David W. Lincicum (California Bar No. 223566)
Burke W. Kappler (D.C. Bar No. 471936)
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Mail Stop NJ-8122
Washington, D.C. 20580
dlincicum@ftc.gov
bkappler@ftc.gov
202-326-2773 (Lincicum)
202-326-2043 (Kappler)
202-326-3062 (facsimile)

Attorneys for Plaintiff Federal Trade Commission

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, **Plaintiff,** **v.** **LifeLock, Inc.** **a corporation; Robert J. Maynard, Jr.,** **individually and as an officer of LifeLock,** **Inc.; and** **Richard Todd Davis,** **individually and as an officer of** **LifeLock, Inc.,** **Defendants.**	**Civil No.** **COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF**

Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten

monies, and other relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this matter under 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

3. Venue is proper in this District under 28 U.S.C. §§ 1391(b) and (c) and 15 U.S.C. § 53(b).

PLAINTIFF

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The Commission enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits deceptive or unfair acts or practices in or affecting commerce.

5. The FTC is authorized to initiate federal district court proceedings by its own attorneys, to enjoin violations of the FTC Act and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b) and 56(a)(2)(A).

DEFENDANTS

6. Defendant LifeLock, Inc. ("LifeLock"), is a Delaware corporation with its principal office or place of business at 60 East Rio Salado Parkway, Tempe, Arizona 85281. LifeLock transacts or has transacted business in this District and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, LifeLock has advertised, marketed, distributed, or sold an identity theft service to consumers in this District and throughout the United States.

7. Defendant Robert J. Maynard, Jr. ("Maynard") was LifeLock's Chief Operating

Officer until on or about May 18, 2007. He then served as LifeLock's Chief Marketing Strategist until his resignation on or about June 11, 2007. Until his resignation, acting alone or in concert with others, he formulated, directed, controlled, had the authority to control, or participated in the acts of practices of LifeLock, including the acts and practices set forth in this Complaint. Defendant Maynard, in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

8. Defendant Richard Todd Davis ("Davis") is the Chief Executive Officer of LifeLock. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of LifeLock, including the acts and practices set forth in this Complaint. Defendant Davis resides in this District and in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

COMMERCE

9. At all times relevant to this Complaint, Defendants have maintained a substantial trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS' BUSINESS ACTIVITIES

10. Since at least April 2005 until at least October 2009, Defendants have advertised, promoted, offered for sale, sold, or otherwise made available to consumers a service purportedly designed to prevent identity theft through placing fraud alerts on consumers' behalf (hereinafter, "the ID theft prevention service").

11. Defendants' ID theft prevention service was based on Defendants taking the following measures:

a. Placing an "Initial Alert" (as defined in Section 605A(a) of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681c-1(a)) on a customer's consumer report with a consumer reporting agency (often referred to as a "credit bureau"), and periodically renewing the alert for an additional 90 days;

b. Obtaining and providing to the customer a copy of his or her free annual disclosure of his or her consumer report, pursuant to Section 612(a) of the FCRA, 15 U.S.C. § 1681j(a);

c. Submitting a request on a customer's behalf to remove the customer's name from lists for prescreened offers of credit, pursuant to Sections 604(c) and 604(e) of the FCRA, 15 U.S.C. §§ 1681b(c) and (e); and

d. Offering a $1 million guarantee to customers who become victims of identity theft while subscribing to the ID theft prevention service.

12. Defendants advertised, promoted, and marketed the ID theft prevention service in a variety of ways, including by print, radio, and television advertisements, and through their www.lifelock.com website.

13. Under Federal law, identity theft includes many types of criminal activities, including the misuse of another person's identifying information to access existing credit accounts, open new accounts, obtain medical care or employment, or to evade law enforcement. 18 U.S.C. § 1028(a)(7).

14. Defendants charged customers a fee of ten dollars ($10) per month for the ID theft prevention service, and enrolled over one million customers.

