

COPY

NO. GV505065

THE STATE OF TEXAS,
Plaintiff,

§
§
§
§
§
§
§

IN THE DISTRICT COURT OF

v.

TRAVIS COUNTY, TEXAS

SONY BMG MUSIC ENTERTAINMENT,
LLC,
Defendant.

126TH JUDICIAL DISTRICT

PLAINTIFF'S FIRST AMENDED PETITION

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff the STATE OF TEXAS, acting by and through the Attorney General of Texas
GREG ABBOTT, complains of Defendant, SONY BMG MUSIC ENTERTAINMENT, LLC ("Sony
BMG"), and for cause of action would respectfully show the Court the following:

FILED

05 DEC 21 AM 10:33

Margaret T. Kelly, Secretary

DISTRICT CLERK
TRAVIS COUNTY, TEXAS

DISCOVERY CONTROL PLAN

1. Discovery is intended to be conducted under Level 2 pursuant to TEX. R. CIV. P. 190.3.

JURISDICTION

2. Greg Abbott, Attorney General of Texas, through his Consumer Protection and Public Health Division, in the name of the State of Texas, brings this action under the authority granted to him by section 48.102 of the Consumer Protection Against Computer Spyware Act ("Spyware Act"), TEX. BUS. & COM. CODE § 48.001 *et seq.* (Vernon Supp. 2005).

3. Greg Abbott, Attorney General of Texas, through his Consumer Protection and Public Health Division, in the name of the State of Texas, further brings this action under the authority granted to him by section 17.47 of the Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), TEX. BUS. & COM. CODE § 17.47 *et seq.* (Vernon 2002 & Supp. 2005).

DEFENDANT

4. Defendant Sony BMG is a limited liability company registered to do business in this State with its principal place of business at 550 Madison Avenue, Floor 15, New York, New York 10022-3211. Defendant Sony BMG may be served with process through its registered agent, Corporation Service Company d/b/a CSC - Lawyers Incorporating Service Company, 701 Brazos, Suite 1050, Austin, Texas 78701.

VENUE

5. Venue for this cause of action lies in Travis County, Texas, for the following reasons:
- A. Under § 15.002 of the TEX. CIV. PRAC. & REM. CODE, venue is proper because a substantial part of the violations are alleged to have occurred in the county of suit;
and
 - B. Under § 17.47(b) of the DTPA, venue is proper because Defendant has done business in the county of suit.

PUBLIC INTEREST

6. Because Plaintiff STATE OF TEXAS has reason to believe that Defendant has engaged in, and will continue to engage in the unlawful practices set forth below, Plaintiff STATE OF TEXAS has reason to believe that Defendant has caused, and will continue to cause damage to residents of the State of Texas and cause adverse effects to legitimate business enterprises that conduct their trade and commerce in a lawful manner in this State. Therefore, the Consumer Protection and Public Health Division of the Office of the Attorney General of Texas believes and is of the opinion that these proceedings are in the public interest.

TRADE AND COMMERCE

7. Defendant is engaged in trade and commerce as that term is defined by DTPA § 17.45(6).

ACTS OF AGENTS

8. Whenever in this Petition it is alleged that Defendant did any act, it is meant that:
- A. Defendant performed or participated in the act; or
 - B. Defendant's officers, agents, or employees performed or participated in the act on behalf of and under the authority of the Defendant.

STATEMENT OF FACTS

9. Defendant Sony BMG markets, distributes, and sells audio compact discs ("CDs") throughout the United States, including in Travis County, Texas. As part of recent CD releases, Sony BMG has included on these CDs, separate from the audio tracks, computer files that are installed on a consumer's personal computer after such CD has been placed in the consumer's computer. Sony represents that these additional components are designed to "protect the audio files embodied on the CD," however these files are used to both play the audio tracks on that computer as well as limit the use of that computer for copying and transferring the audio tracks. Audio CDs distributed by Sony BMG that include these additional computer files are labeled, "Content Protected," on the spine of the CD package; however, Sony BMG makes no disclosures on the packaging that anything will be installed on the consumer's computer. Sony BMG has used at least two types of such "content protection" on CDs distributed in Texas: XCP technology, created by First 4 Internet, Ltd, and MediaMax technology, created by SunnComm International, Inc.
10. Once a consumer places a Sony BMG copy-protected CD in their computer for play, the CD will generally trigger a pop-up multi-page Sony BMG end user license agreement ("EULA"),

following which the consumer must click “agree” or “disagree.” The EULA is displayed in a small box, requiring the consumer to scroll through multiple lines of text to fully review the terms and conditions, and fails to provide a mechanism for the consumer to print those terms. The consumer must click “agree” in order to continue to access the audio files on the CD. After clicking “agree,” Sony BMG’s own media player will load, allowing the consumer to listen to the CD. If the consumer clicks “disagree,” the CD will eject from the computer.

