UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeny

In the Matter of	)	**DOCKET NO. C-4481**
Fandango, LLC,	)	
a limited liability company.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that Fandango, LLC ("respondent") has 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 Fandango, LLC ("Fandango") is a Delaware limited liability company with its principal office or place of business at 12200 W. Olympic Boulevard, Suite 400, Los Angeles, CA 90064.

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

RESPONDENT'S BUSINESS PRACTICES

3. Fandango provides a website and mobile applications that allow consumers to purchase movie tickets and view showtimes, trailers, and reviews.

4. Fandango launched its Fandango Movies application for Apple, Inc.'s iOS operating system in March 2009. In December 2010, Fandango launched an iPad version of the application. Fandango distributes the application through the iTunes App Store, where it describes the application as the "#1 movie ticketing app featured in Apple commercials." The iTunes App Store lists Fandango Movies among the top 10 free applications in the Entertainment category. The application has been downloaded over 18.5 million times.

5. Although the Fandango Movies application is free to install and use, Fandango charges a service fee when a consumer uses the application to purchase a movie ticket. As of August 2013, 20 percent of Fandango's total ticket sales were from its iOS mobile applications.

6. Fandango Movies allows consumers to purchase movie tickets regardless of whether the consumer has a Fandango account. When a consumer purchases tickets, the application provides a choice of payment methods, including an option to pay by credit card. Consumers can choose to save their credit card information on the device for future use. Each time a user purchases tickets after entering a credit card number or selecting a card previously saved on the device, Fandango Movies transmits the consumer's credit card information, including card number, security code, expiration date, and billing zip code, to Fandango's servers. If a consumer chooses to create or log into a Fandango account through the Fandango Movies application, the application transmits the consumer's authentication credentials, including email address and password, to Fandango's servers.

SECURE SOCKETS LAYER CERTIFICATE VALIDATION

7. Consumers frequently use mobile applications on public Wi-Fi networks in venues such as coffee shops, shopping centers, and airports. Consumers may use the Fandango Movies application in such public environments. Indeed, during its launch, Fandango marketed the Fandango Movies application as a way for consumers "to access movie and theater information 'on the go', [and] buy tickets in seconds for more than 16,000 screens across the U.S."

8. Online services often use the Secure Sockets Layer ("SSL") protocol to establish authentic, encrypted connections with consumers. In order to authenticate and encrypt connections, SSL relies on electronic documents called SSL certificates.

9. In the context of mobile applications, an online service (*e.g.*, Fandango) presents an SSL certificate to the application on a consumer's device (*e.g.*, Fandango Movies) to vouch for its identity. The application must then validate the SSL certificate – in effect verifying the identity of the online service – to ensure that the application is connecting to the genuine online service. After completing this process, the online service and the application on the consumer's device can establish a secure connection that is both authenticated and encrypted.

10. If the application fails to perform this process, an attacker could position himself between the application on the consumer's device and the online service by presenting an invalid certificate to the application. The application would accept the invalid certificate and establish a connection between the application and the attacker, allowing the attacker to decrypt, monitor, or alter all communications between the application and the online service. This type of attack is known as a "man-in-the-middle attack." Neither the consumer using the application nor the online service could feasibly detect the attacker's presence.

11. On many public Wi-Fi networks, attackers can use well-known spoofing techniques to facilitate man-in-the-middle attacks.

12. To protect against these attacks, the iOS operating system provides developers with application programming interfaces ("APIs") that allow applications to create secure connections using SSL. By default, these APIs validate SSL certificates and reject the connection if the SSL certificate presented to the application is invalid.

13. The iOS developer documentation warns developers against disabling the default validation settings or otherwise failing to validate SSL certificates, explaining that this "eliminates any benefit you might otherwise have gotten from using a secure connection. The resulting connection is no safer than sending the request via unencrypted HTTP because it provides no protection from spoofing by a fake server."

14. Application developers can easily test for and identify SSL certificate validation vulnerabilities using free or low-cost, publicly available tools.

