UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Plaintiff,

v.

RUBY CORP.
20 Eglinton Avenue West
Toronto, Ontario M4R 1K8,

RUBY LIFE INC., also doing business as
ASHLEYMADISON.COM
20 Eglinton Avenue West
Toronto, Ontario M4R 1K8,

ADL MEDIA INC.
1209 Orange Street
Wilmington, Delaware 19801

Defendants.

Civil Action 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 Section13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain permanent injunctive relief, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), in connection with Defendants' marketing and sale of online dating services.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. § 45(a).

3. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), (b)(3), (c)(2), and (c)(3), 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 FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive 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 restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. § 53(b).

DEFENDANTS

6. Defendant ruby Corp. ("Ruby"), formerly known as Avid Life Media Inc., is a privately-held corporation with its principal place of business at 20 Eglinton Avenue West, Toronto, Ontario M4R 1K8. At all times material to this Complaint, Ruby has acted as a holding company for a number of entities that operate dating websites. Ruby transacts or has transacted business in this district and throughout the United States.

7. Defendant ruby Life Inc. ("Ruby Life"), also doing business as AshleyMadison.com, and formerly known as Avid Dating Life Inc., is a Canadian corporation

with its principal place of business at 20 Eglinton Avenue West, Toronto, Ontario M4R 1K8. At all times material to this Complaint, Ruby Life has owned and operated the Ashley Madison website. Ruby Life transacts or has transacted business in this district and throughout the United States.

8. Defendant ADL Media Inc. ("ADL Media") is a Delaware corporation with its principal place of business at 1209 Orange Street, Wilmington, Delaware 19801. At all times material to this Complaint, ADL Media has collected AshleyMadison.com's U.S. revenue from various payment processors. ADL Media transacts or has transacted business in this district and throughout the United States.

COMMERCE

9. At all times material to this Complaint, Ruby, Ruby Life, and ADL Media have maintained a substantial course of 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. Ruby is a privately-held holding company for various wholly-owned subsidiaries, including Ruby Life and ADL Media (collectively, "Defendants") that together operate a number of dating websites including AshleyMadison.com, CougarLife.com, EstablishedMen.com, and ManCrunch.com.

11. Created in 2002, Defendants' most profitable website is AshleyMadison.com, which is an online dating website for married individuals or people in committed relationships interested in having affairs with other adults. In 2015, Defendants earned an estimated $47.4 million in U.S. revenue from AshleyMadison.com.

12. While AshleyMadison.com has members from over 46 countries, the majority of the website's members reside in the United States. Since 2002, 18,981,464 people from the United States have created profiles on AshleyMadison.com. 15,790,849 of those profiles were male. 3,190,615 were female.

THE ASHLEY MADISON WEBSITE

13. On AshleyMadison.com, consumers establish dating profiles by entering their email address and providing information about themselves in the form of free-form text, selections from menus, and photographs. Defendants do not verify the email addresses consumers use to sign up for AshleyMadison.com.

14. Once consumers create their profiles on AshleyMadison.com, they can engage in a number of activities for free. For example, they can perform searches, receive communications known as "winks," and display and view photographs, among other things.

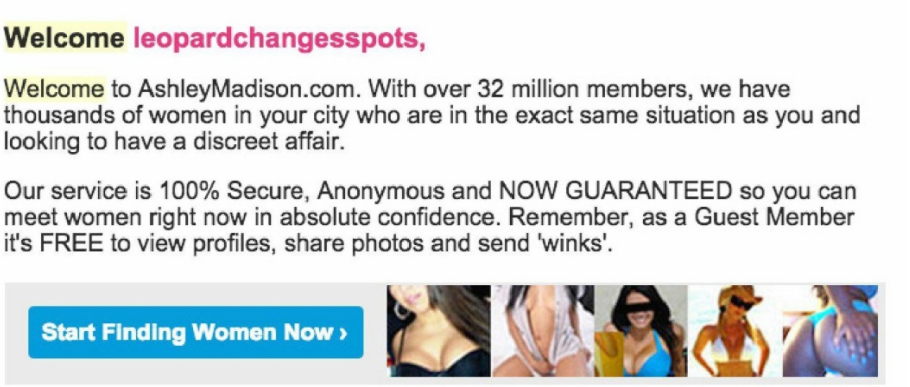
15. Consumers can engage in other activities on AshleyMadison.com only by paying money and upgrading to "full membership." Among other things, full members can send messages, initiate online real-time chats, or send virtual gifts. Other activities, which are not included in full membership, require subscriptions that consumers pay on a monthly basis. For example, "Priority Man" highlights the profiles of male members and elevates their profiles to a top position in search results. Over 1.4 million U.S. consumers paid for services from 2002 through 2015.