XCP Technology

11. Sony BMG CDs that include XCP technology can be identified by a reference on the back cover of the CD to the website “cp.sonybmg.com/xcp.” As described above, consumers playing a Sony BMG CD with XCP are generally prompted with a EULA requiring their acceptance to continue. After accepting the EULA, Sony BMG installs its media player, during which Sony BMG also creates and installs components of its XCP technology in a folder it names “C:/Windows/System32/\$sys\$filesystem.” Unbeknownst to the consumer, Sony BMG also installs a file named “Aries.sys” in the same folder which conceals the XCP files and the folder in which they are installed, such that the owner of the computer performing a search of the file system would not be able to locate and remove the XCP technology. Essentially, the Aries.sys file masks any folder or file name on a consumer’s computer that begins with the characters “\$sys\$,” which are the first characters of the folders, files, and registry entries associated with the XCP technology. Moreover, these hidden files and folder are installed within the consumer’s Microsoft Windows “System32” subfolder, such that a consumer may confuse that software with essential files needed to run the computer’s operating system.

12. The Aries.sys file is not required to play Sony BMG’s XCP copy protected CDs; rather its

purpose is to conceal the XCP technology installed by Sony BMG. In fact, renaming or deleting the Aries.sys file will uncloak the XCP files, and the consumer will be able to continue to use their CD in the same manner as if the Aries.sys file remained. Sony BMG does not disclose the fact that its technology includes this cloaking component to consumers on either the CD itself or in its EULA.

13. Moreover, the audio tracks on Sony BMG's XCP CDs do not require Sony BMG's proprietary media player to play on a computer. On some occasions, consumers inserting a Sony BMG XCP CD into their computer are not prompted with Sony BMG's EULA, rather they are prompted by a window by the operating system asking the consumer if he/she wants to play the CD. Using another media player (for example, Windows Media Player), the consumer is then able to play the audio CD. However, if the consumer inserts the CD and the Sony BMG EULA is displayed, the consumer will no longer be able to use these other media players to play the audio CD.

14. Sony BMG discusses its XCP technology on the website <http://cp.sonybmg.com>. As part of its frequently asked questions, Sony BMG included the following:

"I have heard that the protection software is really malware/spyware. Could this be true?

Of course not. The protection software simply acts to prevent unlimited copying and ripping from discs featuring this protection solution. It is otherwise inactive. The software does not collect any personal information nor is it designed to be intrusive to your computer system. Also, the protection components are never installed without the consumer first accepting the End User License Agreement.

If at some point you wish to remove the software from your machine simply contact customer service [through this link](#). You will, though, be unable to use the disc on your computer once you uninstall the components.

Our technology vendors are constantly looking to improve the product as well as respond to any critical software issues found. Please check [here](#) for upgrades to address any known issues."

15. In reality, Sony BMG's XCP technology remains hidden and active on a consumer's

computer at all times after installation, even when Sony BMG's media player is not active. During the installation process, Sony BMG installs another hidden file named, "\$sys\$drmsrver.exe" which is cloaked and constantly consumes system memory, resulting in a reduction in a consumer's available system resources. In addition, a consumer attempting to remove the XCP technology finds that Sony BMG has made it extremely burdensome if not impossible to do so - Sony BMG does not make an uninstall utility readily available. Until recently, Sony BMG only provided on their website a patch that will "uncloak" the hidden files (in part by deleting the Aries.sys file); it did not, however, provide a way to remove the XCP software in its entirety.

16. In light of the recent public awareness regarding Sony BMG's XCP technology, Sony BMG issued the following statement regarding the service pack that uncloaked the installed components:

"This Service Pack removes the cloaking technology component that has been recently discussed in a number of articles published regarding the XCP Technology used on SONY BMG content protected CDs. This component is not malicious and does not compromise security. However to alleviate any concerns that users may have about the program posing potential security vulnerabilities, this update has been released to enable users to remove this component from their computers."

Despite Sony BMG's assertions, various news sources have recently reported the spread of newly created viruses which exploit Sony BMG's cloaking technology. As a result, a consumer without knowledge of the installation of the Aries.sys file on their computer may be vulnerable to new security risks, and given the cloaked nature of these files, and the extremely burdensome impediments to removing them, that consumer may find it difficult or impossible to protect themselves from future risks.