15. In the course of selling the ID theft prevention service, Defendants routinely collected sensitive information from their customers including, but not limited to: name,

address, e-mail address, telephone number, Social Security number, and, for customers paying with a credit card, the card number, expiration date, and security code number (collectively, "personal information"). Defendants collected this information by telephone, facsimile, and online. It is widely recognized that such personal information may be misused to facilitate identity theft, including, but not limited to, the misuse of existing credit card accounts.

16. Defendants store personal information obtained from customers on computers on the corporate computer network, or on computers maintained by third-party vendors that are accessible from the corporate network. Defendants' employees can access the corporate network using computers located at Defendants' headquarters. Additionally, for at least some portion of time relevant to this Complaint, employees and vendors working from their homes or other locations beyond the Defendants' headquarters could access the network remotely.

Statements about the Effectiveness of Defendants' Service to Prevent Identity Theft

17. From at least December 2006, Defendants, directly or indirectly, have disseminated or caused to be disseminated to consumers advertisements and other promotional materials in connection with the advertising, promotion, marketing, offering for sale, sale, or distribution of their ID theft prevention service. These materials have included, but are not limited to, the following statements, among others:

a. "MY SOCIAL SECURITY # IS XXX-XX-5462. I'm Todd Davis, CEO of LifeLock, and this really is my social security number.* I give it just to prove how safe your identity can be with LifeLock." (Exhibit 1)

b. "Do you ever worry about identity theft? If so, it's time you got to know LifeLock. We work to stop identity theft before it happens. We're so confident,

we back our clients with a $1 million guarantee." (Exhibit 1)

c. "We aim to stop identity theft before it happens. . . . Every three seconds an identity is stolen. We're here to make sure it doesn't happen to you." (Television Ad)

d. "My social security number is XXX-XX-5462. I'm Todd Davis, CEO of LifeLock, and yes, that's my real social security number.* Identity theft is one of the fastest growing crimes in America, victimizing over 10 million people a year and costing billions of dollars. So why publish my social security number? Because I'm absolutely confident LifeLock is protecting my good name and personal information, just like it will yours." (Exhibit 2)

e. "By now you've heard about individuals whose identities have been stolen by identity thieves . . . . LifeLock protects against this ever happening to you. Guaranteed." (Exhibit 3)

f. "LifeLock doesn't just report unauthorized use of credit information, we prevent it by working with the top four credit bureaus to make sure you're contacted to approve any credit transaction before it takes place." (Exhibit 3)

g. "LifeLock clients are contacted every time someone attempts to open credit in their name or change an address." (Exhibit 4)

h. "Please know that we are the first company to prevent identity theft from occurring." (Exhibit 5)

i. "LifeLock will make your personal information useless to a criminal." (Exhibit 6)

j. "Lifelock can keep this [identity theft] from happening to you . . . ." (Exhibit 6)

k. "Every time you apply for new credit or someone tries to do something with your credit: You should receive a phone call from the bank asking if you are actually the person applying for credit in your name." (Exhibit 7)

l. "We work with all major credit bureaus on an ongoing basis, setting up fraud alerts and constantly monitoring what's happening with each person's credit." (Exhibit 8)

m. "Lifelock, the industry leader in proactive identity theft protection, offers a proven solution that prevents your identity from being stolen before it happens." (Exhibit 9) (emphasis in original)

n. "So why is LifeLock CEO Todd Davis still giving out his real Social Security number to anyone who will listen? 'Because between LifeLock's proactive approach and our $1 million service guarantee, I'm more confident than ever before in LifeLock's ability to continue keeping my identity safe.'" (Exhibit 10)

o. "I give [my Social Security number] out just to prove how safe your identity is with LifeLock." (Exhibit 11)

