time of data collection or transfer. You can decide not to participate in the promotion if you don't want your data to be shared.

With whom does TowerRecords.com share my information?

TowerRecords.com does not sell, trade or rent your personal information to others. We will not disclose any of your personally identifiable information except when we have your permission or under special circumstances, such as when we believe in good faith that the law requires it. The exception: TowerRecords.com may share your personal information with our contractors to improve services to you, but only if the contractor agrees to keep such information confidential.

[Return To Questions](#)

What choices do I have on the collection, use, and distribution of my personal information?

You can instruct us to have your name and address removed from our mailing list at any time.

How can I access, update or delete my personal information?

You may edit your TowerRecords.com Account information at any time by using your email address and password. Your TowerRecords.com Account can be deleted or deactivated, but doing so will result in not being able to access any members-only areas of TowerRecords.com.

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.

[Return To Questions](#)**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. You may edit your TowerRecords.com Account information by using your email address and password.

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 to be 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.

What else should I know about my privacy?

Please keep in mind that whenever you voluntarily disclose personal information online (message boards, email, chat areas, etc.) - that information can be collected and used by others. You are solely responsible for maintaining the secrecy of your passwords and/or any account information. Please be careful and responsible whenever you are online.

[Return To the Top](#)

Password Protection

If you forget the password you created for your TowerRecords.com Account and the "hint" feature doesn't help you remember it, you can request that your password be emailed to you by typing your username in [here](#). Your password can only be sent to the email address you provided on your account.

If you receive a password reminder via email and you have not requested it, another customer may have made a typographical error when trying to sign in to their account. In such a situation, your password can only be sent to you, and never another user.

[Return To the Top](#)

[Pricing Policy](#) | [Return Policy](#) | [Privacy Policy](#)
| [Shipping Rates](#) | [Jobs @ Tower](#)
[Affiliate Program](#) | [Corporate Gifts](#) | [Tower](#)
[Franchises](#) | [Site Map](#) | [Help](#) | [Contact Us](#)

Choose your currency:

USD United States Dollars

GO!

[Bottom of Form](#)

[Music](#) | [Classical](#) | [DVD/VHS](#) | [Discover](#) | [Toys](#) | [Accessories](#) | [Sale!](#) | [Gifts](#) | [Stores](#)

Order by Phone: 1-800-ASK-TOWER **Order by Fax: 1-800-538-6938**
Shop AOL: Keyword: Tower
Phone Outside USA: 916-373-3050 **Fax Outside USA: 916-373-2930**

Copyright 2002 MTS, Incorporated.

Tower, Tower Records, TowerRecords.com, Tower CD Listening Station, Tower Outlet, Tower Records Videos Books, Tower Essentials, Tower Gift Card, Pulse! and associated logos are trademarks and/or registered trademarks of MTS, Incorporated in the United States and other countries.

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 violation of 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 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 MTS, Inc., d/b/a Tower Records/Books/Video, is a California corporation with its principal office or place of business at 2500 Del Monte, West Sacramento, California 95691.

Decision and Order

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

3. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondents, 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 that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) 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 (g) any other information from or about an individual consumer that is combined with (a) through (f) above.

2. Unless otherwise specified, “Respondents” shall mean MTS, Inc., and its successors and assigns (including the reorganized debtor or any entity in which property of the bankruptcy estate vests pursuant to any confirmed plan) officers, agents, representatives, and employees; Tower Direct, LLC, and its successors and assigns (including the reorganized debtor or any entity in which property of the bankruptcy estate vests pursuant to any confirmed plan), officers, agents, representatives, and

Decision and Order

employees; and both of them and their successors and assigns, officers, agents, representatives, and employees.

3. “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 online advertising, marketing, promotion, offering for sale, or sale of any product or service, 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 security 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 online 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 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.

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 evaluation and adjustment of Respondents' information security program in light of the results of the testing and monitoring required by subparagraph 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.

III.