MediaMax

17. Sony BMG CDs that include MediaMax technology can be identified by a reference on the

back cover of the CD to the website “www.sunncomm.com/support/sonybmj.” As described above, a consumer placing a Sony BMG MediaMax CD in his or her computer will generally be prompted with a EULA requiring his or her acceptance to continue. In some versions of the MediaMax files, Sony BMG also secretly installs files on the consumer’s computer while the EULA is loading, such that before the consumer can choose to accept the EULA, Sony BMG has already placed over ten megabytes of files on his or her computer. If the consumer does not accept the EULA, the CD ejects from the consumer’s computer; however, the files that Sony BMG installed remain on the consumer’s computer. Sony BMG does not disclose to the consumer that these files have been installed on either the CD packaging or in the EULA, nor does it create any icons or program listing for those files noticeable to a consumer. Moreover, Sony BMG fails to include any uninstall mechanism for removal of these files, making it difficult for a consumer to remove these files which consume space on a consumer’s hard drive.

18. In fact, the Sony BMG EULA further misleads consumers by representing that no files are installed if the EULA is rejected, by stating, “[a]s soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program....” In reality, this installation has already occurred, and these files will not be removed despite a consumer’s refusal to be bound by the terms and conditions of the EULA.

19. Moreover, these files installed by Sony BMG cause further security risks to consumers’ computers. Sony BMG has acknowledged the security problems with the MediaMax files in recent statements, by stating:

“The security issue involves a file folder installed on users’ computers by the MediaMax software that could allow malicious third parties who have localized, lower-privilege access to gain control over a consumer’s computer running the Windows operating system.”

This risk would similarly allow consumers' computers to become more susceptible to malicious software installation. And by creating this risk even when a consumer rejects the EULA, any individual even inserting a MediaMax CD, whether they want to agree to the terms of the EULA or not, has now made their computer susceptible to these attacks.

CONSUMER PROTECTION AGAINST COMPUTER SPYWARE ACT VIOLATIONS

20. Paragraphs 1 through 19 are incorporated herein by reference.

21. Defendant, as alleged above, has knowingly caused computer software to be copied to a computer in this state, of which it is not the owner or operator, and used that software to:

- A. Prevent the owner's or operator's reasonable efforts to block the installation of or to disable computer software by:
 - 1) presenting the owner or operator with an option to decline the installation of software knowing that, when the option is selected, the installation process will continue to proceed; or
 - 2) misrepresenting that software has been disabled, in violation of Spyware Act § 48.053(4);
- B. Change the name, location, or other designation of computer software to prevent the owner from locating and removing the software, in violation of Spyware Act § 48.053(5); and
- C. Create randomized or intentionally deceptive file names or random or intentionally deceptive directory folders, formats, or registry entries to avoid detection and prevent the owner from removing computer software, in violation of Spyware Act § 48.053(6).

22. Defendant, as alleged above, has further induced the owner or operator of a computer in this state, of which Defendant is not the owner or operator, to install a computer software component to the computer by intentionally misrepresenting the extent to which the installation is necessary for security or privacy reasons, to open or view text, or to play a particular type of musical or other content, in violation of Spyware Act § 48.055(1).

DECEPTIVE TRADE PRACTICES ACT VIOLATIONS

23. Paragraphs 1 through 19 are incorporated herein by reference.

24. Defendant, as alleged above and detailed below, has in the course of trade and commerce engaged in false, misleading, or deceptive acts and practices declared unlawful in DTPA §§ 17.46(a) and (b). Such acts include but are not limited to:

- A. Engaging in false, misleading or deceptive acts or practices in the conduct of trade or commerce, in violation of DTPA § 17.46(a);
- B. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities which they do not have, in violation of DTPA § 17.46(b)(5);
- C. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another, in violation of DTPA § 17.46(b)(7);
- D. Representing that an agreement confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law in violation of DTPA § 17.46(b)(12); and
- E. Failing to disclose information concerning goods or services which was known at the

time of the transaction in order to induce a consumer into a transaction into which the consumer would not have otherwise entered, in violation of DTPA § 17.46(b)(24).

PRAYER

25. Because Defendant has engaged in the unlawful acts and practices described above, Defendant has violated and will continue to violate the law as alleged in this Petition. Unless enjoined by this Honorable Court, Defendant will continue to violate the laws of the STATE OF TEXAS and cause injury, loss, and damage to the STATE OF TEXAS and to the general public.

26. WHEREFORE, Plaintiff prays that Defendant be cited according to law to appear and answer herein; and upon notice and hearing TEMPORARY and PERMANENT INJUNCTIONS be issued, restraining and enjoining Defendant, Defendant's agents, servants, employees and attorneys and any other person in active concert or participation with any Defendant from engaging in practices declared unlawful by the Spyware Act and DTPA, including but not limited to:

A. Offering for sale or selling any good which includes or installs any software which violates the Spyware Act, including but not limited to:

1) Preventing a computer owner's or operator's reasonable efforts to block the installation of or to disable computer software by:

A) presenting the owner or operator with an option to decline the installation of software knowing that, when the option is selected, the installation process will continue or has already occurred; or

B) misrepresenting that software has been disabled;

2) Changing the name, location, or other designation of computer software to prevent the owner from locating and removing the software, including, but

not limited to, hiding or cloaking any files such that a consumer cannot readily locate them; or

- 3) Creating randomized or intentionally deceptive file names or random or intentionally deceptive directory folders, formats, or registry entries to avoid detection and prevent the owner from removing computer software, including, but not limited to, hiding or cloaking files or directories such that a consumer cannot readily locate them.