18. In fact, the ID theft prevention service did not prevent identity theft and did not provide many of the protections claimed by Defendants. Among other things:

a. The ID theft prevention service did not protect against all types of identity theft. The centerpiece of the ID theft prevention service was Defendants' placement and renewal of Initial Fraud Alerts on their customers' consumer reports. Although Initial Alerts can provide notice to creditors and other businesses that someone may be impersonating another, the Initial Alerts only are useful if the business accesses the consumer's consumer report as part of the transaction, most

commonly when the identity thief is attempting to open a new account in the consumer's name. The Alerts do not protect against more common types of identity theft, such as misuse of an existing credit account, that typically do not involve obtaining consumer reports. Nor do the alerts protect against other types of identity theft, such as medical identity theft, employment-related identity theft, or using another's identity to evade law enforcement.

b. In some cases, the ID theft prevention service could fail to prevent identity theft even as to transactions in which consumer reports were obtained. Some businesses ignore fraud alerts or fail to take sufficient precautions to confirm the identity of the applicant. In some instances, identity thieves can thwart even reasonable precautions.

c. The ID theft prevention service does not prevent unauthorized changes to customers' address information because the Initial Alerts Defendants place for customers do not require users of the customers' consumer reports to contact customers with fraud alerts before changing address information.

d. The ID theft prevention service did not ensure that a consumer will receive a telephone call from a potential creditor before a new account was opened in the consumer's name. Section 605A of the FCRA permits but does not require businesses to call consumers before opening the account, and also allows businesses to use other "reasonable steps to verify the consumer's identity."

e. The ID theft prevention service did not provide ongoing monitoring or review of customers' credit files.

Statements about the Security of Customers' Information

19. Since at least December 2006, Defendants, directly or indirectly, have disseminated or caused to be disseminated to consumers privacy policies and statements, including, but not necessarily limited to, the following statements regarding the privacy, confidentiality, and security of personal information they receive from their customers:

a. "Only authorized employees of LifeLock will have access to the data that you provide to us, and that access is granted only on a 'need to know' basis."

b. "All stored personal data is electronically encrypted."

c. "Any data that we transmit over a private network will be sent via secure, encrypted channels."

d. "When you enter sensitive information (such as credit card number and/or social security number) on our registration or order forms, we encrypt that information using secure socket layer technology (SSL)."

e. "Your documents, while in our care, will be treated as if they were cash."

f. "Lifelock uses highly secure physical, electronic, and managerial procedures to safeguard the confidentiality and security of the data you provide to us."

(Exhibit 12).

20. In fact, until at least September 2007, Defendants engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to personal information stored on its corporate network, in transit through its corporate network or over the internet, or maintained in Defendants' offices. Among other things, Defendants:

a. Created an unnecessary risk to personal information by storing it on the network and transmitting it over the network and the internet in clear readable text;

b. Failed to require employees, vendors, and others with access to personal information to use hard-to-guess passwords or to implement related security measures, such as periodically changing passwords or suspending users after a certain number of unsuccessful log-in attempts;

c. Failed to limit access to personal information stored on or in transit through its networks only to employees and vendors needing access to the information to perform their jobs;

d. Failed to use readily available security measures to routinely prevent unauthorized access to personal information, such as by installing patches and critical updates on its network;

e. Did not adequately assess the vulnerability of the network and web applications to commonly known and reasonably foreseeable attacks, such as SQL injection attacks;

f. Failed to employ sufficient measures to detect and prevent unauthorized access to the corporate network or to conduct security investigations, such as by installing antivirus or anti-spyware programs on computers used by employees to remotely access the network or regularly recording and reviewing activity on the network;

g. Did not implement simple, low-cost, and readily available defenses to commonly known and reasonably foreseeable attacks; and

h. Failed, from at least December 2006 until February 2007, to secure paper documents containing personal information that were received by facsimile in an open and easily accessible area.

As a result of these practices, an unauthorized person could obtain access to personal

information stored on Defendants' corporate network, in transit through Defendants' corporate network or over the internet, or maintained in Defendants' offices.

VIOLATIONS OF SECTION 5(a) OF THE FTC ACT

21. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

22. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

Count I

23. Through the means described in Paragraph 17, Defendants have represented, directly or indirectly, expressly or by implication, that the ID theft prevention service provided complete protection against all forms of identity theft by making customers' personal information useless to identity thieves.