IT IS FURTHER ORDERED that Respondents obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biannually thereafter for ten (10) years after service of the order that:

Decision and Order

A. sets forth the specific administrative, technical, and physical safeguards that Respondents have implemented and maintained during the reporting period;

B. explains 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. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph II of this order; and

D. certifies 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, for biannual reports, has so operated throughout the reporting period.

Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or holding Global Information Assurance Certification from the SysAdmin, Audit, Network, Security Institute, or by a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

Respondents shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of Respondents, 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 biannual Assessments shall be retained by the Respondents until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

Decision and Order

IV.

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:

1. a sample copy of each different print, broadcast, cable, or Internet advertisement, promotion, information collection form, Web page, screen, email message, or other document containing any representation regarding Respondents' online collection, use, and security of personal information from or about consumers. Each Web page copy shall be dated and contain the full URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting the information on the Web. *Provided, however*, that after creation of any Web page or screen in compliance with this order, Respondents shall not be required to retain a print or electronic copy of: (1) any amended Web page or screen to the extent that the amendment does not affect Respondents' compliance obligations under this order; or (2) any Web page or screen that contains a hypertext link to Respondents' privacy policy, but otherwise does not relate to Respondents' compliance obligations under this order.

2. any documents, whether prepared by or on behalf of Respondents, 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 biannual Assessment required under Paragraph III of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of Respondents, relating to Respondents' compliance

Decision and Order

with Paragraphs II and III of this order for the compliance period covered by such biannual Assessment.

V.

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 managerial 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.

VI.

IT IS FURTHER ORDERED that Respondents shall notify the Commission at least thirty (30) days prior to any change in either corporation 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 following the dismissal or closing of the current bankruptcy cases; or a change in either corporate name or address. *Provided, however,* that, with respect to any proposed change in either corporation about which either Respondent learns 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 Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Decision and Order

VII.

IT IS FURTHER ORDERED that Respondents shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which they have complied with this order.

VIII.

This order will terminate on May 28, 2024, 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 Paragraph 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 Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that 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 will terminate according to this Paragraph 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.

Analysis

Analysis of Proposed Consent Order to Aid Public Comment

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

Analysis

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

Analysis

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.

Analysis

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

AMERICAN AIR LIQUIDE, INC.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-4109; File No. 0410020
Complaint, April 29, 2004--Decision, June 29, 2004

This consent order addresses the acquisition by Respondent L’Air Liquide, S. A., a world leader in industrial and medical gases and related equipment, of Messer Griesheim GmbH (“MGI”) – which produces and sells industrial gases in the United States – and the subsequent transfer of MGI to L’Air Liquide’s wholly-owned subsidiary, Respondent American Air Liquide, whose own United States subsidiary produces and supplies oxygen, nitrogen, argon, and many other industrial gases to customers for numerous applications in the petrochemical, manufacturing, and fabrication industries and the medical field. The order, among other things, requires Respondent American Air Liquide to divest the air separation units and related assets currently owned and operated by MGI in Vacaville, California; Irwindale, California; San Antonio, Texas; Westlake, Louisiana; DeLisle, Mississippi; and Waxahachie, Texas to an acquirer approved by the Commission. An accompanying Order to Hold Separate requires American Air Liquide to preserve the air separation units as viable, competitive and ongoing operations until the divestiture is achieved.

Participants

For the Commission: *Christina R. Perez, James E. Southworth, Tammy L. Imhoff, Richard A. Levy, Eli Barach, Joseph Eckhaus, Michael R. Moiseyev, Elizabeth A. Piotrowski, Charlotte Wojcik, Jeffrey H. Fischer and Mark W. Frankena.*

For the Respondent: *George Cary and Brian Byrne, Cleary, Gottlieb, Steen & Hamilton.*

COMPLAINT

Pursuant to the Federal Trade Commission Act and the Clayton Act, and by virtue of the authority vested in it by said Acts, the Federal Trade Commission (“Commission”), having reason to believe that the proposed acquisition by L’Air Liquide, Société