16. As part of their service, Defendants collect, maintain, and transmit a host of personal information including: full name; username; gender; address, including zip codes; relationship status; date of birth; ethnicity; height; weight; email address; sexual preferences and

desired encounters; desired activities; photographs; payment card numbers; hashed passwords; answers to security questions; and travel locations and dates. Defendants also collect and maintain consumers' communications with each other, such as messages and chats.

DEFENDANTS' USE OF ENGAGER PROFILES TO COMMUNICATE WITH CONSUMERS

17. When consumers sign up on AshleyMadison.com, the welcome message states that they "have thousands of women in [the consumer's] city who are in the exact same situation as [the consumer] and looking to have a discreet affair."



18. Until August 2014, Defendants engaged in a practice of using "engager profiles"—that is, fake profiles created by Defendants' staff who communicate with consumers in the same way that consumers would communicate with each other—as a way to engage or attract additional consumers to AshleyMadison.com. In 2014, there were 28,417 engager profiles on the website. All but 3 of the engager profiles were female.

19. Defendants created these profiles using profile information, including photographs, from existing members who had not had any account activity within the preceding one or more years.

20. Until August 2014, when U.S. consumers clicked on the "Start Finding Women

Now" link depicted in Paragraph 17, engager profiles appeared in their search results. Defendants created these engager profiles to interact with consumers by sending winks, automated replies, and stock messages. Defendants sent these communications to members on AshleyMadison.com who did not have credits in their accounts.

21. Because these engager profiles contained the same type of information as someone who was actually using the website, there was no way for a consumer to determine whether an engager profile was fake or real. To consumers using AshleyMadison.com, the communications generated by engager profiles were indistinguishable from communications generated by actual members.

22. As a result of Defendants' use of engager profiles, in many instances until April 2013, consumers without credits in their accounts were induced to upgrade to full memberships so that they could send emails and engage in online real-time chats with these fake profiles.

DELETION OF CONSUMER PROFILES

23. When consumers signed up for AshleyMadison.com, Defendants explained that their system is "100% secure" because consumers can delete their "digital trail."



24. If consumers decide they want to delete their profiles on AshleyMadison.com, they can click on a "Delete Profile" link in their profile settings, which will give them two options: a "Basic Deactivation" or a "Full Delete" (see Exhibit A).

25. Basic Deactivation allows consumers to remove their profiles from search results, but profile information and messages are still accessible to other people with whom consumers have communicated. Consumers can use the Basic Deactivation option free of charge, and it is reversible if they decide to return to AshleyMadison.com.

26. Defendants market the Full Delete option on AshleyMadison.com as a way for consumers to remove their profiles from the website completely. The Full Delete option states that it includes removal of: profiles from search results; profiles from the website; messages sent and received; messages from a recipient's mailboxes, including winks and virtual gifts; site usage history; personally identifiable information; and photographs from the site.

27. Until July 2015, Defendants charged consumers $19 to use the Full Delete option. This option, along with the accompanying charge, was available to consumers who decided to no longer engage with the site. From December 2012 through December 2015, 125,714 U.S. consumers paid a total of $2,388,566 for the Full Delete option.

28. In many instances, Defendants removed consumer profiles from AshleyMadison.com within 48 hours of receiving a Full Delete request, but retained personal information for up to 12 months. In other instances, Defendants failed to remove consumer profiles from their internal systems.

29. After purchasing the Full Delete option, for the first time, Defendants notified consumers that "[s]ome information will be retained for 6-12 months due to legal and financial reasons after which it will be removed as well."