FANDANGO'S SECURITY FAILURES

15. From March 2009 to March 2013, the Fandango Movies application for iOS failed to validate SSL certificates, overriding the defaults provided by the iOS APIs.

16. Before March 2013, Fandango did not test the Fandango Movies application to ensure that the application was validating SSL certificates and securely transmitting consumers' sensitive personal information. Although Fandango commissioned limited security audits of its applications starting in 2011, more than two years after the release of its iOS application, respondent limited the scope of these security audits to issues presented when the "code is decompiled or disassembled," *i.e.*, threats arising only from attackers who had physical access to a device. As a result, these audits did not assess whether the iOS application's transmission of information, including credit card information, was secure.

17. Moreover, Fandango does not have a clearly publicized and effective channel for receiving security vulnerability reports, and instead relies upon its general Customer Service system to escalate security vulnerability reports to the proper employees. In December 2012, a security researcher informed respondent through its Customer Service web form that its iOS application was vulnerable to man-in-the-middle attacks because it did not validate SSL certificates. Because the security researcher's message included the term "password," Fandango's Customer Service system flagged the message as a password reset request and replied with an automated message providing the researcher with instructions on how to reset passwords. Fandango's Customer Service system then marked the security researcher's message as "resolved," and did not escalate it for further review.

18. After Commission staff contacted respondent, Fandango tested the Fandango Movies application for iOS and confirmed that the application failed to validate SSL certificates. Fandango discovered that the vulnerability also affected a separate iOS movie ticketing application that Fandango developed and hosted for a third party. Within three weeks of being contacted by Commission staff, respondent issued an update to both iOS

applications that enabled SSL certificate validation by restoring the iOS API default settings, thereby correcting the security vulnerability.

19. Respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security in the development and maintenance of its mobile application, including:

    a. Overriding the default SSL certificate validation settings provided by the iOS APIs without implementing other security measures to compensate for the lack of SSL certificate validation;

    b. Failing to appropriately test, audit, assess, or review its applications, including failing to ensure that the transmission of sensitive personal information was secure; and

    c. Failing to maintain an adequate process for receiving and addressing security vulnerability reports from third parties.

20. As a result of these failures, attackers could have, in connection with attacks that redirect and intercept network traffic, decrypted, monitored, or altered any of the information transmitted from or to the application, including the consumer's credit card number, security code, expiration date, billing zip code, email address, and password. The misuse of credit card information and authentication credentials can lead to identity theft and financial harm, the compromise of personal information maintained on other online services, and related consumer harms.

21. Fandango could have prevented these vulnerabilities and ensured the secure transmission of consumers' sensitive personal information, including credit card information, at virtually no cost by simply implementing the default SSL certificate validation settings.

FANDANGO'S PRIVACY AND SECURITY REPRESENTATIONS

22. Fandango disseminated or caused to be disseminated to consumers the following in-app representation regarding the security of credit card and account information stored on and transmitted through the application:

> Your Fandango iPhone Application allows you to store your credit card and Fandango account information on your device so you can conveniently purchase movie tickets. Your information is securely stored on your device and transferred with your approval during each transaction.

23. When a consumer selects the option to "Buy" a ticket using the Fandango Movies application, respondent disseminated or caused to be disseminated the following in-app representation regarding the security of the transaction before presenting the consumer with the option to pay by entering – and if desired, storing on the device for future use – the consumer's credit card information:

You don’t need an account to securely purchase tickets.

FANDANGO’S DECEPTIVE REPRESENTATIONS

24. As described in Paragraphs 22 and 23, Fandango represented, expressly or by implication, that it provides reasonable and appropriate security for ticket purchases made through the Fandango Movies application for iOS.

25. In truth and in fact, as set forth in Paragraphs 7 – 21, in many instances, Fandango did not provide reasonable and appropriate security for ticket purchases made through the Fandango Movies application for iOS. Therefore, the representation set forth in Paragraph 24 was false or misleading.

26. The acts and practices of respondent 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, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this thirteenth day of August, 2014, has issued this complaint against respondent.

By the Commission, Commissioner McSweeny not participating.

Donald S. Clark
Secretary