B. Misrepresenting the extent to which a computer software component must be installed on a computer in order to play a particular type of musical or other content.

C. Failing to clearly and conspicuously disclose, on the packaging of any CD sold in Texas:

- 1) The fact, if true, that computer files must be installed on a consumer's computer in order for the consumer to listen to the music via that computer, and the approximate size, and purpose, of those files;
- 2) The fact, if true, that using the CD in a computer will cause certain files to be loaded into the computer's memory, such that they will consume system resources even when the music CD is not in the computer;
- 3) The fact, if true, that the CD includes any form of digital rights management protection that will limit the copying or transfer of the audio music files on the CD; and
- 4) The fact, if true, that a consumer will be required to accept the terms and conditions of a license agreement prior to being able to listen to or otherwise

access the CD on a computer.

- D. Misrepresenting the function or use of any files that are copied or installed onto a person's computer by Defendant's CDs, including, but not limited to, representing that any computer files are necessary for copy protection or digital rights management purposes if they are not.
- E. Failing to clearly and conspicuously disclose, prior to copying or installing any files onto a person's computer, any risk or potential for harm to that person's computer related to the copying or installation of any computer files by Defendant's CDs, including vulnerability to viruses or malware, data and file integrity, or any other damage that may be caused to a person's computer.
- F. Failing to take immediate remedial action upon discovering that any computer file included on any of Defendant's CDs causes any risk or potential for harm to a person's computer, including vulnerability to viruses or malware, data and file integrity, or any other damage that may be caused to a person's computer.
- G. Failing to clearly and conspicuously disclose, prior to copying or installing any files onto a person's computer, all terms and conditions of any license agreement Defendant requires that person to accept in order to fully listen to and access a CD on a computer.
- H. Failing to clearly and conspicuously disclose, prior to copying or installing computer files on a person's computer, the type and purpose of, and amount of system resources used by, all such files.
- I. Failing to include an uninstall utility on or with any CD that will copy or install files

on a person's computer, such that the person is able to completely remove all files installed by Defendant from his or her computer.

- J. Failing to adopt and implement policies and procedures to analyze, review, and update any computer files included on Defendant's CDs to insure compliance with State and Federal law.

27. In addition, Plaintiff STATE OF TEXAS respectfully prays that this Court:

- A. Adjudge against Defendant civil penalties in favor of Plaintiff STATE OF TEXAS in the amount of One Hundred Thousand Dollars (\$100,000.00) for each violation of the Spyware Act, pursuant to Spyware Act § 48.102(a);
- B. Adjudge against Defendant civil penalties in favor of Plaintiff STATE OF TEXAS in the amount of Twenty Thousand Dollars (\$20,000.00) for each violation of the DTPA, pursuant to DTPA § 17.47(c);
- C. Make such additional orders and judgments against Defendant as are necessary to compensate identifiable persons for actual damages or to restore money or property, real or personal, which may have been acquired by means of any unlawful act or practice, pursuant to DTPA § 17.47(d);
- D. Order Defendant to pay Plaintiff STATE OF TEXAS attorneys' fees and costs of court pursuant to Spyware Act § 48.102(c);
- E. Order Defendant to pay all costs of Court, costs of investigation, and reasonable attorney's fees pursuant to TEX. GOVT. CODE ANN. § 402.006(c); and
- F. Grant all other relief to which the Plaintiff STATE OF TEXAS may show itself entitled.

Respectfully submitted,

GREG ABBOTT
Attorney General of Texas

BARRY R. McBEE
First Assistant Attorney General

EDWARD D. BURBACH
Deputy Attorney General for Litigation

PAUL D. CARMONA
Chief, Consumer Protection & Public Health Division

A handwritten signature in black ink, appearing to read "Paul Singer", written over a horizontal line.

PAUL SINGER
State Bar No. 24033197
C. BRAD SCHUELKE
State Bar No. 24008000
JOHN SABA, JR.
State Bar No. 24037415
Assistant Attorneys General
Office of the Attorney General
Consumer Protection & Public Health Division
P.O. Box 12548
Austin, Texas 78711-2548
(512) 463-2185 (telephone)
(512) 473-8301 (facsimile)