DEFENDANTS' STATEMENTS REGARDING
PRIVACY AND DATA SECURITY

30. Until at least October 2015, Defendants described AshleyMadison.com as secure:

a. on the homepage by prominently displaying an icon of a "Trusted Security Award," an icon indicating that the website was an "SSL Secure Site," and an image indicating that the website offered "100% Discreet Service";



b. in statements by Defendants' executives on AshleyMadison.com that the website was "100% secure," "risk free," and "completely anonymous";

c. in advertisements describing AshleyMadison.com as "secure," "anonymous," and "risk free" (see Exhibits B–C); and

d. in Defendants' Terms and Conditions and Privacy Policy via a link on the AshleyMadison.com sign-up page. With respect to the security safeguards, the Privacy Policy states:

> We treat data as an asset that must be protected against loss and unauthorized access. To safeguard confidentiality and security of your PII, we use industry standard practices and technologies including but not limited to "firewalls," encrypted transmission via SSL (Secure Socket Layer) and strong data encryption of sensitive personal and/or financial information when it is stored to disk.

DEFENDANTS' FAILURE TO REASONABLY SECURE THEIR NETWORK AGAINST UNAUTHORIZED ACCESS

31. Defendants have engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to personal information on their network. Among other things, Defendants have:

a. failed to have a written organizational information security policy;

b. failed to implement reasonable access controls. For example, they:

i. failed to regularly monitor unsuccessful login attempts;

ii. failed to secure remote access;

iii. failed to revoke passwords for ex-employees of their service providers;

iv. failed to restrict access to systems based on employees' job functions;

v. failed to deploy reasonable controls to identify, detect, and prevent the retention of passwords and encryption keys in clear text files on Defendants' network; and

vi. allowed their employees to reuse passwords to access multiple servers and services;

c. failed to adequately train Defendants' personnel to perform their data security-related duties and responsibilities;

d. failed to ascertain that third-party service providers implemented reasonable security measures to protect personal information. For example, Defendants failed to contractually require service providers to implement reasonable security; and

e. failed to use readily available security measures to monitor their system and assets at discrete intervals to identify data security events and verify the effectiveness of protective measures.

32. In addition, contrary to Defendants' statement in Paragraph 30(a), Defendants never received a "Trusted Security Award" from any organization.

SECURITY INCIDENTS

33. To gain remote access to Defendants' corporate network, employees of Defendants and their service providers needed to use (1) their own unique passwords, and (2) a second, shared password common to all legitimate users of Defendants' network. Defendants' failures described in Paragraph 31 resulted in inadequate security for both of these passwords. For example, individual passwords and encryption keys were stored as plain text in emails and text files on Defendants' network, and a text file containing the "shared password" for access to the Defendants' virtual private network (VPN) was available on the Defendants' Google Drive.

34. As a result of Defendants' failures, intruders were able to gain access to these passwords and log in to the networks of Defendants and their service providers on multiple occasions in 2014 and 2015. Specifically:

a. On multiple occasions from November 1, 2014, through April 9, 2015, intruders were able to log into Defendants' VPN, which was a system used to allow remote access to Defendants' corporate network; and

b. On May 17, 2015, and June 9, 2015, there were successful unauthorized logins to one of AshleyMadison.com's payment processors using Defendants' credentials.

35. Because of Defendants' failure to monitor their system logs at discrete intervals, Defendants were unaware that there were unauthorized individuals who had access to employee and service provider credentials. It was not until after the data breach that Defendants became aware of these unauthorized logins.

DATA BREACH

36. On July 12, 2015, Defendants' employees detected a large file of data being transferred from one database to another. The next day, a notice appeared on two of Defendants' customer service computers stating that the company had been hacked and demanding the immediate shut down of AshleyMadison.com and EstablishedMen.com. The message warned that if Defendants did not immediately and permanently shut down those websites, the hackers would release all customer records for the sites, as well as employee documents and email communications.

