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 UNITE D STATES DISTRICT COURT
FOR THE DISTRICT OF AR IZONA

Federal Trade Commission,)
)

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:

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 0.00000 1.00000 0.0000 0.(d th)Tj18.3600 0.0000 TD(a)Tj5.2800 0.0000 TD(t su

hd for c

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’ c

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, Defenda

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 vulnerabile1.0000h60d(y0000iTbDle(sya)Tj12.3600Tj5.2800 0

d.withoraisedtFai1000000000000Tj1.2800 network(s)Tj150.0000 TD(availaTiconductablepe)Tj100 0.0000 TD(eesc006.0000 20

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

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. Throug

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 r a r a r a