24. In truth and in fact, as described in Paragraph 18, the ID theft prevention service did not provide complete protection against all identity theft and did not make customers' personal information useless to identity thieves.

25. Therefore, the making of the representation set forth in Paragraph 23 of this Complaint constitutes a deceptive act or practice, in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count II

26. Through the means described in Paragraph 17, Defendants have represented, directly or indirectly, expressly or by implication, that the ID theft prevention service prevented unauthorized changes to customers' address information.

27. In truth and in fact, as described in Paragraph 18, at the time this representation

was made, the ID theft prevention service did not prevent unauthorized changes to customers' address information because the Initial Alerts Defendants place for customers do not require users of the customers' consumer reports to contact customers with fraud alerts before changing address information.

28. Therefore, the making of the representation set forth in Paragraph 26 of this Complaint constitutes a deceptive act or practice, in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count III

29. Through the means described in Paragraph 17, Defendants have represented, directly or indirectly, expressly or by implication, that the ID theft prevention service constantly monitored activity on each of its customers' consumer reports.

30. In truth and in fact, as described in Paragraph 18, the ID theft prevention service did not monitor activity on customers' consumer reports.

31. Therefore, the making of the representation set forth in Paragraph 29 of this Complaint constitutes a deceptive act or practice, in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count IV

32. Through the means described in Paragraph 17, Defendants have represented, directly or indirectly, expressly or by implication, that the ID theft prevention service would ensure that a customer would always receive a phone call from a potential creditor before a new credit account was opened in the customer's name.

33. In truth and in fact, as described in Paragraph 18, the ID theft prevention service did not ensure that a customer would receive a phone call from a potential creditor before a new

credit account was opened in their name because the Initial Alerts that Defendants placed for customers do not require that the potential creditor contact consumers before opening new credit accounts.

34. Therefore, the making of the representation set forth in Paragraph 32 of this Complaint constitutes a deceptive act or practice, in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count V

35. Through the means described in Paragraph 19, Defendants have represented, directly or indirectly, expressly or by implication, that they employed reasonable and appropriate measures to protect personal information of customers from unauthorized access.

36. In truth and in fact, as described in Paragraph 20, Defendants did not employ reasonable and appropriate measures to protect personal information of customers from unauthorized access.

37. Therefore, the making of the representation set forth in Paragraph 35 of this Complaint constitutes a deceptive act or practice, in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count VI

38. Through the means described in Paragraph 19, Defendants have represented, directly or indirectly, expressly or by implication, that they encrypted sensitive customer information that they stored or transmitted in the course of their business.

39. In truth and in fact, as described in Paragraph 20, Defendants did not encrypt sensitive customer information that they stored or transmitted in the course of their business.

40. Therefore, the making of the representation set forth in Paragraph 38 of this

Complaint constitutes a deceptive act or practice, in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count VII

41. Through the means described in Paragraph 19, Defendants have represented, directly or indirectly, expressly or by implication, that they limited access to sensitive customer information only to authorized employees on a "need-to-know" basis.

42. In truth and in fact, as described in Paragraph 20, Defendants did not limit access to sensitive customer information only to authorized employees on a "need-to-know" basis.

43. Therefore, the making of the representation set forth in Paragraph 41 of this Complaint constitutes a deceptive act or practice, in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

44. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

45. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

PRAYER FOR RELIEF

Wherefore, Plaintiff Federal Trade Commission, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Court's own equitable powers, requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act by Defendants;

B. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including, but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

C. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

Willard K. Tom
General Counsel

s/ Burke Kappler

Dated: March 8, 2010

DAVID W. LINCICUM
BURKE W. KAPPLER
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Mail Stop NJ-3158
Washington, D.C. 20580
202-326-2773 (Lincicum)
202-326-2043 (Kappler)
202-326-3062 (facsimile)
dlincicum@ftc.gov (e-mail)
bkappler@ftc.gov (e-mail)

Attorneys for Plaintiff

FEDERAL TRADE COMMISSION