37. On August 18 and 20, 2015, a group identifying itself as "The Impact Team" published 9.7 gigabytes of information online pertaining to more than 36 million AshleyMadison.com customers and Defendants themselves. The information included the full name of paying customers and usernames and email addresses of non-paying customers, in conjunction with the following categories of information:

a. profile information—including relationship status, gender, date of birth, sexual preferences and desired encounters, and desired activities;

b. account information—including codes corresponding to security questions, security answers, and hashed passwords; and

c. billing information for paying customers including billing addresses and the last four digits of consumers' credit and debit card numbers. Full credit card numbers for some consumers were contained in the published data.

38. Information of consumers who paid for Full Delete was included in the information that was published online.

39. Once information was published, a number of websites appeared where people could determine whether someone was a member of AshleyMadison.com by inputting an email address.

THE IMPACT OF DEFENDANTS' FAILURES ON CONSUMERS

40. Defendants' failures to provide reasonable security for the sensitive, personal information they collected, transmitted, and stored, including sexual preferences and desired encounters, desired activities, email addresses, security questions and answers, real names, billing addresses, and credit card numbers, has caused or is likely to cause substantial injury to consumers in the form of extortion, fraud, disclosure of sensitive, personal information, and other harm.

41. The security incidents and data breach described in Paragraphs 33–39 exacerbated the risk of these harms. These incidents led to the creation of websites where people could determine whether someone was a member of AshleyMadison.com, thereby disclosing consumers' highly sensitive, private information. Consumers could not reasonably avoid these harms.

42. Defendants could have prevented or mitigated these risks through relatively low-cost measures.

VIOLATIONS OF THE FTC ACT

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

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

45. Acts or practices are unfair under Section 5 of the FTC Act if they cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I
MISREPRESENTATIONS REGARDING NETWORK SECURITY

46. As described in Paragraph 30, Defendants have represented, expressly or by implication, directly or indirectly, that they took reasonable steps to ensure that AshleyMadison.com was secure.

47. In truth and in fact, as described in Paragraphs 31–39, Defendants did not take reasonable steps to ensure that AshleyMadison.com was secure. Therefore, the representation set forth in Paragraph 46 is false or misleading.

COUNT II
MISREPRESENTATIONS REGARDING USER PROFILES

48. As described in Paragraphs 17 and 22, until April 2013, Defendants have represented, expressly or by implication, directly or indirectly, that communications received by members were from actual women interested in communicating with those members.

49. In truth and in fact, as described in Paragraph 18, many of the communications received by members were not from actual women, but instead were from engager profiles

Defendants' staff created. Therefore, the representation set forth in Paragraph 48 is false or misleading.

COUNT III
MISREPRESENTATIONS REGARDING THE TERMS AND CONDITIONS FOR DELETING PROFILES

50. As described in Paragraphs 23–27, Defendants have represented, expressly or by implication, directly or indirectly, that they would delete all of the information of consumers who chose the Full Delete option on AshleyMadison.com.

51. In truth and in fact, as described in Paragraphs 28–29, even for those consumers who paid a $19 fee for the Full Delete option, Defendants retained the information from those profiles for up to 12 months. Therefore, the representation set forth in Paragraph 50 is false or misleading.

COUNT IV
MISREPRESENTATIONS REGARING DATA SECURITY SEAL

52. As described in Paragraph 30(a), Defendants have represented, expressly or by implication, directly or indirectly, that AshleyMadison.com had received a "Trusted Security Award."

53. In truth and in fact, as described in Paragraph 32, Defendants never received a "Trusted Security Award." Therefore, the representation set forth in Paragraph 52 is false or misleading.

COUNT V
UNFAIR SECURITY PRACTICES

54. As set forth in Paragraph 31, Defendants have failed to take reasonable steps to prevent unauthorized access to personal information on their network.

55. Defendants' actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

56. Therefore, Defendants' practices as described in Paragraph 54 above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

CONSUMER INJURY

57. Consumers have suffered or are likely 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

58. 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

59. Wherefore, the FTC, 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, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

c. Award the FTC 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,

David C. Shonka
Acting General Counsel

Dated: 12/14/16

Shameka L. Walker
D.C. Bar. No. 493891
Andrea V. Arias
D.C. Bar No. 1004270
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
202-326-2570 (Walker)
202-326-2715 (Arias)

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION