

1 Microsoft alleges violations of the Computer Fraud and Abuse Act against all defendants.
2 Microsoft alleges violations of the Washington Consumer Protection Act against Eric C. Ralls
3 (“Ralls”) and Does 1-9 (the “Doe Defendants”). Microsoft brings claims in tort against Eric C.
4 Ralls (“Ralls”), Vertro, Inc. (“Vertro”), and the Doe Defendants under the laws of Washington.
5 Microsoft brings its claim for breach of contract against RedOrbit under Washington law, and its
6 claims in tort against RedOrbit under Texas law in accordance with an agreement between
7 Microsoft and RedOrbit, Inc. (“RedOrbit”).

8 **THE PARTIES**

9 1. Plaintiff Microsoft Corporation (“Microsoft”) is a Washington corporation
10 with its principal place of business in Redmond, Washington.

11 2. Defendant Eric C. Ralls is an individual believed to be a resident of Dallas,
12 Texas. On information and belief, Ralls was the president of RedOrbit, Inc. during the period of
13 time when the events giving rise to this complaint occurred.

14 3. Defendant RedOrbit, Inc., formerly known as Red Nova, Inc., is a Texas
15 corporation with its principal place of business in Tyler, Texas. RedOrbit publishes a website
16 named RedOrbit.com. Through RedOrbit.com, RedOrbit purports to provide a variety of
17 photographs, articles, and videos on science-related subjects.

18 4. Defendant Vertro, Inc., formerly known as Miva, Inc., formerly known as
19 FindWhat.com, is a Delaware Corporation with its principal place of business in New York, New
20 York. Vertro is an Internet company that owns and operates a line of software products. In June
21 2005, FindWhat.com changed its name to Miva, Inc. In June 2009, Miva, Inc changed its name
22 to Vertro, Inc. For purposes of clarity, this complaint will refer to the entity variously known as
23 FindWhat.com, Miva, Inc., or Vertro, Inc., as “Vertro.” On information and belief, until March
24 12, 2009, Vertro owned and operated business units known, *inter alia*, as SearchFeed and Miva
25 Media. While owned and operated by Vertro, Miva Media operated an online auction based pay-
26 per-click advertising network in North America and Europe.

27 5. Microsoft is unaware of the true name and capacity of the Doe Defendants and
28 therefore sues the Doe Defendants by that fictitious name. Microsoft will amend this complaint

THE PRESENT CONTROVERSY

Microsoft’s adCenter Platform

10. Microsoft owns and operates an online advertising platform called Microsoft adCenter™ (“adCenter”).¹ As part of its adCenter business, Microsoft contracts with various companies who wish to place advertisements on the Internet (hereinafter, “Advertisers”). Through the adCenter platform, Advertisers manage various aspects of their online advertising campaigns including budgeting, ad-placement, and analysis of results. Microsoft places the Advertisers’ advertisements on, among other places, a network of websites published by other entities or individuals (hereinafter, “Publishers”) that also participate in Microsoft’s advertising network program.

11. An individual viewing a Publisher’s website can click on an advertisement of interest. This action connects the individual to the Advertiser’s website where additional information about the product or service being advertised will be displayed. The goal of the Advertiser at this point is to encourage the individual to take additional actions such as requesting more information about or purchasing the Advertiser’s products or services. These additional actions taken on an Advertiser’s website are referred to as “conversions,” and may be tracked and monitored by Advertisers.

12. Following a click on an advertisement, the adCenter platform debits the account of the Advertiser that paid to place the advertisement, and credits the account of the Publisher of the website where the click occurred. In one common approach known as “pay-per-click,” Advertisers pay for each click on their advertisement, although on the adCenter platform advertisers are generally not charged for clicks of dubious quality or origin. Similarly, the Publisher’s account is credited for each click. A pay-per-click system allows Publishers to profit from the time, effort, and money invested in developing interesting and useful websites without requiring them to directly charge users for access to their websites. It benefits Advertisers by allowing them to place advertisements on websites likely to attract individuals interested in their

¹ Microsoft has renamed adCenter to “pubCenter,” but for purposes of clarity, this complaint refers to it as “adCenter” throughout.

1 products or services, and by connecting them with the individuals who have, by clicking on an
2 advertisement, shown an interest in their products or services.

3 13. Consistent with its Terms of Use, Microsoft's adCenter platform gathers and
4 maintains valuable data related to its advertising operations. Among other data, it maintains
5 account information for both Advertisers and Publishers, records the placement of
6 advertisements, and records contextual data related to each click. The data accumulated by
7 adCenter is a significant asset for Microsoft. It enables Microsoft to manage and develop its
8 adCenter business, and it enables the Advertisers and Publishers that participate in adCenter to
9 effectively manage their own advertising campaigns. Microsoft adCenter's nationwide and
10 global operations are supported by a Microsoft-owned network of computers that receive,
11 process, store, and communicate the data to different parts of, or participants in, the adCenter
12 network.

13 **Click-Fraud and Click-Laundering, Generally**

14 14. Pay-per-click systems are not immune to fraud. An unscrupulous Publisher
15 could, for example, use automated scripts, end-user computers infected with malware², or hired-
16 individuals to generate a large number of clicks on the advertisements placed on its website by
17 adCenter. Because such methods merely imitate the actions of a legitimate user of a web browser
18 clicking on an advertisement, but do so for the sole purpose of generating a charge per click
19 without having any interest in the product or service being advertised, the clicks are considered
20 fraudulent. This activity is termed "click-fraud." A Publisher engaged in click-fraud can reap ill-
21 gotten profits because, for each click recorded, the Publisher's account is credited at the expense
22 of the Advertiser whose advertisement was clicked.

23 15. For example, in one simple click-fraud scheme, a Publisher hires individuals to
24 simply visit the Publisher's website and repeatedly click on the advertisements placed there. In
25 the absence of fraud-detection measures, each time such a hired-individual clicks on an

26 ² The term "malware" as used in this Second Amended Complaint, refers to malicious software that is surreptitiously
27 installed on a user's computer without the user's knowledge or consent, and which operates to harm the user's
28 computer and/or other vulnerable networked computers, and/or interfere with the user's use of the computer.
"Spyware" is a type of malware that typically collects information about a user and the user's online activity without
the user's knowledge.

1 advertisement on the Publisher's site, the account of the Advertiser whose advertisement is
2 clicked can potentially be debited, and the account of the Publisher of the website where the click
3 occurred is credited. Such a click should be deemed fraudulent because the person behind the
4 click has no legitimate interest in the products or services advertised and is clicking on the
5 advertisement for the sole purpose of defrauding the Advertiser.

6 16. In other more sophisticated schemes, Publishers can generate a large number
7 of invalid clicks by channeling innocent end-users browsing online to websites the Publisher
8 controls and tricking them into clicking on online advertisements. A variety of techniques can be
9 used to channel users to a particular website. For example, a Publisher can purchase Internet
10 traffic from individuals or entities that have installed malware on end-users' computers connected
11 to the Internet. The malware can then be used to route the end-users to websites controlled by the
12 paying Publisher. Once on the website controlled by the Publisher, the end-user can be tricked
13 into clicking on advertisements. For example, links to advertisements can be hidden beneath
14 links to legitimate-looking topics. By clicking on the legitimate-looking link, the end-user causes
15 a click on the invisible advertisement to be recorded.

16 17. In other instances, infected end-user computers are recruited into networks of
17 infected computers known as "bot-nets" that can be remotely controlled for illegal purposes.
18 Such bot-nets can be used to generate clicks on advertisements on websites with no participation
19 from the end-user. Bot-nets that are specialized for this purpose are referred to as "click-bots."
20 Automated scripts can also be used to generate clicks on advertisements.

21 18. It is not uncommon for a Publisher to pay other entities or individuals to find
22 users and channel them to its website. There is nothing inherently fraudulent about this practice.
23 In the absence of fraud, it is commonly referred to as "buying traffic." However, these other
24 entities or individuals can also use all of the fraudulent means already alleged to generate invalid
25 traffic. In these cases, the traffic is commonly referred to as "bad traffic." The Publisher that
26 purchases bad traffic, regardless of whether it knows of the fraudulent origin of the traffic, can
27 ultimately profit from it by using it to drive up the number of clicks on the advertisements placed
28 on its website. At the end of the line is an Advertiser who is charged for the invalid clicks that

1 are generated through these schemes.

2 19. Click fraud schemes damage Microsoft as well as the Advertisers and
3 legitimate Publishers participating in Microsoft's adCenter advertising network or any advertising
4 network. Advertisers are wrongfully charged for fraudulent clicks, Microsoft must expend
5 resources in investigating and remedying the harms caused by the click fraud, adCenter
6 operations are disrupted, the reputations of Microsoft and adCenter are damaged, and Microsoft's
7 relations with the victimized Advertisers are harmed. Beyond this, the underground economy that
8 has grown up around the monetization of fraudulently generated clicks depends upon, and in
9 effect finances, the creation and propagation of malware that is used to infect and capture the
10 computers of end-users world-wide.

11 20. At its very essence, click-fraud is the theft of money from Advertisers by
12 fraudsters. This thievery is all the more insidious because it can be difficult to detect. Individuals
13 and entities bent on fraud have grown adept at hiding the improper origin of the invalid clicks
14 through technical measures meant to defeat the fraud-detection systems deployed, for example,
15 by adCenter. Microsoft refers to such attempts at hiding the improper origin of clicks as "click-
16 laundering," and it will refer to them as such in this complaint. Click-laundering techniques
17 include channeling unsuspecting end-users to websites where they can be tricked into triggering
18 clicks on advertisements, and using scripts or other methods to alter the information associated
19 with the clicks recorded, for example, by adCenter. Click-laundering techniques also include
20 using click-bots to generate clicks, but routing the click-bot traffic through various websites to
21 disguise its fraudulent origin. Over time, click-laundering operations have grown in scale and
22 sophistication and now constitute a major engine of click-fraud.

23 **RedOrbit and Ralls' History of Purchasing Fraudulently Generated Traffic.**

24 21. Microsoft is informed and believes, and on that basis alleges, that beginning no
25 later than 2005 and continuing each year thereafter up to and through August 2010, RedOrbit has
26 purchased traffic from vendors that generate it using malware and, potentially, other fraudulent
27 means. RedOrbit's history in this regard was unknown to Microsoft when it allowed RedOrbit to
28 join the adCenter beta program in September 2008.

1 22. In 2006, in *Elite Street, LLC v. Eric Ralls and Red Nova, Inc.*, No.
2 602496/2006 (N.Y. Sup. Ct., New York Cnty, 2006), Elite Street, Inc. (“Elite Street”) sued
3 RedOrbit (F/K/A Red Nova, Inc.) for, *inter alia*, breach of contract based on RedOrbit’s alleged
4 non-payment for advertising services. RedOrbit made the following admissions in its
5 counterclaims. That on or about August 25, 2005, it entered into a contract with Elite Street,
6 known as an “Insertion Order,” pursuant to which Elite Street agreed to provide advertising
7 services to RedOrbit. That it entered into a second and third insertion order with Elite Street in
8 November 2005. That, starting in December 2005, Internet users began to complain to RedOrbit
9 that RedOrbit’s website hijacked their browsers through the use of malware, and that RedOrbit’s
10 advertisements continually “popped-up” on their computers, interrupting their ability to use their
11 computers. That, despite these problems, RedOrbit made all payments under the first, second,
12 and third insertion orders. That, on or about January 11, 2006, it entered into a fourth insertion
13 order pursuant to which Elite Street agreed to provide advertising services to RedOrbit for
14 approximately six months. That, in February, March, April, and May 2006, RedOrbit received
15 additional complaints from Internet users that RedOrbit’s website hijacked their browser through
16 the use of malware, and that RedOrbit’s advertisements continually “popped-up” on their
17 computers interrupting their ability to use their computers. That, it continued to pay Elite Street
18 during this period.

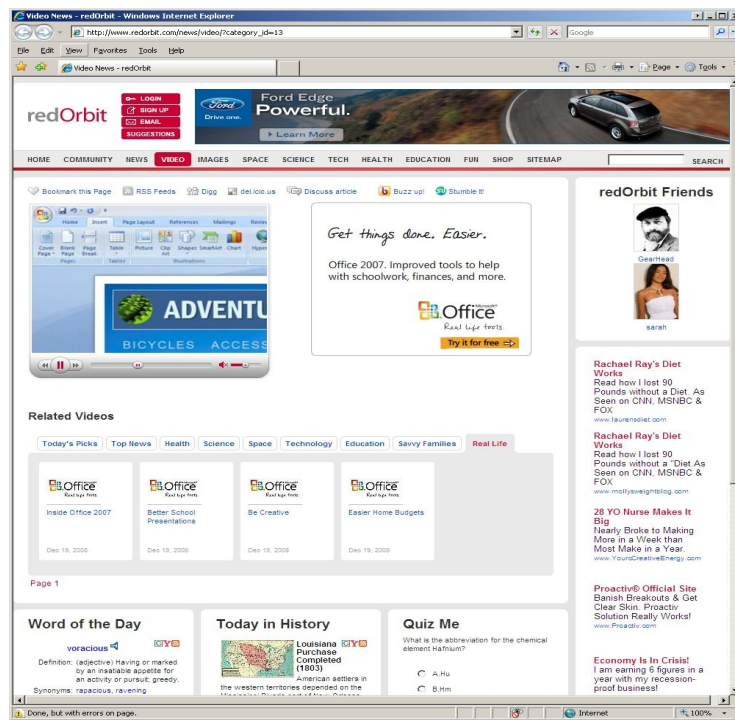
19 23. In 2007, in *Pennyweb, Inc. v. Argonaut Media, Inc., RedOrbit, Inc., and Does*
20 *1-10*, Case No. BC373664 (Cal. Super. Ct., Los Angeles Cnty, 2007), Pennyweb, Inc.
21 (“Pennyweb”) sued Argonaut Media, Inc., (“Argonaut”) and RedOrbit for, *inter alia*, breach of
22 contract. Pennyweb made the following accusations against RedOrbit: That, on or about June
23 21, 2006, Argonaut and RedOrbit entered into an “Online Media Placement Agreement” to create
24 and provide Internet advertising services for RedOrbit.com. That, on or about July 25, 2006,
25 Argonaut, after designing the display ad “creative” for RedOrbit, contracted with Pennyweb, an
26 Internet advertising network, to run the RedOrbit creative across multiple websites that comprised
27 Pennyweb’s network of affiliated websites. That, the type of creative designed by Argonaut for
28 RedOrbit to advertise the RedOrbit site was a “popped URL.” That, in essence, when an Internet

1 user would log onto one of the websites in Pennyweb's network of affiliated websites,
2 Pennyweb's ad-serving technology would deliver the RedOrbit "popped URL" to that user's
3 personal computer in such a form that the user's entire personal computer screen would be taken
4 over by the RedOrbit.com website. That, when the "popped URL" in the form of the
5 RedOrbit.com webpage, appeared on a user's screen, that page would contain up to five
6 advertisements from five separate advertisers. That, in that scenario, RedOrbit would pay for one
7 impression, and in turn be paid by the up-to-five advertisers whose advertisements were displayed
8 on the RedOrbit site.

9 24. Microsoft is informed and believes, and on that basis alleges that RedOrbit did
10 receive malware-generated traffic during 2006, a practice that continued through 2007 and 2008,
11 including the following eleven observed incidents, which Microsoft believes to constitute a tiny
12 fraction of those that actually occurred: On February 17, 2006, a computer infected with the
13 malware known as "Deskwizz/Searchingbooth" was observed to send traffic to an intermediate
14 site that then displayed Redorbit.com. On April 22, 2006, a computer infected with the malware
15 known as "YourEnhancement" was observed to send traffic through various intermediary
16 websites to RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On April 28,
17 2006, a computer infected with the Deskwizz/Searchingbooth malware was observed to send
18 traffic to RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On April 29,
19 2006, a computer infected with the YourEnhancement malware was observed to send traffic to
20 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On May 21, 2006, a
21 computer infected with the malware known as "Look2me" was observed to direct traffic to
22 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On July 7, 2006, a
23 computer infected with the malware known as "Dollarrevenue" was observed to send traffic to
24 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On March 17, 2007, a
25 computer infected with the Deskwizz/Searchingbooth malware was observed to send traffic to
26 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On December 6, 14, 20,
27 and 24, 2008, malware-originated traffic, including traffic generated by the malware known as
28 "Interplusclick," was observed to pass through an intermediate website known as

1 SearchFeed.com, which sent the traffic on to RedOrbit.com.

2 25. The image below shows the screen of a malware-infected system which, on
3 December 20, 2008, was forced to visit the RedOrbit site on which multiple advertisements for
4 Office 2007 were displayed. The image shown appeared entirely unrequested by the user, filled
5 the entire computer screen, gave no indications of why RedOrbit.com had appeared, and gave no
6 indication of how users could find and remove the malware that caused the RedOrbit.com to
7 appear:



22 Events Giving Rise to This Complaint

23 **RedOrbit joins the adCenter beta program**

24 26. This action arises out of the Defendants' general abuse of the adCenter online
25 service by generating clicks through fraudulent means and laundering those clicks to escape
26 detection, and of Defendants' continued and ongoing use of malware-generated traffic to force
27 end-users to view advertisements for Microsoft products.

28 27. RedOrbit joined the Microsoft adCenter Publisher beta program on or around

1 September 19, 2008. By agreeing to participate in the beta program, RedOrbit agreed to the
2 Microsoft adCenter Publisher Pre-Release License and Service Agreement (the “Agreement”),
3 attached hereto as Exhibit A, as all Publishers must. The Agreement prohibited, *inter alia*, the
4 following acts:

- 5 • “work[ing] around any technical limitations in the Service or introduce[ing] or us[ing]
6 any device, software, or routine that interferes or attempts to interfere with the
7 operation of the Service or otherwise attempt[ing] to access the Service in any manner
8 other than those authorized by Microsoft;
- 9 • access[ing] the Service from any websites or other locations, other than [the
10 Publisher’s] Websites that have been approved by Microsoft;
- 11 • “Cach[ing], stor[ing], copy[ing], distribut[ing], or redirect[ing] any Ads delivered by
12 the Service;
- 13 • directly or indirectly generat[ing] impressions or clicks on an [sic] Ads, or
14 authoriz[ing] or encourag[ing] others to do so, through any automated, deceptive,
15 fraudulent or other invalid means;
- 16 • Edit[ing], modify[ing], filter[ing], obscur[ing], or reorder[ing] any Ads (including
17 their associated links) supplied by the Service; or
- 18 • Fram[ing], minimiz[ing], remov[ing], redirect[ing], delay[ing], or otherwise
19 inhibit[ing] or modify[ing] the display of any web page accessed by the links included
20 with an Ad.” Exhibit A, ¶ 4.

21 28. The Agreement further gave Microsoft the right to withhold payment for clicks
22 that Microsoft deemed fraudulent, and to terminate the Publisher’s participation in adCenter at
23 any time. The Agreement further stated that

24 Washington state law governs the interpretation of this agreement and
25 applies to claims for breach of it, regardless of conflict of laws principles.

26 The laws of the state where you live govern all other claims, including
27 claims under state consumer protection laws, unfair competition laws, and
28 in tort. Exhibit A, ¶ 15.

RedOrbit and Ralls agree to buy traffic from Vertro

1
2 29. Between September, 2008, when RedOrbit joined the adCenter program, and
3 December 2008, adCenter received data from RedOrbit's primary web property, RedOrbit.com,
4 and recorded approximately 75 clicks considered "valid" per day on advertisements placed there.
5 During this time, unbeknownst to Microsoft, RedOrbit was buying traffic from SearchFeed, a
6 business unit of Vertro. The volume of traffic that Ralls purchased from SearchFeed was sizable.
7 By mid-January 2009, on information and belief, Ralls owed SearchFeed approximately \$180,000
8 for traffic purchased in the prior months.

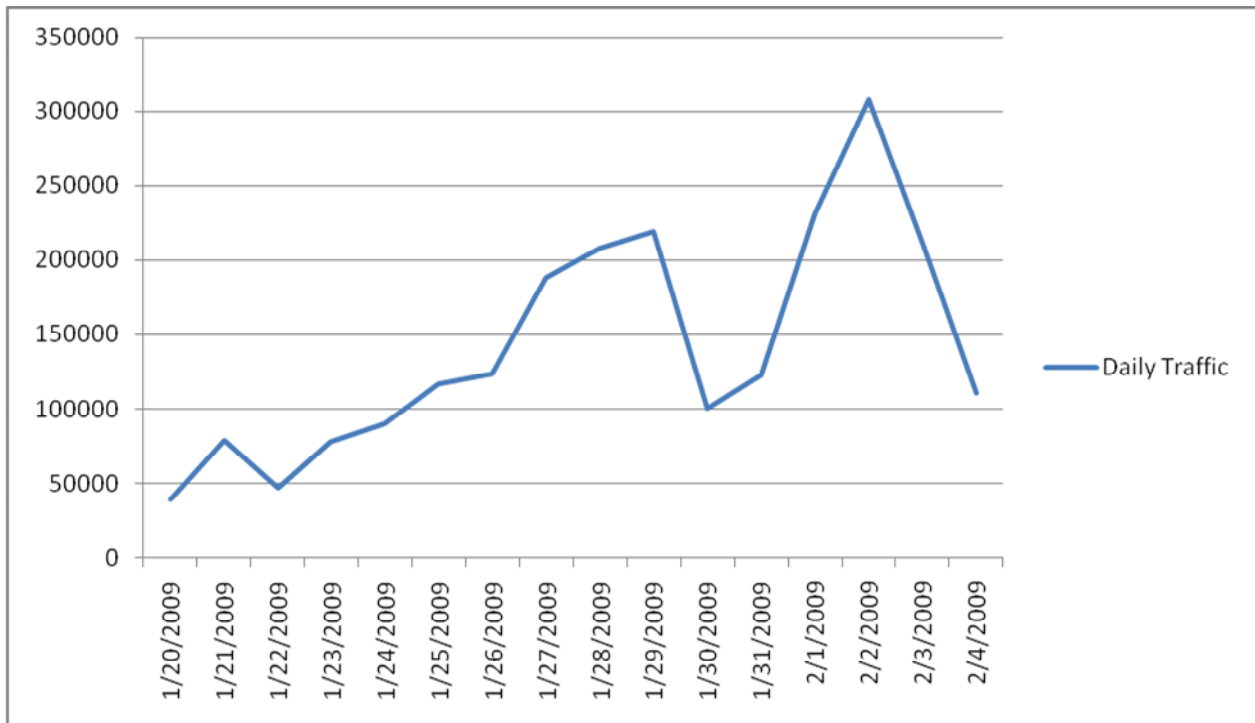
9 30. On January 13, 2009, Miva Media, another division of Vertro, contacted Ralls
10 and asked if he would be interested in a "business development opportunity," offering to sell
11 RedOrbit traffic from its own network of affiliated websites.

12 31. Ralls told Miva Media that one of his goals was to generate "high interaction
13 (ctr)," meaning, a high click through rate, with the ads on his site. Miva Media responded that it
14 had a number of different "feeds" starting at the price of one cent per visit that would be a good
15 fit for him. On January 14, Miva Media set up an account for RedOrbit in their system, and on
16 January 16, Ralls gave Vertro credit card details to fund the purchases of traffic. On information
17 and belief, Vertro's SearchFeed division stopped sending RedOrbit traffic on or about January 19.
18 On January 20, a Miva Media division feed to RedOrbit went live, and began directing traffic
19 generated on websites affiliated with the Miva Media network to RedOrbit. RedOrbit and Ralls
20 began testing the traffic generated by the Miva Media feed.

21 32. The monitoring obviously encouraged Ralls and RedOrbit, because by 7:53
22 A.M., E.S.T. on January 21, RedOrbit boosted its advertising budget on Miva to \$2500.
23 Evidently the traffic flooded in, because by 3:00 PM that day, Ralls asked Vertro if there was any
24 way to limit the hourly spend so that his entire budget would not be consumed in one or two
25 hours. At Vertro's suggestion, that evening, Ralls authorized Vertro to divide his daily campaign
26 into 24 separate sequential one hour campaigns, and funded each with a budget of \$50. Vertro
27 had the 24 campaigns ready to go live by January 22. On January 23, Ralls increased the budget
28 for each of the 24 sequential one-hour campaigns to \$100. Meanwhile, Vertro was "optimizing"

1 the feed to RedOrbit, and by January 24 had removed some of the sources from the feed that were
2 giving RedOrbit a less than 10% “ROI” or, presumably, “return on investment.”

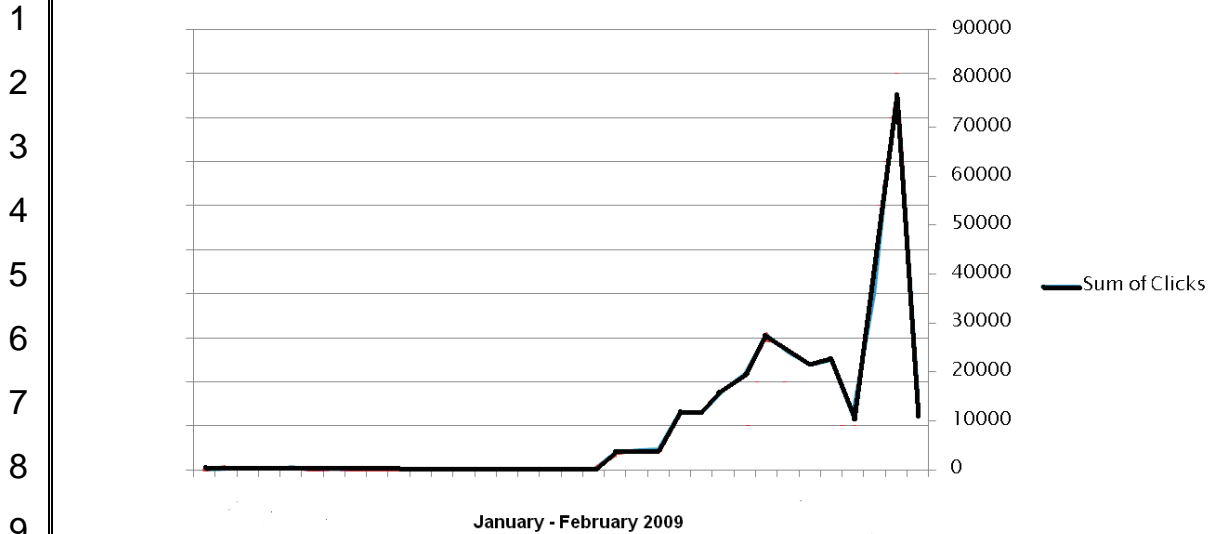
3 33. A graph of the traffic from Vertro to RedOrbit.com between January 20 and
4 February 4 shows that it occurred in two spikes, with the first spike beginning on January 20 and
5 cresting on approximately January 28-29, and the second spike beginning on approximately
6 January 31 and cresting on approximately February 2.



20 **Microsoft detects a massive surge of fraudulent clicks on RedOrbit.com**

21 34. Starting on January 20, 2009, the same day the Miva Media feed to
22 RedOrbit.com went live, and continuing until February 4, 2009, adCenter recorded a substantial
23 surge in clicks on RedOrbit.com. These increased to an average of more than 10,000 clicks per
24 day. A graph of the clicks recorded from RedOrbit.com shows the peculiar surge, which occurred
25 in two spikes. The first spike began on January 20 and crested on approximately January 27, and
26 the second spike began on approximately January 31 and crested on approximately February 2,
27 closely matching the pattern of traffic from Vertro to RedOrbit.

28



35. Microsoft monitors the click-traffic on its adCenter network. It noticed the growth in clicks from RedOrbit.com and began investigating. Due to the sophisticated means believed to be employed by the Defendants to generate and launder the invalid clicks, the investigation into their activities was complex and time-consuming. By June 2009, Microsoft acquired sufficient evidence to cause it to believe that Ralls and RedOrbit were culpable for the January-February 2009 click-surge. Microsoft had already refunded advertisers for all clicks deemed fraudulent on RedOrbit's website during the time period at issue. The evidence, including evidence gathered through forensic analysis of Microsoft's own logs, showing that a script, click-bot or other automated process was being used to generate clicks, includes the following:

36. First, during the period of the click-surge, overall traffic to RedOrbit.com actually fell. Consistent with that, "impressions" also fell. Impressions occur when a user's browser shows an advertisement. However, at the same time traffic and impressions declined, the number of clicks on advertisements soared. The ratio measuring the number of clicks on advertisements to impressions of advertisements is referred to as the "click-through rate." The declining impressions and soaring clicks resulted in an abnormally high click-through rate.

37. Second, a very high percentage of the clicks lacked data normally associated with clicks generated when a person clicks on an advertisement from a browser. However, this

1 data is often missing from clicks generated by click-bots, scripts, or other automated processes
2 that simulate clicks on an advertisement.

3 38. Third, for the very high percentage of the clicks that lacked the normal data,
4 the average impression-to-click interval was abnormally short. The impression-to-click interval
5 measures the time delay between when a page with an advertisement is first visited and when the
6 advertisement is clicked on. A short interval is consistent with automated activity.

7 39. Fourth, conversions also declined during this period. *See* ¶ 11, *supra*
8 (explaining “conversions”). This is consistent with a declining percentage of actual users clicking
9 on advertisements.

10 40. Fifth, for a large number of clicks, Microsoft was able to determine the website
11 from which the traffic was referred to RedOrbit.com. For the majority of these clicks, the
12 referring websites appeared to have many commonalities among their designs, naming
13 conventions, content, and registration data. This suggesting that a small number of entities
14 designed and operated them. The websites appeared to lack any real content or serve any purpose
15 beyond routing traffic around the Internet. Some of these websites are linked through registration
16 and other data to some of the providers from which Vertro purchased traffic for resale to
17 RedOrbit.com between January 20 and February 4, 2009.

18 41. This evidence, among other facts, compelled Microsoft to the conclusion that
19 one or more of the Defendants had engaged in the fraudulent generation of fraudulent clicks and
20 had taken purposeful steps to launder the fraudulent clicks by hiding their improper origin.

21 42. The fraudulently generated clicks resulted in fraudulent data being sent to the
22 adCenter servers, corrupting the data on those servers. This data was used by adCenter to
23 determine which Advertiser should be charged for each click, and whether and how much
24 RedOrbit should be credited. RedOrbit and Ralls’ potential profits grew with each fraudulent
25 click.

26 43. On April 14, 2009, Ralls and RedOrbit sought payment from Microsoft for
27 clicks recorded in January and February 2009. On May 21, 2009, Ralls and RedOrbit again
28 sought payment from Microsoft, this time under threat of litigation, demanding that Microsoft pay

1 RedOrbit \$252,001.32 on or before the close of business on May 29, 2009. On information and
2 belief, by these acts, Ralls and RedOrbit intended to profit from the click-fraud operation.

3 **RedOrbit, Ralls, and Vertro knew of the fraudulent nature of the Vertro traffic**

4 44. On information and belief, Ralls and Vertro knew that some of the traffic from
5 Vertro was malware-generated. On January 23, Ralls informed Vertro that a percentage of
6 connections made by traffic from the Vertro network to RedOrbit.com stayed on RedOrbit.com
7 for less than one second. Microsoft is informed and believes and on that basis alleges that this is
8 a classic indication that the traffic is generated by a malware automated process, such as a click-
9 bot.

10 45. On information and belief, Vertro knew from the time the Miva Media feed to
11 RedOrbit went live that a significant portion of the traffic sold to RedOrbit between January 20
12 and February 3, 2009 came from websites featuring pornography or were generated in response to
13 searches on “adult” terms, and that Ralls and RedOrbit knew this fact no later than February 3.
14 Ralls detected that advertisements for RedOrbit.com were being placed by Miva Media on
15 pornography sites and on February 3 requested that he no longer be sent traffic from these
16 sources. However, on February 5, after Ralls saw how significantly his incoming traffic declined
17 without the traffic generated on pornography sites or in response to adult search terms, he
18 instructed Vertro to start sending him such traffic again.

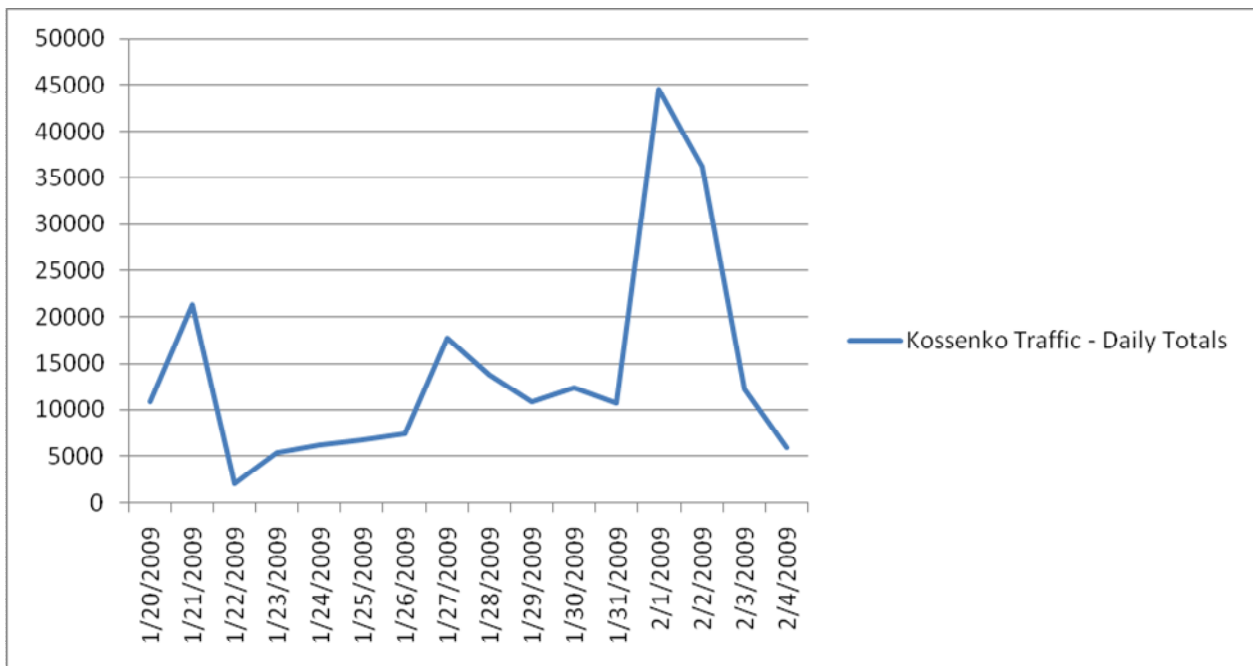
19 46. Microsoft is informed and believes and on that basis alleges that pornography
20 sites are often sources of fraudulent traffic. A high percentage of traffic originating from
21 pornography sites and directed to a purported science and technology site would have alerted both
22 Ralls and Vertro to the likely fraudulent origin of the traffic. The decline in traffic that Ralls
23 observed following his temporary decision to stop receiving traffic from pornography websites or
24 in response to searches on adult search terms would have alerted him to the fact that starting
25 January 20, a significant percentage of the traffic he had purchased and that he had used to
26 generate clicks on adCenter ads on RedOrbit had come from those sources.

27 47. Vertro knew that one of the largest contributors of traffic to the feed that was
28 being sold to RedOrbit was an individual named Saveli Kossenko (“Kossenko”). Overall,

1 Kossenko contributed 9.85% of the traffic sold to RedOrbit between January 20 and February 4.
 2 Vertro knew that Kossenko was reputed to use malware to generate traffic. In *In re Miva, Inc.*,
 3 *Securities Litigation*, 511 F. Supp. 2d 1242 (M.D. FL, 2007), Vertro, known at the time as
 4 FindWhat.com, was sued for securities fraud. In its March 2007 ruling denying a motion to
 5 dismiss, the court summarized some of the allegations related to Kossenko as follows:

6 During the class period, two of FindWhat's main revenue generating
 7 distribution partners (Saveli Kossenko and Dmitri I/n/u), who represented
 8 36% of FindWhat's revenues, were using illegal means to inflate revenues.
 9 This included the use of spyware, browser hijacking software, and “non-
 10 human traffic.” The use of such illicit methods of creating internet traffic,
 11 commonly referred to as “click-fraud,” . . . *Id.* at 1249.

12 48. The traffic from Kossenko that Vertro sold to RedOrbit shows that Kossenko’s
 13 contribution to the feed also occurred in three spikes, the second cresting on January 27, and the
 14 third cresting on February 2:



15
16
17
18
19
20
21
22
23
24
25
26
27 49. On information and belief, Ralls and RedOrbit determined, based on the
 28 soaring click-through rate on RedOrbit.com, that the traffic purchased from Vertro was fraudulent

1 in origin and was resulting in a massive number of fraudulent clicks on advertisements on
2 RedOrbit.com. On information and belief, Ralls and RedOrbit intended to profit from that traffic
3 by inducing Microsoft to charge Advertisers for the fraudulent clicks and to credit RedOrbit's
4 account for the clicks. On information and belief, Ralls and RedOrbit accessed and used
5 adCenter's computers to manage the RedOrbit account. On information and belief, their purpose
6 in doing so was to further the click-fraud operation.

7 50. On February 9, 2009, during the time when, on information and belief, Ralls
8 was still hoping to continue operating as a publisher on Microsoft's adCenter network, Ralls
9 requested that Vertro set up a new campaign related to health, saying, "please use this text," for
10 the campaign:

11 Mailscanner has detected a possible fraud attempt from www.redorbit.com claiming to be
12 www.redOrbit.com – science, Health, Technology . . . redOrbit.com is the premier
13 science, health, and technology news and information portal on the web. Learn something
14 new today."

15 51. On information and belief, the text requested by Ralls was meant to be used in
16 advertisements placed on Vertro's network of affiliated websites. On information and belief,
17 Vertro set the campaign up the same day without questioning the strange and misleading text of
18 the campaign.

19 **Ralls and RedOrbit Concealed Evidence Related to the Click-Surge**

20 52. On January 26, February 4, February 5, February 6, and February 9, 2009
21 Microsoft sent Ralls and RedOrbit e-mails informing them that the RedOrbit account was under
22 investigation and seeking information from them. In response to Microsoft's inquiries, Ralls
23 admitted that "I've been watching this very closely every hour for a few weeks." On January 26
24 and thereafter, Ralls and RedOrbit claimed that the click-surge resulted from various supposedly
25 legitimate factors (*see* ¶¶ 53-56, *infra*). On information and belief, Ralls and RedOrbit knew the
26 click-surge could not be attributed to those factors, and the explanations were a deliberate attempt
27 to mislead Microsoft's investigators. On February 6, Microsoft asked Ralls, "what specifically do
28 you think caused the dramatic increase in CTRs from January 20th onward?" Of all of the

1 explanations he came up with, Ralls never once mentioned that RedOrbit had started receiving the
2 Miva Media feed on exactly that day.

3 53. Instead, Ralls and RedOrbit claimed that the click-surge resulted from a better
4 match between the advertisements and the content of RedOrbit.com, a factor commonly referred
5 to as “ad relevance.” On January 26, 2009, Ralls stated, “[s]omething happened on your end, and
6 now the ads usually match the content on our site. As you can see, it makes a HUGE difference!”
7 In the same January 26, 2009 e-mail, Ralls stated, “[w]e carefully choose titles, descriptions and
8 keywords for video clips and news stories that contain very clear terms that match our overall site
9 content, and we change those throughout the day and watch how that impacts the ads that you
10 run.” On February 4, 2009, Ralls stated, “We had very weak ad relevancy for a long time --
11 nothing but diet ads were displaying through our adCenter tags. . . . Ad relevancy started getting
12 much better towards the end of January, and when that happened I began rolling out adCenter
13 tags onto more of our pages.” On February 6, 2009, Ralls stated, “[a]s I mentioned before, I feel
14 that greatly improved ad relevancy and removing most of the fat diet ads are the main reason for
15 this increase.”

16 54. On information and belief, Ralls and RedOrbit intended Microsoft to believe
17 that users were simply more interested in the advertisements being shown, and therefore were
18 clicking on them at a higher rate. However, conversions (*see* ¶ 10, *supra*) fell during the period
19 of the click surge, (*see* ¶ 35, *supra*) which implies that exactly the opposite occurred.

20 55. Second, Ralls and RedOrbit attempted to attribute the click-surge to the
21 addition of more “advertising tags” to RedOrbit.com. Advertising tags are small pieces of code
22 that, when processed by the browser of an end-user, cause the end-user’s browser to download an
23 advertisement to be placed in the webpage that the end-user is viewing. On January 26, 2009,
24 Ralls stated, “[w]e have also started adding your tags to more of our pages.” On February 4,
25 2009, Ralls stated, “[a]d relevancy started getting much better towards the end of January, and
26 when that happened I began rolling out adCenter tags onto more of our pages.” However,
27 evidence shows that Ralls and RedOrbit had not added more adCenter tags until on or around
28 January 25, 2009, five days after the start of the click-surge. The additional tags played a

1 negligible role in the click-surge thereafter, which Ralls and RedOrbit would have been aware of,
2 since, as Ralls admitted, he had been “watching this very closely every hour for a few weeks.”

3 56. Third, Ralls and RedOrbit attempted to attribute the click surge to changes
4 made to a video player on RedOrbit.com that, they claimed, caused more users to see more
5 advertisements. On February 5, 2009, Ralls stated, “we added an update to our video player . . .”
6 On February 6, 2009, Ralls stated, “we changed from an auto video player to a user initiated
7 video player. That means our videos no longer started playing automatically when you visit our
8 video page. It seems logical that this system allows visitors to scan the page before their attention
9 is immediately drawn to the video player.” However, the number of times end-users saw
10 advertisements on RedOrbit.com, i.e., impressions of advertisements, actually fell during the
11 period of the click surge (*see* ¶ 32, *supra*).

12 57. On February 10, with Microsoft pressing its investigation, Ralls cut the budget
13 for his campaigns with Miva Media from \$2400 per day to \$1200 per day, saying, “I need to slow
14 things down over the next 7-10 days.” On information and belief, Ralls took this step to reduce
15 the volume of traffic to RedOrbit.com that Ralls knew to be illicit.

16 58. On information and belief, in addition to attempting to lead Microsoft to
17 believe that the click-surge had legitimate origins, Ralls and RedOrbit purposefully took other
18 steps to hinder Microsoft’s investigation by denying Microsoft access to its weblogs. Weblogs
19 are detailed records of activity on a website. RedOrbit’s weblogs would have allowed Microsoft
20 to confirm the accuracy of Ralls’ explanations for the click-surge.

21 59. On February 5, 2009, Microsoft requested RedOrbit’s “weblogs” for the time
22 period from January 18 to February 4, 2009. On February 5, 2009, Ralls responded to
23 Microsoft’s request for weblogs by asking, “[e]xactly what other data would you like to see?” On
24 February 6, 2009, Microsoft again requested RedOrbit’s weblogs for the period from January 18
25 to February 4, 2009. On February 6, 2009, Ralls responded, “what do you mean by weblogs? I’m
26 confused by this request.”

27 60. On information and belief, Ralls and RedOrbit knew what weblogs were and
28 were not “confused by [the] request.” Later, Ralls admitted that RedOrbit’s policy was, in fact, to

1 destroy their weblogs after three days.

2 61. On February 9, 2009, Microsoft provided Ralls and RedOrbit with a detailed
3 explanation as to what weblogs were, and again requested RedOrbit's weblogs. On February 9,
4 2009 Ralls responded, stating, "[t]hat is a very serious request. I'm happy to give you whatever
5 you need to resolve this as soon as possible, but I need to protect my company. Are you OK with
6 signing an NDA?" The parties negotiated a non-disclosure agreement (the "NDA") and signed it
7 on or around June 10-11, 2009. Between February and June, 2009, Microsoft's investigators
8 studied the forensic data related to the click surge in an attempt to determine the degree of
9 RedOrbit and Ralls' culpability.

10 62. However, in June 2009, RedOrbit did not provide Microsoft the weblogs that it
11 had offered if Microsoft signed the NDA. Instead, RedOrbit only gave Microsoft access to
12 information provided through an analytics suite known as "Urchin." Microsoft reviewed the
13 information provided. On June 12, 2009, for the first time, RedOrbit informed Microsoft that it
14 only saved its weblogs for three days, after which time it deleted them.

15 63. Through its analysis of evidence gathered between January and June, 2009,
16 Microsoft determined that Ralls and RedOrbit shared culpability for the click-fraud operation in
17 January and February 2009.

18 **June, 2009-August, 2010**

19 64. Microsoft is informed and believes, and on that basis alleges that from June
20 2009 to August 2010, RedOrbit and Ralls have continued to buy malware-generated traffic. On
21 information and belief, RedOrbit and Ralls knew the traffic was generated by malware, and
22 purchased it with the intention of profiting by routing it to RedOrbit.com, where it would either
23 cause clicks on or impressions of advertisements.

24 65. On information and belief, during this time, RedOrbit has participated in
25 advertising programs through which RedOrbit is credited and the Advertiser is charged each time
26 its advertisement is shown, without a click being required. On information and belief, RedOrbit
27 and Ralls have worked with various intermediaries who distribute advertising, including
28 advertisements of Microsoft products and services.

1 66. On June 27, 2009, a computer infected with the malware known as
2 “Selectusers” was observed to open a full-screen pop-up browser window that traversed several
3 intermediate web sites before displaying a RedOrbit.com webpage. This webpage displayed an
4 advertisement for a show on MSN™, which is Microsoft’s online portal.

5 67. On April 3, 2010, a computer infected with the malware known as “Outerinfo”
6 was observed to open a pop-under browser window that directed traffic to a webpage hosted on
7 the net-mine.com domain, which redirected the traffic to a webpage on RedOrbit.com. This
8 webpage displayed a banner advertisement for Hotmail™, Microsoft’s web-based mail service, as
9 well as a video for Hotmail.

10 68. On July 21, 2010, a computer infected with the malware known as “Surfptp”
11 was observed to open a browser window, which through a complex series of operations,
12 eventually displayed a webpage on RedOrbit.com. This webpage displayed an advertisement for
13 Bing™, Microsoft’s online search service.

14 69. On August 1, 2010, a computer infected with the malware known as
15 “Trafficrevenue” was observed to open a browser window, which through a complex series of
16 operations, eventually displayed a webpage on RedOrbit.com. This webpage displayed an
17 advertisement for Bing.

18 70. On information and belief, these instances were not isolated events, but a
19 continuation of an ongoing practice that RedOrbit and Ralls engaged in from at least 2005. On
20 information and belief, these observed incidents represent a tiny fraction of the incidents that
21 actually occurred during this time period.

22 **CLAIM I – COMPUTER FRAUD AND ABUSE ACT**

23 **Count 1: 18 U.S.C. §§ 1030(a)(4) and 1030(a)(5)(A)**

24 **Against Ralls, RedOrbit, and Doe Defendants**

25 71. Microsoft incorporates and realleges each and every allegation contained in
26 paragraphs 1 to 70 of this Complaint.

27 72. Between January 20 and February 4, 2009 Ralls and RedOrbit purchased
28 traffic that generated clicks on advertisements on RedOrbit.com. This traffic was generated by

1 Vertro and Doe Defendants through the use of malware or other fraudulent means. On
2 information and belief, Ralls, RedOrbit, and Doe Defendants knew of the fraudulent origin of the
3 traffic Ralls and RedOrbit were purchasing. In spite of this knowledge, Ralls, RedOrbit, and Doe
4 Defendants persisted in attempting to profit by, *inter alia*, using the fraudulent traffic to generate
5 clicks on advertisements placed on RedOrbit.com by Microsoft, and then demanding payment
6 from Microsoft for the fraudulent clicks on April 14 and May 21, 2009.

7 73. On information and belief, Ralls, RedOrbit, and Doe Defendants accessed and
8 used adCenter's computers to manage the RedOrbit account. On information and belief, their
9 purpose in doing so was to further the click-fraud operation. Ralls, RedOrbit, and Doe
10 Defendants used the adCenter computers without authorization or in excess of authorized access
11 to those computers.

12 74. The fraudulent clicks caused the transmission of fraudulent data to Microsoft's
13 adCenter computers, thereby impairing the integrity and availability of data, the systems that rely
14 on that data, and the information related to that data. On information and belief, Ralls, RedOrbit,
15 and Doe Defendants knew the fraudulent data would be transmitted to Microsoft's adCenter
16 computers, knew it would cause damage to those computers, intended it to cause damage to those
17 computers, and intended for it to result in payment to RedOrbit for the fraudulent clicks. The
18 transmission of fraudulent data to adCenter computers was done without authorization or in
19 excess of authorized access to those computers.

20 75. These acts furthered the intended fraud by improperly inducing Microsoft to
21 credit the account of RedOrbit in an amount in excess of \$252,000, which was the object of the
22 fraud, while simultaneously debiting the Advertisers' accounts. On information and belief, Ralls,
23 RedOrbit, and Doe Defendants acted knowingly and with intent to defraud. The acts of Ralls,
24 RedOrbit, and Doe Defendants violated 18 U.S.C. §1030(a)(4) and 18 U.S.C. § 1030(a)(5)(A).

25 76. The Defendants caused loss in excess of \$5000 to Microsoft in an amount to be
26 proven at trial in that adCenter operations were disrupted; the integrity of the data used by
27 adCenter systems was impaired; Microsoft's reputation and the reputation of adCenter were
28 damaged; and Microsoft expended considerable resources to investigate and police the

1 Defendants' fraudulent acts, to conduct a damage assessment, to repair the damage that resulted
2 from those acts, and to conduct an accounting and refund the advertisers affected by the
3 fraudulently-generated clicks.

4 **Count 2: 18 U.S.C. § 1030(a)(5)(A)**

5 **Against Vertro and Doe Defendants**

6 77. Microsoft incorporates and realleges each and every allegation contained in
7 paragraphs 1 to 70 of this Complaint.

8 78. Between January 20 and February 4, 2009 Vertro purchased traffic from the
9 Doe Defendants and sold it to RedOrbit and Ralls. This traffic generated clicks on
10 advertisements on RedOrbit.com. This traffic was generated by Doe Defendants through the use
11 of malware or other fraudulent means. On information and belief, Vertro and Doe Defendants
12 knew of the fraudulent origin of the traffic that Vertro was purchasing and reselling to RedOrbit.
13 On information and belief, Vertro and Doe Defendants knew the traffic would generate fraudulent
14 clicks on advertisements on RedOrbit.com, and Vertro took deliberate steps to increase the click-
15 through rate on advertisements on RedOrbit.com.

16 79. The fraudulent clicks on advertisements on RedOrbit.com caused the
17 transmission of fraudulent data to Microsoft's adCenter computers, thereby impairing the
18 integrity and availability of data, the systems that rely on that data, and the information related to
19 that data. On information and belief, Vertro and Doe Defendants knew the fraudulent data would
20 be transmitted to Microsoft's adCenter computers, knew it would cause damage to those
21 computers, intended it to cause damage to those computers, and intended for it to result in
22 payment to RedOrbit for the fraudulent clicks. The transmission of fraudulent data to adCenter
23 computers was done without authorization or in excess of authorized access to those computers.

24 80. On information and belief, Vertro and Doe Defendants acted knowingly and
25 intentionally. The acts of Vertro and Doe Defendants violated 18 U.S.C. §1030(a)(5)(A).

26 81. The Defendants caused loss in excess of \$5000 to Microsoft in an amount to be
27 proven at trial in that adCenter operations were disrupted; the integrity of the data used by
28 adCenter systems was impaired; Microsoft's reputation and the reputation of adCenter were

1 damaged; and Microsoft expended considerable resources to investigate and police the
2 Defendants' fraudulent acts, to conduct a damage assessment, to repair the damage that resulted
3 from those acts, and to conduct an accounting and refund the advertisers affected by the
4 fraudulently-generated clicks.

5 **CLAIM II – BREACH OF CONTRACT**

6 **Against RedOrbit, Inc.**

7 82. Microsoft realleges and incorporates by this reference each and every
8 allegation set forth in paragraphs 1 through 63 above.

9 83. RedOrbit agreed to use the pre-release version of the Microsoft adCenter
10 Publisher online advertising service technology (the "Service"). By installing, accessing, and
11 otherwise using the Service, RedOrbit consented to the terms of the Agreement.

12 84. Under the terms of the Agreement, RedOrbit was contractually prohibited from
13 engaging in certain acts.

14 85. Microsoft performed all conditions, covenants, and promises required to be
15 performed by Microsoft in accordance with the terms and conditions of the Agreement, except
16 those that Microsoft was prevented or legally excused from performing and those to which its
17 performance was waived.

18 86. Between September 2008 and February 2009, RedOrbit purchased traffic that
19 generated impressions and/or clicks on advertisements on its website. The traffic RedOrbit
20 purchased was generated through the use of malware. On information and belief, RedOrbit knew
21 of the fraudulent origin of the traffic it was purchasing. It therefore breached the contract,
22 including by "directly or indirectly generat[ing] impressions or clicks on an [sic] Ads, or
23 authoriz[ing] or encourag[ing] others to do so, through [] automated, deceptive, fraudulent or
24 other invalid means."

25 87. The fraudulently generated clicks injured Microsoft in an amount to be proven
26 at trial in that adCenter operations were disrupted; the integrity of the data used by adCenter
27 systems was impaired; Microsoft's reputation and the reputation of adCenter were damaged; and
28 Microsoft expended considerable resources to investigate and police the Defendants' fraudulent

1 acts, to conduct a damage assessment, to repair the damage that resulted from those acts, and to
2 conduct an accounting and refund the advertisers affected by the fraudulently-generated clicks.

3 88. Microsoft has been injured by RedOrbit's breaches of the applicable terms and
4 conditions in an amount to be proven at trial.

5 **CLAIM III –TORTIOUS INTERFERENCE WITH EXISTING**

6 **CONTRACTUAL RELATIONS**

7 **Count 1, Under Washington Law**

8 **Against Ralls and Doe Defendants**

9 89. Microsoft realleges and incorporates by this reference each and every
10 allegation set forth in paragraphs 1 through 70 above.

11 90. During the period of Ralls and Doe Defendants' fraudulent acts, Microsoft was
12 a party to contracts with multiple Advertisers. Those contracts required the Advertisers to pay
13 Microsoft based on the number of valid clicks reported on advertisements placed on
14 RedOrbit.com.

15 91. On information and belief, Ralls and Doe Defendants were aware of those
16 contracts, and willfully and intentionally interfered with them by generating and transmitting to
17 Microsoft fraudulent click data, knowing that the data would cause Microsoft to charge the
18 Advertisers' accounts for the fraudulent clicks.

19 92. Ralls and Doe Defendants' interference with the contracts was the direct and
20 proximate cause of damage to Microsoft in an amount to be proven at trial. In particular, Ralls
21 and Doe Defendants' acts damaged Microsoft in that adCenter operations were disrupted; the
22 integrity of the data used by adCenter systems was impaired; Microsoft's reputation and the
23 reputation of adCenter were damaged; Microsoft expended considerable resources to investigate
24 and police the fraudulent acts of Ralls and Doe Defendants, to conduct a damage assessment, to
25 repair the damage that resulted from those acts, and to conduct an accounting and refund the
26 advertisers affected by the fraudulently-generated clicks; and Microsoft's business with the
27 Advertisers was harmed.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Count 2, Under Texas Law

Against RedOrbit

93. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 70 above.

94. During the period of RedOrbit’s fraudulent acts, Microsoft was a party to contracts with multiple Advertisers. Those contracts required the Advertisers to pay Microsoft based on the number of valid clicks reported on advertisements placed on RedOrbit.com.

95. On information and belief, RedOrbit was aware of those contracts, and willfully and intentionally interfered with them by fraudulently and maliciously generating and transmitting to Microsoft fraudulent click data, knowing that the data would cause Microsoft to charge the Advertisers’ accounts for the fraudulent clicks.

96. RedOrbit’s interference with the contracts was the direct and proximate cause of damage to Microsoft in an amount to be proven at trial. In particular, RedOrbit’s acts damaged Microsoft in that adCenter operations were disrupted; the integrity of the data used by adCenter systems was impaired; Microsoft’s reputation and the reputation of adCenter were damaged; Microsoft expended considerable resources to investigate and police RedOrbit’s fraudulent acts, to conduct a damage assessment, to repair the damage that resulted from those acts, and to conduct an accounting and refund the advertisers affected by the fraudulently-generated clicks; and Microsoft's business with the Advertisers was harmed.

CLAIM IV – TRESPASS TO CHATTELS

Count 1, Under Washington Law

Against Ralls and Doe Defendants

97. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 70 above.

98. On information and belief, Microsoft alleges that Ralls and Doe Defendants interfered with Microsoft’s use of adCenter by using its servers for improper purposes; by generating and communicating fraudulent data to it during the January 20-February 4, 2009 click-

1 surge; and by causing Microsoft to store and process the fraudulent data, to debit the accounts of
2 Advertisers for the fraudulent clicks, and to credit the account of RedOrbit.

3 99. As a result of the interference of Ralls and Doe Defendants with Microsoft's
4 use of adCenter, Microsoft was harmed in an amount to be proven at trial. In particular, adCenter
5 operations were disrupted; Microsoft was deprived of the use of its property; the integrity of the
6 data used by adCenter systems was impaired; Microsoft's reputation and the reputation of
7 adCenter were damaged; and Microsoft expended considerable resources to investigate and police
8 the fraudulent acts of Ralls and Doe Defendants, to conduct a damage assessment, to repair the
9 damage that resulted from those acts, and to conduct an accounting and refund the Advertisers
10 affected by the fraudulently-generated clicks.

11 **Count 2, under Texas Law**

12 **Against RedOrbit**

13 100. Microsoft realleges and incorporates by this reference each and every
14 allegation set forth in paragraphs 1 through 70 above.

15 101. On information and belief, Microsoft alleges that RedOrbit interfered with
16 Microsoft's use of adCenter by using its servers for improper purposes; and by fraudulently and
17 maliciously generating and communicating fraudulent data to it during the January 20-February 4,
18 2009 click-surge; and by causing Microsoft to store and process the fraudulent data, to debit the
19 accounts of Advertisers for the fraudulent clicks, and to credit the account of RedOrbit.

20 102. As a result of the interference of RedOrbit with Microsoft's use of adCenter,
21 Microsoft was harmed in an amount to be proven at trial. In particular, adCenter operations were
22 disrupted; the integrity of the data used by adCenter systems was impaired; Microsoft was
23 deprived of the use of its property; Microsoft's reputation and the reputation of adCenter were
24 damaged; and Microsoft expended considerable resources to investigate and police the fraudulent
25 acts of RedOrbit, to conduct a damage assessment, to repair the damage that resulted from those
26 acts, and to conduct an accounting and refund the advertisers affected by the fraudulently-
27 generated clicks.

1
2 **Count 3, under Washington Law**

3 **Against Vertro and Doe Defendants**

4 103. Microsoft realleges and incorporates by this reference each and every
5 allegation set forth in paragraphs 1 through 70 above.

6 104. On information and belief, Microsoft alleges that Vertro and Doe Defendants
7 interfered with Microsoft's use of adCenter by causing fraudulent data to be generated and
8 communicated to Microsoft during the January 20-February 4, 2009 click-surge; and by causing
9 Microsoft to store and process the fraudulent data, to debit the accounts of Advertisers for the
10 fraudulent clicks, and to credit the account of RedOrbit.

11 105. As a result of the interference of Vertro and Doe Defendants with Microsoft's
12 use of adCenter, Microsoft was harmed in an amount to be proven at trial. In particular, adCenter
13 operations were disrupted; Microsoft was deprived of the use of its property; the integrity of the
14 data used by adCenter systems was impaired; Microsoft's reputation and the reputation of
15 adCenter were damaged; and Microsoft expended considerable resources to investigate and police
16 the fraudulent acts of Vertro and Doe Defendants, to conduct a damage assessment, to repair the
17 damage that resulted from those acts, and to conduct an accounting and refund the Advertisers
18 affected by the fraudulently-generated clicks.

19
20 **CLAIM V -- WASHINGTON CONSUMER PROTECTION ACT**

21 (Wash. Rev. Code §§ 19.86.020 *et seq.*)

22 **Count 1**

23 **Against Ralls and Doe Defendants for acts between September 2008 and August 2010**

24 106. Microsoft realleges and incorporates by this reference each and every
25 allegation set forth in paragraphs 1 through 70 above.

26 107. Beginning no later than December 2008 and continuing at least through August
27 2010, Ralls and Doe Defendants each engaged in one or more of a series of deceptive acts and
28 practices that included installing, or causing to be installed, malware on end-user computers; by

1 means of that malware “hijacking” the end-users’ browsers; forcing the hijacked browsers to
2 automatically navigate to RedOrbit.com webpages; and prominently displaying advertisements
3 for Microsoft’s products on those webpages. Ralls and Doe Defendants’ acts had the capacity to
4 deceive a substantial portion of the public, as, on information and belief, the malware was widely
5 disseminated using surreptitious techniques to infect vulnerable end-user computers.

6 108. On information and belief Ralls and Doe Defendants’ deceptive acts and
7 practices were intended to drive traffic to RedOrbit.com webpages displaying advertisements for
8 Microsoft’s products to increase clicks on those advertisements or impressions of those
9 advertisements, for which RedOrbit would have received payment from Microsoft or an
10 intermediary distributing Microsoft advertisements, and were thus actions taken in commerce.

11 109. These deceptive acts and practices were against the public interest. On
12 information and belief they were committed in the course of Ralls and Doe Defendants’ business;
13 and the acts are part of a generalized course of conduct extending from as early as 2005 to as
14 recently as August 2010; and there are no indications that Ralls or Doe Defendants are likely to
15 cease their actions without a court-ordered injunction.

16 110. Microsoft’s costs increased as a result of the malware-generated traffic causing
17 impressions and/or clicks on advertisements for its products. Microsoft’s goodwill and business
18 reputation were harmed by Ralls and Doe Defendants’ deceptive acts. Users’ browsers were
19 “hijacked” and forced to navigate to RedOrbit.com which prominently displayed Microsoft
20 advertisements. On information and belief, users associate the intrusive, disruptive, and annoying
21 experience of having their browsers hijacked with the Microsoft advertisements they are shown,
22 and this harms Microsoft’s goodwill and business reputation. In addition, on information and
23 belief, users attribute the disruptive experience, not to malware, but to supposed defects in
24 Microsoft products, further damaging Microsoft’s goodwill and business reputation.

25 111. The damage to Microsoft’s goodwill and business reputation are directly
26 caused by these deceptive acts.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Count 2

Against RedOrbit for acts between March 2009 and August 2010

112. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 70 above.

113. Beginning no later than June 2009 and continuing at least through August 2010, RedOrbit engaged in deceptive acts and practices by using malware-generated traffic to force end-users to view advertisements on RedOrbit.com. RedOrbit’s acts had the capacity to deceive a substantial portion of the public, as, on information and belief, the malware was widely disseminated using surreptitious techniques to infect vulnerable end-user computers.

114. On information and belief, RedOrbit’s deceptive acts and practices were intended to drive web traffic to RedOrbit.com webpages displaying Microsoft’s products to increase clicks on those advertisements or impressions of those advertisements for which RedOrbit would have received payment from Microsoft or an intermediary selling Microsoft advertisements, and were thus actions taken in commerce.

115. These deceptive acts and practices were against the public interest. On information and belief they were committed in the course of RedOrbit’s business; the acts are part of a generalized course of conduct extending from at least 2005 to as recently as August 2010; and there are no indications that RedOrbit is likely to cease its actions without a court-ordered injunction.

116. Microsoft’s costs increased as a result of the malware-generated traffic causing impressions and/or clicks on advertisements for its products. Microsoft’s goodwill and business reputation were harmed by RedOrbit’s deceptive acts. Users’ browsers were “hijacked” and forced to navigate to sites prominently displaying Microsoft advertisements. On information and belief users associate the intrusive, disruptive, and annoying experience of having their browsers hijacked with the Microsoft advertisements they are shown, and this harms Microsoft’s goodwill and business reputation. In addition, on information and belief users attribute the disruptive experience, not to malware, but to supposed defects in Microsoft products, further damaging

1 Microsoft's goodwill and business reputation.

2 117. The damage to Microsoft's goodwill and business reputation are directly
3 caused by RedOrbit's deceptive acts.

4 **CLAIM VI -- NEGLIGENCE**

5 **Against Vertro**

6 118. Microsoft realleges and incorporates by this reference each and every
7 allegation set forth in paragraphs 1 through 70 above.

8 119. Vertro's failure to ensure that the traffic it purchased and resold was
9 reasonably and tolerably free of malware generated clicks created the reasonably foreseeable risk
10 of monetary, operational, and reputational injury to online advertisers, and operators – like
11 Microsoft – of online advertising platforms. On information and belief, Vertro knew that click-
12 traffic sold to RedOrbit would be used to generate clicks on advertisements placed on
13 RedOrbit.com through Microsoft's adCenter platform.

14 120. Vertro therefore had a duty to exercise reasonable care to prevent the risk of
15 such injury from taking effect.

16 121. Vertro breached that duty by failing to exercise reasonable care to ensure that
17 the online traffic that it aggregated and resold was free of malware generated clicks.

18 122. Vertro's breach of that duty was the proximate cause of Microsoft's injury as
19 each fraudulent click that Vertro sold to RedOrbit that resulted in a click on an advertisement
20 placed by adCenter on RedOrbit.com caused fraudulent data to be sent to Microsoft's adCenter
21 servers, and forced Microsoft to reimburse advertisers for the fraudulent clicks.

22 123. Microsoft's damages are legally compensable. As a result of Vertro's breach
23 of duty, Microsoft was harmed in an amount to be proven at trial. In particular, adCenter
24 operations were disrupted; the integrity of the data used by adCenter systems was impaired;
25 Microsoft was deprived of the use of its property; Microsoft's reputation and the reputation of
26 adCenter were damaged; and Microsoft expended considerable resources to investigate and police
27 the negligent acts of Vertro, to conduct a damage assessment, to repair the damage that resulted
28 from those acts, and to conduct an accounting and refund the advertisers affected by the

1 fraudulently-generated clicks.

2 **PRAYER FOR RELIEF**

3 WHEREFORE, Microsoft prays for Judgment against the Defendants as follows:

4 1. For temporary and permanent injunctive relief against the Defendants, and that the
5 Defendants, their officers, agents, representatives, servants, employees, attorneys, successors and
6 assignees, and all others in active concert or participation with the Defendants, be enjoined and
7 restrained from continuing to violate the laws alleged herein; and be enjoined and restrained from
8 assisting, aiding, or abetting any other person or business entity in engaging in or performing any
9 of such;

10 2. For actual damages, in an amount to be proven at trial and treble damages as
11 appropriate;

12 3. For disgorgement of the Defendants' ill-gotten profits;

13 4. For attorneys' fees and costs;

14 5. For exemplary and punitive damages, and

15 6. For such other or additional relief as is just and proper.

16 **Jury Trial Demanded**

17 //

18 //

19 //

20 //

21 Dated: December 10, 2010.

22 Respectfully submitted,

23 ORRICK HERRINGTON & SUTCLIFFE LLP

24 By: /s/ Mark Parris

25 Mark Parris (Bar No. 13870)

26 mparris@orrick.com

27 Jeffrey Cox (Bar No. 37534)

28 jcox@orrick.com

701 Fifth Avenue, Suite 5600

Seattle, WA 98104

Telephone: (206) 839-4300

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I. Neel Chatterjee (Pro Hac Vice)
nchatterjee@orrick.com
Gabriel M. Ramsey (Pro Hac Vice)
gramsey@orrick.com
ORRICK HERRINGTON & SUTCLIFFE
LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

Attorneys for Plaintiff
MICROSOFT CORPORATION

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I certify that on December 10, 2010, the foregoing FIRST AMENDED COMPLAINT was electronically filed with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the service list below.

Parker C Folse, III: pfolse@susmangodfrey.com

Ian B Crosby: icrosby@susmangodfrey.com

s/ Heather Bond _____

EXHIBIT A

1 Microsoft alleges violations of the Computer Fraud and Abuse Act against all defendants.
2 Microsoft alleges violations of the Washington Consumer Protection Act against Eric C. Ralls
3 (“Ralls”) and Does 1-9 (the “Doe Defendants”). Microsoft brings claims in tort against Eric C.
4 Ralls (“Ralls”), Vertro, Inc. (“Vertro”), and the Doe Defendants under the laws of Washington.
5 Microsoft brings its claim for breach of contract against RedOrbit under Washington law, and its
6 claims in tort against RedOrbit under Texas law in accordance with an agreement between
7 Microsoft and RedOrbit, Inc. (“RedOrbit”).

8 **THE PARTIES**

9 1. Plaintiff Microsoft Corporation (“Microsoft”) is a Washington corporation
10 with its principal place of business in Redmond, Washington.

11 2. Defendant Eric C. Ralls is an individual believed to be a resident of Dallas,
12 Texas. On information and belief, Ralls was the president of RedOrbit, Inc. during the period of
13 time when the events giving rise to this complaint occurred.

14 3. Defendant RedOrbit, Inc., formerly known as Red Nova, Inc., is a Texas
15 corporation with its principal place of business in Tyler, Texas. RedOrbit publishes a website
16 named RedOrbit.com. Through RedOrbit.com, RedOrbit purports to provide a variety of
17 photographs, articles, and videos on science-related subjects.

18 4. Defendant Vertro, Inc., formerly known as Miva, Inc., formerly known as
19 FindWhat.com, is a Delaware Corporation with its principal place of business in New York, New
20 York. Vertro is an Internet company that owns and operates a line of software products. In June
21 2005, FindWhat.com changed its name to Miva, Inc. In June 2009, Miva, Inc changed its name
22 to Vertro, Inc. For purposes of clarity, this complaint will refer to the entity variously known as
23 FindWhat.com, Miva, Inc., or Vertro, Inc., as “Vertro.” On information and belief, until March
24 12, 2009, Vertro owned and operated business units known, *inter alia*, as SearchFeed and Miva
25 Media. While owned and operated by Vertro, Miva Media operated an online auction based pay-
26 per-click advertising network in North America and Europe.

27 5. Microsoft is unaware of the true name and capacity of the Doe Defendants and
28 therefore sues the Doe Defendants by that fictitious name. Microsoft will amend this complaint

THE PRESENT CONTROVERSY

Microsoft’s adCenter Platform

10. Microsoft owns and operates an online advertising platform called Microsoft adCenter™ (“adCenter”).¹ As part of its adCenter business, Microsoft contracts with various companies who wish to place advertisements on the Internet (hereinafter, “Advertisers”). Through the adCenter platform, Advertisers manage various aspects of their online advertising campaigns including budgeting, ad-placement, and analysis of results. Microsoft places the Advertisers’ advertisements on, among other places, a network of websites published by other entities or individuals (hereinafter, “Publishers”) that also participate in Microsoft’s advertising network program.

11. An individual viewing a Publisher’s website can click on an advertisement of interest. This action connects the individual to the Advertiser’s website where additional information about the product or service being advertised will be displayed. The goal of the Advertiser at this point is to encourage the individual to take additional actions such as requesting more information about or purchasing the Advertiser’s products or services. These additional actions taken on an Advertiser’s website are referred to as “conversions,” and may be tracked and monitored by Advertisers.

12. Following a click on an advertisement, the adCenter platform debits the account of the Advertiser that paid to place the advertisement, and credits the account of the Publisher of the website where the click occurred. In one common approach known as “pay-per-click,” Advertisers pay for each click on their advertisement, although on the adCenter platform advertisers are generally not charged for clicks of dubious quality or origin. Similarly, the Publisher’s account is credited for each click. A pay-per-click system allows Publishers to profit from the time, effort, and money invested in developing interesting and useful websites without requiring them to directly charge users for access to their websites. It benefits Advertisers by allowing them to place advertisements on websites likely to attract individuals interested in their

¹ Microsoft has renamed adCenter to “pubCenter,” but for purposes of clarity, this complaint refers to it as “adCenter” throughout.

1 products or services, and by connecting them with the individuals who have, by clicking on an
2 advertisement, shown an interest in their products or services.

3 13. Consistent with its Terms of Use, Microsoft's adCenter platform gathers and
4 maintains valuable data related to its advertising operations. Among other data, it maintains
5 account information for both Advertisers and Publishers, records the placement of
6 advertisements, and records contextual data related to each click. The data accumulated by
7 adCenter is a significant asset for Microsoft. It enables Microsoft to manage and develop its
8 adCenter business, and it enables the Advertisers and Publishers that participate in adCenter to
9 effectively manage their own advertising campaigns. Microsoft adCenter's nationwide and
10 global operations are supported by a Microsoft-owned network of computers that receive,
11 process, store, and communicate the data to different parts of, or participants in, the adCenter
12 network.

13 **Click-Fraud and Click-Laundering, Generally**

14 14. Pay-per-click systems are not immune to fraud. An unscrupulous Publisher
15 could, for example, use automated scripts, end-user computers infected with malware², or hired-
16 individuals to generate a large number of clicks on the advertisements placed on its website by
17 adCenter. Because such methods merely imitate the actions of a legitimate user of a web browser
18 clicking on an advertisement, but do so for the sole purpose of generating a charge per click
19 without having any interest in the product or service being advertised, the clicks are considered
20 fraudulent. This activity is termed "click-fraud." A Publisher engaged in click-fraud can reap ill-
21 gotten profits because, for each click recorded, the Publisher's account is credited at the expense
22 of the Advertiser whose advertisement was clicked.

23 15. For example, in one simple click-fraud scheme, a Publisher hires individuals to
24 simply visit the Publisher's website and repeatedly click on the advertisements placed there. In
25 the absence of fraud-detection measures, each time such a hired-individual clicks on an

26 ² The term "malware" as used in this Second Amended Complaint, refers to malicious software that is surreptitiously
27 installed on a user's computer without the user's knowledge or consent, and which operates to harm the user's
28 computer and/or other vulnerable networked computers, and/or interfere with the user's use of the computer.
"Spyware" is a type of malware that typically collects information about a user and the user's online activity without
the user's knowledge.

1 advertisement on the Publisher's site, the account of the Advertiser whose advertisement is
2 clicked can potentially be debited, and the account of the Publisher of the website where the click
3 occurred is credited. Such a click should be deemed fraudulent because the person behind the
4 click has no legitimate interest in the products or services advertised and is clicking on the
5 advertisement for the sole purpose of defrauding the Advertiser.

6 16. In other more sophisticated schemes, Publishers can generate a large number
7 of invalid clicks by channeling innocent end-users browsing online to websites the Publisher
8 controls and tricking them into clicking on online advertisements. A variety of techniques can be
9 used to channel users to a particular website. For example, a Publisher can purchase Internet
10 traffic from individuals or entities that have installed malware on end-users' computers connected
11 to the Internet. The malware can then be used to route the end-users to websites controlled by the
12 paying Publisher. Once on the website controlled by the Publisher, the end-user can be tricked
13 into clicking on advertisements. For example, links to advertisements can be hidden beneath
14 links to legitimate-looking topics. By clicking on the legitimate-looking link, the end-user causes
15 a click on the invisible advertisement to be recorded.

16 17. In other instances, infected end-user computers are recruited into networks of
17 infected computers known as "bot-nets" that can be remotely controlled for illegal purposes.
18 Such bot-nets can be used to generate clicks on advertisements on websites with no participation
19 from the end-user. Bot-nets that are specialized for this purpose are referred to as "click-bots."
20 Automated scripts can also be used to generate clicks on advertisements.

21 18. It is not uncommon for a Publisher to pay other entities or individuals to find
22 users and channel them to its website. There is nothing inherently fraudulent about this practice.
23 In the absence of fraud, it is commonly referred to as "buying traffic." However, these other
24 entities or individuals can also use all of the fraudulent means already alleged to generate invalid
25 traffic. In these cases, the traffic is commonly referred to as "bad traffic." The Publisher that
26 purchases bad traffic, regardless of whether it knows of the fraudulent origin of the traffic, can
27 ultimately profit from it by using it to drive up the number of clicks on the advertisements placed
28 on its website. At the end of the line is an Advertiser who is charged for the invalid clicks that

1 are generated through these schemes.

2 19. Click fraud schemes damage Microsoft as well as the Advertisers and
3 legitimate Publishers participating in Microsoft's adCenter advertising network or any advertising
4 network. Advertisers are wrongfully charged for fraudulent clicks, Microsoft must expend
5 resources in investigating and remedying the harms caused by the click fraud, adCenter
6 operations are disrupted, the reputations of Microsoft and adCenter are damaged, and Microsoft's
7 relations with the victimized Advertisers are harmed. Beyond this, the underground economy that
8 has grown up around the monetization of fraudulently generated clicks depends upon, and in
9 effect finances, the creation and propagation of malware that is used to infect and capture the
10 computers of end-users world-wide.

11 20. At its very essence, click-fraud is the theft of money from Advertisers by
12 fraudsters. This thievery is all the more insidious because it can be difficult to detect. Individuals
13 and entities bent on fraud have grown adept at hiding the improper origin of the invalid clicks
14 through technical measures meant to defeat the fraud-detection systems deployed, for example,
15 by adCenter. Microsoft refers to such attempts at hiding the improper origin of clicks as "click-
16 laundering," and it will refer to them as such in this complaint. Click-laundering techniques
17 include channeling unsuspecting end-users to websites where they can be tricked into triggering
18 clicks on advertisements, and using scripts or other methods to alter the information associated
19 with the clicks recorded, for example, by adCenter. Click-laundering techniques also include
20 using click-bots to generate clicks, but routing the click-bot traffic through various websites to
21 disguise its fraudulent origin. Over time, click-laundering operations have grown in scale and
22 sophistication and now constitute a major engine of click-fraud.

23 **RedOrbit and Ralls' History of Purchasing Fraudulently Generated Traffic.**

24 21. Microsoft is informed and believes, and on that basis alleges, that beginning no
25 later than 2005 and continuing each year thereafter up to and through August 2010, RedOrbit has
26 purchased traffic from vendors that generate it using malware and, potentially, other fraudulent
27 means. RedOrbit's history in this regard was unknown to Microsoft when it allowed RedOrbit to
28 join the adCenter beta program in September 2008.

1 22. In 2006, in *Elite Street, LLC v. Eric Ralls and Red Nova, Inc.*, No.
2 602496/2006 (N.Y. Sup. Ct., New York Cnty, 2006), Elite Street, Inc. (“Elite Street”) sued
3 RedOrbit (F/K/A Red Nova, Inc.) for, *inter alia*, breach of contract based on RedOrbit’s alleged
4 non-payment for advertising services. RedOrbit made the following admissions in its
5 counterclaims. That on or about August 25, 2005, it entered into a contract with Elite Street,
6 known as an “Insertion Order,” pursuant to which Elite Street agreed to provide advertising
7 services to RedOrbit. That it entered into a second and third insertion order with Elite Street in
8 November 2005. That, starting in December 2005, Internet users began to complain to RedOrbit
9 that RedOrbit’s website hijacked their browsers through the use of malware, and that RedOrbit’s
10 advertisements continually “popped-up” on their computers, interrupting their ability to use their
11 computers. That, despite these problems, RedOrbit made all payments under the first, second,
12 and third insertion orders. That, on or about January 11, 2006, it entered into a fourth insertion
13 order pursuant to which Elite Street agreed to provide advertising services to RedOrbit for
14 approximately six months. That, in February, March, April, and May 2006, RedOrbit received
15 additional complaints from Internet users that RedOrbit’s website hijacked their browser through
16 the use of malware, and that RedOrbit’s advertisements continually “popped-up” on their
17 computers interrupting their ability to use their computers. That, it continued to pay Elite Street
18 during this period.

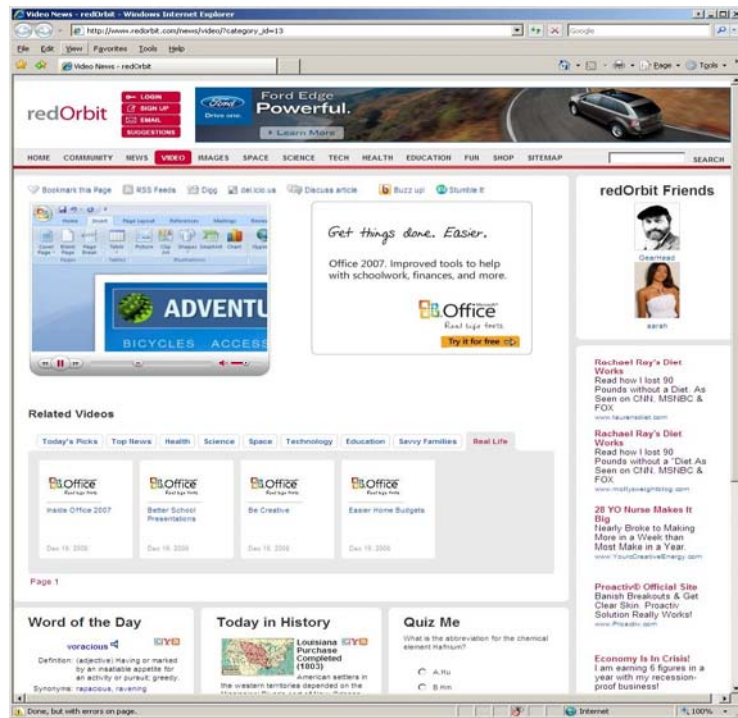
19 23. In 2007, in *Pennyweb, Inc. v. Argonaut Media, Inc., RedOrbit, Inc., and Does*
20 *1-10*, Case No. BC373664 (Cal. Super. Ct., Los Angeles Cnty, 2007), Pennyweb, Inc.
21 (“Pennyweb”) sued Argonaut Media, Inc., (“Argonaut”) and RedOrbit for, *inter alia*, breach of
22 contract. Pennyweb made the following accusations against RedOrbit: That, on or about June
23 21, 2006, Argonaut and RedOrbit entered into an “Online Media Placement Agreement” to create
24 and provide Internet advertising services for RedOrbit.com. That, on or about July 25, 2006,
25 Argonaut, after designing the display ad “creative” for RedOrbit, contracted with Pennyweb, an
26 Internet advertising network, to run the RedOrbit creative across multiple websites that comprised
27 Pennyweb’s network of affiliated websites. That, the type of creative designed by Argonaut for
28 RedOrbit to advertise the RedOrbit site was a “popped URL.” That, in essence, when an Internet

1 user would log onto one of the websites in Pennyweb’s network of affiliated websites,
2 Pennyweb’s ad-serving technology would deliver the RedOrbit “popped URL” to that user’s
3 personal computer in such a form that the user’s entire personal computer screen would be taken
4 over by the RedOrbit.com website. That, when the “popped URL” in the form of the
5 RedOrbit.com webpage, appeared on a user’s screen, that page would contain up to five
6 advertisements from five separate advertisers. That, in that scenario, RedOrbit would pay for one
7 impression, and in turn be paid by the up-to-five advertisers whose advertisements were displayed
8 on the RedOrbit site.

9 24. Microsoft is informed and believes, and on that basis alleges that RedOrbit did
10 receive malware-generated traffic during 2006, a practice that continued through 2007 and 2008,
11 including the following eleven observed incidents, which Microsoft believes to constitute a tiny
12 fraction of those that actually occurred: On February 17, 2006, a computer infected with the
13 malware known as “Deskwizz/Searchingbooth” was observed to send traffic to an intermediate
14 site that then displayed Redorbit.com. On April 22, 2006, a computer infected with the malware
15 known as “YourEnhancement” was observed to send traffic through various intermediary
16 websites to RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On April 28,
17 2006, a computer infected with the Deskwizz/Searchingbooth malware was observed to send
18 traffic to RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On April 29,
19 2006, a computer infected with the YourEnhancement malware was observed to send traffic to
20 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On May 21, 2006, a
21 computer infected with the malware known as “Look2me” was observed to direct traffic to
22 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On July 7, 2006, a
23 computer infected with the malware known as “Dollarrevenue” was observed to send traffic to
24 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On March 17, 2007, a
25 computer infected with the Deskwizz/Searchingbooth malware was observed to send traffic to
26 RedOrbit.com, causing RedOrbit.com to be displayed on the computer. On December 6, 14, 20,
27 and 24, 2008, malware-originated traffic, including traffic generated by the malware known as
28 “Interplusclick,” was observed to pass through an intermediate website known as

1 SearchFeed.com, which sent the traffic on to RedOrbit.com.

2 25. The image below shows the screen of a malware-infected system which, on
 3 December 20, 2008, was forced to visit the RedOrbit site on which multiple advertisements for
 4 Office 2007 were displayed. The image shown appeared entirely unrequested by the user, filled
 5 the entire computer screen, gave no indications of why RedOrbit.com had appeared, and gave no
 6 indication of how users could find and remove the malware that caused the RedOrbit.com to
 7 appear:



8
9
10
11
12
13
14
15
16
17
18
19
20
21
22 **Events Giving Rise to This Complaint**

23 **RedOrbit joins the adCenter beta program**

24 26. This action arises out of the Defendants' general abuse of the adCenter online
 25 service by generating clicks through fraudulent means and laundering those clicks to escape
 26 detection, and of Defendants' continued and ongoing use of malware-generated traffic to force
 27 end-users to view advertisements for Microsoft products.

28 27. RedOrbit joined the Microsoft adCenter Publisher beta program on or around

1 September 19, 2008. By agreeing to participate in the beta program, RedOrbit agreed to the
2 Microsoft adCenter Publisher Pre-Release License and Service Agreement (the “Agreement”),
3 attached hereto as Exhibit A, as all Publishers must. The Agreement prohibited, *inter alia*, the
4 following acts:

- 5 • “work[ing] around any technical limitations in the Service or introduce[ing] or us[ing]
6 any device, software, or routine that interferes or attempts to interfere with the
7 operation of the Service or otherwise attempt[ing] to access the Service in any manner
8 other than those authorized by Microsoft;
- 9 • access[ing] the Service from any websites or other locations, other than [the
10 Publisher’s] Websites that have been approved by Microsoft;
- 11 • “Cach[ing], stor[ing], copy[ing], distribut[ing], or redirect[ing] any Ads delivered by
12 the Service;
- 13 • directly or indirectly generat[ing] impressions or clicks on an [sic] Ads, or
14 authoriz[ing] or encourag[ing] others to do so, through any automated, deceptive,
15 fraudulent or other invalid means;
- 16 • Edit[ing], modify[ing], filter[ing], obscur[ing], or reorder[ing] any Ads (including
17 their associated links) supplied by the Service; or
- 18 • Fram[ing], minimiz[ing], remov[ing], redirect[ing], delay[ing], or otherwise
19 inhibit[ing] or modify[ing] the display of any web page accessed by the links included
20 with an Ad.” Exhibit A, ¶ 4.

21 28. The Agreement further gave Microsoft the right to withhold payment for clicks
22 that Microsoft deemed fraudulent, and to terminate the Publisher’s participation in adCenter at
23 any time. The Agreement further stated that

24 Washington state law governs the interpretation of this agreement and
25 applies to claims for breach of it, regardless of conflict of laws principles.

26 The laws of the state where you live govern all other claims, including
27 claims under state consumer protection laws, unfair competition laws, and
28 in tort. Exhibit A, ¶ 15.

RedOrbit and Ralls agree to buy traffic from Vertro

1
2 29. Between September, 2008, when RedOrbit joined the adCenter program, and
3 December 2008, adCenter received data from RedOrbit's primary web property, RedOrbit.com,
4 and recorded approximately 75 clicks considered "valid" per day on advertisements placed there.
5 During this time, unbeknownst to Microsoft, RedOrbit was buying traffic from SearchFeed, a
6 business unit of Vertro. The volume of traffic that Ralls purchased from SearchFeed was sizable.
7 By mid-January 2009, on information and belief, Ralls owed SearchFeed approximately \$180,000
8 for traffic purchased in the prior months.

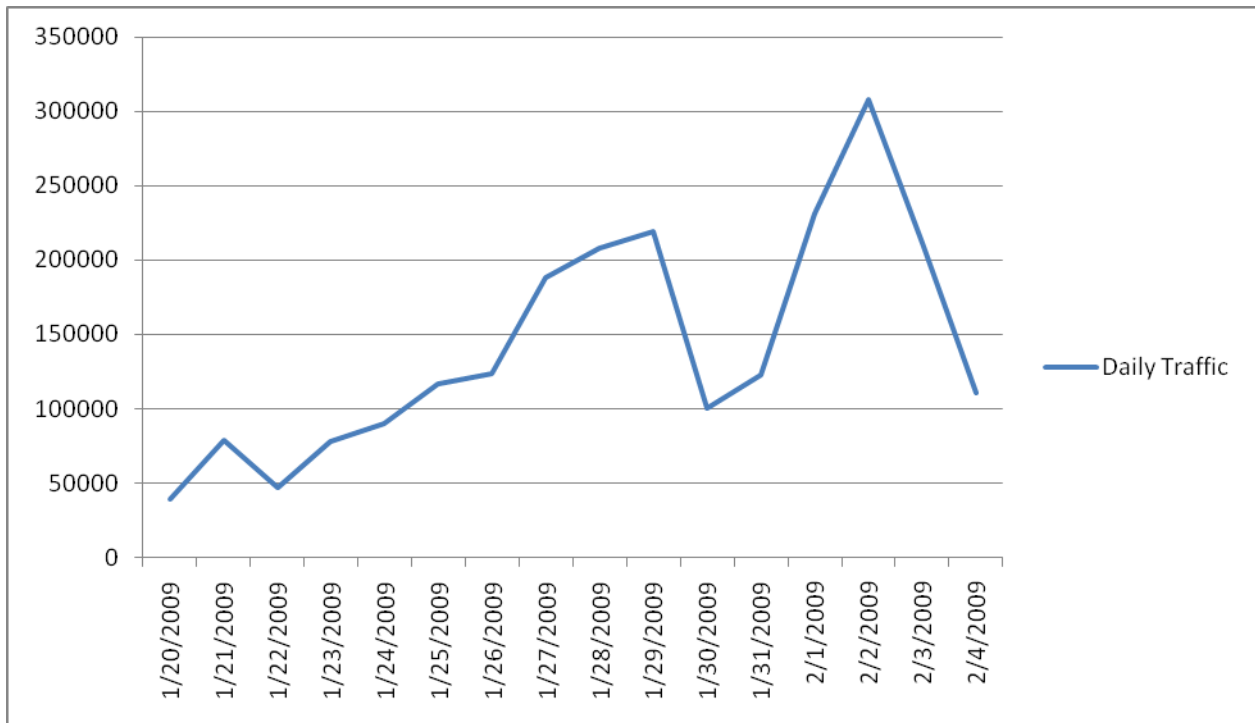
9 30. On January 13, 2009, Miva Media, another division of Vertro, contacted Ralls
10 and asked if he would be interested in a "business development opportunity," offering to sell
11 RedOrbit traffic from its own network of affiliated websites.

12 31. Ralls told Miva Media that one of his goals was to generate "high interaction
13 (ctr)," meaning, a high click through rate, with the ads on his site. Miva Media responded that it
14 had a number of different "feeds" starting at the price of one cent per visit that would be a good
15 fit for him. On January 14, Miva Media set up an account for RedOrbit in their system, and on
16 January 16, Ralls gave Vertro credit card details to fund the purchases of traffic. On information
17 and belief, Vertro's SearchFeed division stopped sending RedOrbit traffic on or about January 19.
18 On January 20, a Miva Media division feed to RedOrbit went live, and began directing traffic
19 generated on websites affiliated with the Miva Media network to RedOrbit. RedOrbit and Ralls
20 began testing the traffic generated by the Miva Media feed.

21 32. The monitoring obviously encouraged Ralls and RedOrbit, because by 7:53
22 A.M., E.S.T. on January 21, RedOrbit boosted its advertising budget on Miva to \$2500.
23 Evidently the traffic flooded in, because by 3:00 PM that day, Ralls asked Vertro if there was any
24 way to limit the hourly spend so that his entire budget would not be consumed in one or two
25 hours. At Vertro's suggestion, that evening, Ralls authorized Vertro to divide his daily campaign
26 into 24 separate sequential one hour campaigns, and funded each with a budget of \$50. Vertro
27 had the 24 campaigns ready to go live by January 22. On January 23, Ralls increased the budget
28 for each of the 24 sequential one-hour campaigns to \$100. Meanwhile, Vertro was "optimizing"

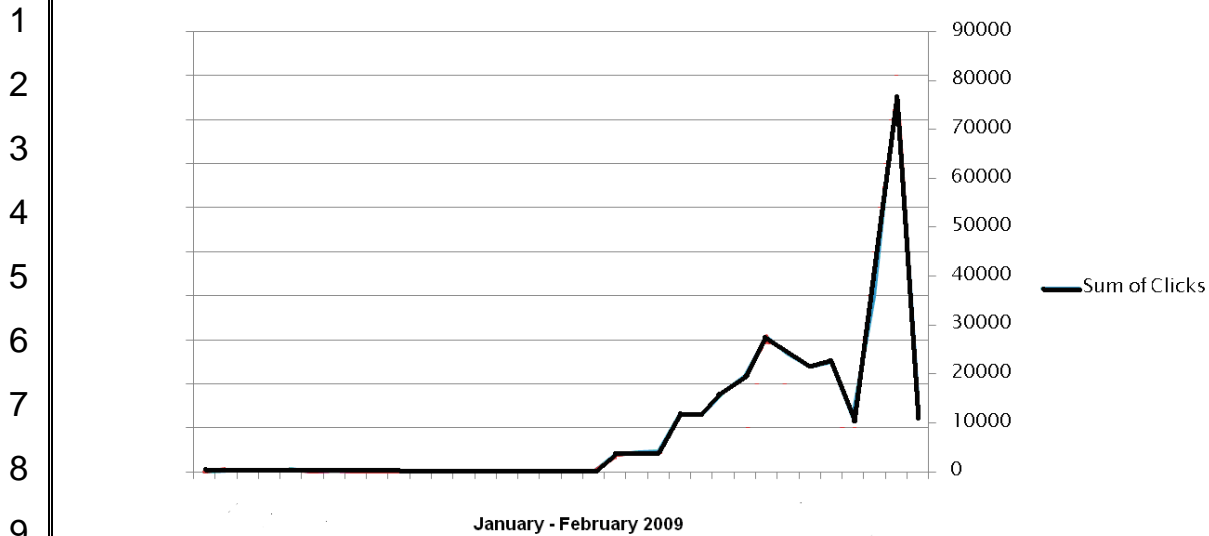
1 the feed to RedOrbit, and by January 24 had removed some of the sources from the feed that were
2 giving RedOrbit a less than 10% “ROI” or, presumably, “return on investment.”

3 33. A graph of the traffic from Vertro to RedOrbit.com between January 20 and
4 February 4 shows that it occurred in two spikes, with the first spike beginning on January 20 and
5 cresting on approximately January 28-29, and the second spike beginning on approximately
6 January 31 and cresting on approximately February 2.



20 Microsoft detects a massive surge of fraudulent clicks on RedOrbit.com

21 34. Starting on January 20, 2009, the same day the Miva Media feed to
22 RedOrbit.com went live, and continuing until February 4, 2009, adCenter recorded a substantial
23 surge in clicks on RedOrbit.com. These increased to an average of more than 10,000 clicks per
24 day. A graph of the clicks recorded from RedOrbit.com shows the peculiar surge, which occurred
25 in two spikes. The first spike began on January 20 and crested on approximately January 27, and
26 the second spike began on approximately January 31 and crested on approximately February 2,
27 closely matching the pattern of traffic from Vertro to RedOrbit.



35. Microsoft monitors the click-traffic on its adCenter network. It noticed the growth in clicks from RedOrbit.com and began investigating. Due to the sophisticated means believed to be employed by the Defendants to generate and launder the invalid clicks, the investigation into their activities was complex and time-consuming. By June 2009, Microsoft acquired sufficient evidence to cause it to believe that Ralls and RedOrbit were culpable for the January-February 2009 click-surge. Microsoft had already refunded advertisers for all clicks deemed fraudulent on RedOrbit's website during the time period at issue. The evidence, including evidence gathered through forensic analysis of Microsoft's own logs, showing that a script, click-bot or other automated process was being used to generate clicks, includes the following:

36. First, during the period of the click-surge, overall traffic to RedOrbit.com actually fell. Consistent with that, "impressions" also fell. Impressions occur when a user's browser shows an advertisement. However, at the same time traffic and impressions declined, the number of clicks on advertisements soared. The ratio measuring the number of clicks on advertisements to impressions of advertisements is referred to as the "click-through rate." The declining impressions and soaring clicks resulted in an abnormally high click-through rate.

37. Second, a very high percentage of the clicks lacked data normally associated with clicks generated when a person clicks on an advertisement from a browser. However, this

1 data is often missing from clicks generated by click-bots, scripts, or other automated processes
2 that simulate clicks on an advertisement.

3 38. Third, for the very high percentage of the clicks that lacked the normal data,
4 the average impression-to-click interval was abnormally short. The impression-to-click interval
5 measures the time delay between when a page with an advertisement is first visited and when the
6 advertisement is clicked on. A short interval is consistent with automated activity.

7 39. Fourth, conversions also declined during this period. *See* ¶ 11, *supra*
8 (explaining “conversions”). This is consistent with a declining percentage of actual users clicking
9 on advertisements.

10 40. Fifth, for a large number of clicks, Microsoft was able to determine the website
11 from which the traffic was referred to RedOrbit.com. For the majority of these clicks, the
12 referring websites appeared to have many commonalities among their designs, naming
13 conventions, content, and registration data. This suggesting that a small number of entities
14 designed and operated them. The websites appeared to lack any real content or serve any purpose
15 beyond routing traffic around the Internet. Some of these websites are linked through registration
16 and other data to some of the providers from which Vertro purchased traffic for resale to
17 RedOrbit.com between January 20 and February 4, 2009.

18 41. This evidence, among other facts, compelled Microsoft to the conclusion that
19 one or more of the Defendants had engaged in the fraudulent generation of fraudulent clicks and
20 had taken purposeful steps to launder the fraudulent clicks by hiding their improper origin.

21 42. The fraudulently generated clicks resulted in fraudulent data being sent to the
22 adCenter servers, corrupting the data on those servers. This data was used by adCenter to
23 determine which Advertiser should be charged for each click, and whether and how much
24 RedOrbit should be credited. RedOrbit and Ralls’ potential profits grew with each fraudulent
25 click.

26 43. On April 14, 2009, Ralls and RedOrbit sought payment from Microsoft for
27 clicks recorded in January and February 2009. On May 21, 2009, Ralls and RedOrbit again
28 sought payment from Microsoft, this time under threat of litigation, demanding that Microsoft pay

1 RedOrbit \$252,001.32 on or before the close of business on May 29, 2009. On information and
2 belief, by these acts, Ralls and RedOrbit intended to profit from the click-fraud operation.

3 **RedOrbit, Ralls, and Vertro knew of the fraudulent nature of the Vertro traffic**

4 44. On information and belief, Ralls and Vertro knew that some of the traffic from
5 Vertro was malware-generated. On January 23, Ralls informed Vertro that a percentage of
6 connections made by traffic from the Vertro network to RedOrbit.com stayed on RedOrbit.com
7 for less than one second. Microsoft is informed and believes and on that basis alleges that this is
8 a classic indication that the traffic is generated by a malware automated process, such as a click-
9 bot.

10 45. On information and belief, Vertro knew from the time the Miva Media feed to
11 RedOrbit went live that a significant portion of the traffic sold to RedOrbit between January 20
12 and February 3, 2009 came from websites featuring pornography or were generated in response to
13 searches on “adult” terms, and that Ralls and RedOrbit knew this fact no later than February 3.
14 Ralls detected that advertisements for RedOrbit.com were being placed by Miva Media on
15 pornography sites and on February 3 requested that he no longer be sent traffic from these
16 sources. However, on February 5, after Ralls saw how significantly his incoming traffic declined
17 without the traffic generated on pornography sites or in response to adult search terms, he
18 instructed Vertro to start sending him such traffic again.

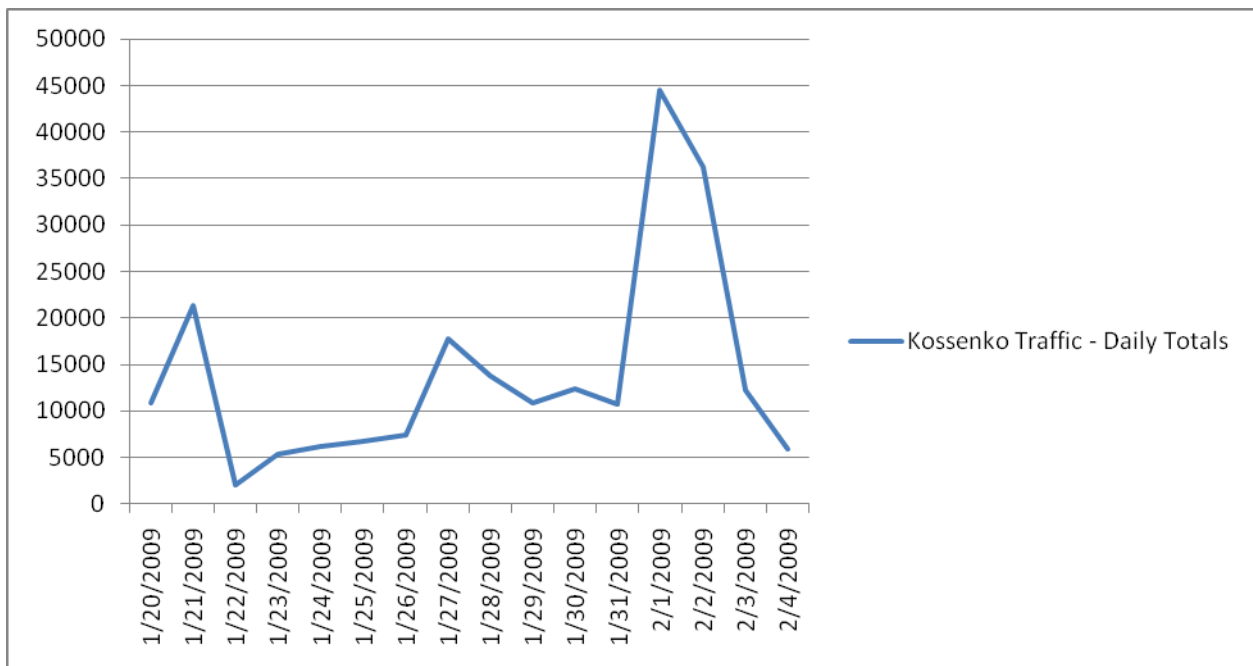
19 46. Microsoft is informed and believes and on that basis alleges that pornography
20 sites are often sources of fraudulent traffic. A high percentage of traffic originating from
21 pornography sites and directed to a purported science and technology site would have alerted both
22 Ralls and Vertro to the likely fraudulent origin of the traffic. The decline in traffic that Ralls
23 observed following his temporary decision to stop receiving traffic from pornography websites or
24 in response to searches on adult search terms would have alerted him to the fact that starting
25 January 20, a significant percentage of the traffic he had purchased and that he had used to
26 generate clicks on adCenter ads on RedOrbit had come from those sources.

27 47. Vertro knew that one of the largest contributors of traffic to the feed that was
28 being sold to RedOrbit was an individual named Saveli Kossenko (“Kossenko”). Overall,

1 Kossenko contributed 9.85% of the traffic sold to RedOrbit between January 20 and February 4.
 2 Vertro knew that Kossenko was reputed to use malware to generate traffic. In *In re Miva, Inc.*,
 3 *Securities Litigation*, 511 F. Supp. 2d 1242 (M.D. FL, 2007), Vertro, known at the time as
 4 FindWhat.com, was sued for securities fraud. In its March 2007 ruling denying a motion to
 5 dismiss, the court summarized some of the allegations related to Kossenko as follows:

6 During the class period, two of FindWhat's main revenue generating
 7 distribution partners (Saveli Kossenko and Dmitri I/n/u), who represented
 8 36% of FindWhat's revenues, were using illegal means to inflate revenues.
 9 This included the use of spyware, browser hijacking software, and “non-
 10 human traffic.” The use of such illicit methods of creating internet traffic,
 11 commonly referred to as “click-fraud,” . . . *Id.* at 1249.

12 48. The traffic from Kossenko that Vertro sold to RedOrbit shows that Kossenko’s
 13 contribution to the feed also occurred in three spikes, the second cresting on January 27, and the
 14 third cresting on February 2:



15
16
17
18
19
20
21
22
23
24
25
26
27 49. On information and belief, Ralls and RedOrbit determined, based on the
 28 soaring click-through rate on RedOrbit.com, that the traffic purchased from Vertro was fraudulent

1 in origin and was resulting in a massive number of fraudulent clicks on advertisements on
2 RedOrbit.com. On information and belief, Ralls and RedOrbit intended to profit from that traffic
3 by inducing Microsoft to charge Advertisers for the fraudulent clicks and to credit RedOrbit's
4 account for the clicks. On information and belief, Ralls and RedOrbit accessed and used
5 adCenter's computers to manage the RedOrbit account. On information and belief, their purpose
6 in doing so was to further the click-fraud operation.

7 50. On February 9, 2009, during the time when, on information and belief, Ralls
8 was still hoping to continue operating as a publisher on Microsoft's adCenter network, Ralls
9 requested that Vertro set up a new campaign related to health, saying, "please use this text," for
10 the campaign:

11 Mailscanner has detected a possible fraud attempt from www.redorbit.com claiming to be
12 www.redOrbit.com – science, Health, Technology . . . redOrbit.com is the premier
13 science, health, and technology news and information portal on the web. Learn something
14 new today."

15 51. On information and belief, the text requested by Ralls was meant to be used in
16 advertisements placed on Vertro's network of affiliated websites. On information and belief,
17 Vertro set the campaign up the same day without questioning the strange and misleading text of
18 the campaign.

19 **Ralls and RedOrbit Concealed Evidence Related to the Click-Surge**

20 52. On January 26, February 4, February 5, February 6, and February 9, 2009
21 Microsoft sent Ralls and RedOrbit e-mails informing them that the RedOrbit account was under
22 investigation and seeking information from them. In response to Microsoft's inquiries, Ralls
23 admitted that "I've been watching this very closely every hour for a few weeks." On January 26
24 and thereafter, Ralls and RedOrbit claimed that the click-surge resulted from various supposedly
25 legitimate factors (*see* ¶¶ 53-56, *infra*). On information and belief, Ralls and RedOrbit knew the
26 click-surge could not be attributed to those factors, and the explanations were a deliberate attempt
27 to mislead Microsoft's investigators. On February 6, Microsoft asked Ralls, "what specifically do
28 you think caused the dramatic increase in CTRs from January 20th onward?" Of all of the

1 explanations he came up with, Ralls never once mentioned that RedOrbit had started receiving the
2 Miva Media feed on exactly that day.

3 53. Instead, Ralls and RedOrbit claimed that the click-surge resulted from a better
4 match between the advertisements and the content of RedOrbit.com, a factor commonly referred
5 to as “ad relevance.” On January 26, 2009, Ralls stated, “[s]omething happened on your end, and
6 now the ads usually match the content on our site. As you can see, it makes a HUGE difference!”
7 In the same January 26, 2009 e-mail, Ralls stated, “[w]e carefully choose titles, descriptions and
8 keywords for video clips and news stories that contain very clear terms that match our overall site
9 content, and we change those throughout the day and watch how that impacts the ads that you
10 run.” On February 4, 2009, Ralls stated, “We had very weak ad relevancy for a long time --
11 nothing but diet ads were displaying through our adCenter tags. . . . Ad relevancy started getting
12 much better towards the end of January, and when that happened I began rolling out adCenter
13 tags onto more of our pages.” On February 6, 2009, Ralls stated, “[a]s I mentioned before, I feel
14 that greatly improved ad relevancy and removing most of the fat diet ads are the main reason for
15 this increase.”

16 54. On information and belief, Ralls and RedOrbit intended Microsoft to believe
17 that users were simply more interested in the advertisements being shown, and therefore were
18 clicking on them at a higher rate. However, conversions (*see* ¶ 10, *supra*) fell during the period
19 of the click surge, (*see* ¶ 35, *supra*) which implies that exactly the opposite occurred.

20 55. Second, Ralls and RedOrbit attempted to attribute the click-surge to the
21 addition of more “advertising tags” to RedOrbit.com. Advertising tags are small pieces of code
22 that, when processed by the browser of an end-user, cause the end-user’s browser to download an
23 advertisement to be placed in the webpage that the end-user is viewing. On January 26, 2009,
24 Ralls stated, “[w]e have also started adding your tags to more of our pages.” On February 4,
25 2009, Ralls stated, “[a]d relevancy started getting much better towards the end of January, and
26 when that happened I began rolling out adCenter tags onto more of our pages.” However,
27 evidence shows that Ralls and RedOrbit had not added more adCenter tags until on or around
28 January 25, 2009, five days after the start of the click-surge. The additional tags played a

1 negligible role in the click-surge thereafter, which Ralls and RedOrbit would have been aware of,
2 since, as Ralls admitted, he had been “watching this very closely every hour for a few weeks.”

3 56. Third, Ralls and RedOrbit attempted to attribute the click surge to changes
4 made to a video player on RedOrbit.com that, they claimed, caused more users to see more
5 advertisements. On February 5, 2009, Ralls stated, “we added an update to our video player . . .”
6 On February 6, 2009, Ralls stated, “we changed from an auto video player to a user initiated
7 video player. That means our videos no longer started playing automatically when you visit our
8 video page. It seems logical that this system allows visitors to scan the page before their attention
9 is immediately drawn to the video player.” However, the number of times end-users saw
10 advertisements on RedOrbit.com, i.e., impressions of advertisements, actually fell during the
11 period of the click surge (*see* ¶ 32, *supra*).

12 57. On February 10, with Microsoft pressing its investigation, Ralls cut the budget
13 for his campaigns with Miva Media from \$2400 per day to \$1200 per day, saying, “I need to slow
14 things down over the next 7-10 days.” On information and belief, Ralls took this step to reduce
15 the volume of traffic to RedOrbit.com that Ralls knew to be illicit.

16 58. On information and belief, in addition to attempting to lead Microsoft to
17 believe that the click-surge had legitimate origins, Ralls and RedOrbit purposefully took other
18 steps to hinder Microsoft’s investigation by denying Microsoft access to its weblogs. Weblogs
19 are detailed records of activity on a website. RedOrbit’s weblogs would have allowed Microsoft
20 to confirm the accuracy of Ralls’ explanations for the click-surge.

21 59. On February 5, 2009, Microsoft requested RedOrbit’s “weblogs” for the time
22 period from January 18 to February 4, 2009. On February 5, 2009, Ralls responded to
23 Microsoft’s request for weblogs by asking, “[e]xactly what other data would you like to see?” On
24 February 6, 2009, Microsoft again requested RedOrbit’s weblogs for the period from January 18
25 to February 4, 2009. On February 6, 2009, Ralls responded, “what do you mean by weblogs? I’m
26 confused by this request.”

27 60. On information and belief, Ralls and RedOrbit knew what weblogs were and
28 were not “confused by [the] request.” Later, Ralls admitted that RedOrbit’s policy was, in fact, to

1 destroy their weblogs after three days.

2 61. On February 9, 2009, Microsoft provided Ralls and RedOrbit with a detailed
3 explanation as to what weblogs were, and again requested RedOrbit's weblogs. On February 9,
4 2009 Ralls responded, stating, "[t]hat is a very serious request. I'm happy to give you whatever
5 you need to resolve this as soon as possible, but I need to protect my company. Are you OK with
6 signing an NDA?" The parties negotiated a non-disclosure agreement (the "NDA") and signed it
7 on or around June 10-11, 2009. Between February and June, 2009, Microsoft's investigators
8 studied the forensic data related to the click surge in an attempt to determine the degree of
9 RedOrbit and Ralls' culpability.

10 62. However, in June 2009, RedOrbit did not provide Microsoft the weblogs that it
11 had offered if Microsoft signed the NDA. Instead, RedOrbit only gave Microsoft access to
12 information provided through an analytics suite known as "Urchin." Microsoft reviewed the
13 information provided. On June 12, 2009, for the first time, RedOrbit informed Microsoft that it
14 only saved its weblogs for three days, after which time it deleted them.

15 63. Through its analysis of evidence gathered between January and June, 2009,
16 Microsoft determined that Ralls and RedOrbit shared culpability for the click-fraud operation in
17 January and February 2009.

18 **June, 2009-August, 2010**

19 64. Microsoft is informed and believes, and on that basis alleges that from June
20 2009 to August 2010, RedOrbit and Ralls have continued to buy malware-generated traffic. On
21 information and belief, RedOrbit and Ralls knew the traffic was generated by malware, and
22 purchased it with the intention of profiting by routing it to RedOrbit.com, where it would either
23 cause clicks on or impressions of advertisements.

24 65. On information and belief, during this time, RedOrbit has participated in
25 advertising programs through which RedOrbit is credited and the Advertiser is charged each time
26 its advertisement is shown, without a click being required. On information and belief, RedOrbit
27 and Ralls have worked with various intermediaries who distribute advertising, including
28 advertisements of Microsoft products and services.

1 66. On June 27, 2009, a computer infected with the malware known as
2 “Selectusers” was observed to open a full-screen pop-up browser window that traversed several
3 intermediate web sites before displaying a RedOrbit.com webpage. This webpage displayed an
4 advertisement for a show on MSN™, which is Microsoft’s online portal.

5 67. On April 3, 2010, a computer infected with the malware known as “Outerinfo”
6 was observed to open a pop-under browser window that directed traffic to a webpage hosted on
7 the net-mine.com domain, which redirected the traffic to a webpage on RedOrbit.com. This
8 webpage displayed a banner advertisement for Hotmail™, Microsoft’s web-based mail service, as
9 well as a video for Hotmail.

10 68. On July 21, 2010, a computer infected with the malware known as “Surfptp”
11 was observed to open a browser window, which through a complex series of operations,
12 eventually displayed a webpage on RedOrbit.com. This webpage displayed an advertisement for
13 Bing™, Microsoft’s online search service.

14 69. On August 1, 2010, a computer infected with the malware known as
15 “Trafficrevenue” was observed to open a browser window, which through a complex series of
16 operations, eventually displayed a webpage on RedOrbit.com. This webpage displayed an
17 advertisement for Bing.

18 70. On information and belief, these instances were not isolated events, but a
19 continuation of an ongoing practice that RedOrbit and Ralls engaged in from at least 2005. On
20 information and belief, these observed incidents represent a tiny fraction of the incidents that
21 actually occurred during this time period.

22 **CLAIM I – COMPUTER FRAUD AND ABUSE ACT**

23 **Count 1: 18 U.S.C. §§ 1030(a)(4) and 1030(a)(5)(A)**

24 **Against Ralls, RedOrbit, and Doe Defendants**

25 71. Microsoft incorporates and realleges each and every allegation contained in
26 paragraphs 1 to 70 of this Complaint.

27 72. Between January 20 and February 4, 2009 Ralls and RedOrbit purchased
28 traffic that generated clicks on advertisements on RedOrbit.com. This traffic was generated by

1 Vertro and Doe Defendants through the use of malware or other fraudulent means. On
2 information and belief, Ralls, RedOrbit, and Doe Defendants knew of the fraudulent origin of the
3 traffic Ralls and RedOrbit were purchasing. In spite of this knowledge, Ralls, RedOrbit, and Doe
4 Defendants persisted in attempting to profit by, *inter alia*, using the fraudulent traffic to generate
5 clicks on advertisements placed on RedOrbit.com by Microsoft, and then demanding payment
6 from Microsoft for the fraudulent clicks on April 14 and May 21, 2009.

7 73. On information and belief, Ralls, RedOrbit, and Doe Defendants accessed and
8 used adCenter's computers to manage the RedOrbit account. On information and belief, their
9 purpose in doing so was to further the click-fraud operation. Ralls, RedOrbit, and Doe
10 Defendants used the adCenter computers without authorization or in excess of authorized access
11 to those computers.

12 74. The fraudulent clicks caused the transmission of fraudulent data to Microsoft's
13 adCenter computers, thereby impairing the integrity and availability of data, the systems that rely
14 on that data, and the information related to that data. On information and belief, Ralls, RedOrbit,
15 and Doe Defendants knew the fraudulent data would be transmitted to Microsoft's adCenter
16 computers, knew it would cause damage to those computers, intended it to cause damage to those
17 computers, and intended for it to result in payment to RedOrbit for the fraudulent clicks. The
18 transmission of fraudulent data to adCenter computers was done without authorization or in
19 excess of authorized access to those computers.

20 75. These acts furthered the intended fraud by improperly inducing Microsoft to
21 credit the account of RedOrbit in an amount in excess of \$252,000, which was the object of the
22 fraud, while simultaneously debiting the Advertisers' accounts. On information and belief, Ralls,
23 RedOrbit, and Doe Defendants acted knowingly and with intent to defraud. The acts of Ralls,
24 RedOrbit, and Doe Defendants violated 18 U.S.C. §1030(a)(4) and 18 U.S.C. § 1030(a)(5)(A).

25 76. The Defendants caused loss in excess of \$5000 to Microsoft in an amount to be
26 proven at trial in that adCenter operations were disrupted; the integrity of the data used by
27 adCenter systems was impaired; Microsoft's reputation and the reputation of adCenter were
28 damaged; and Microsoft expended considerable resources to investigate and police the

1 Defendants' fraudulent acts, to conduct a damage assessment, to repair the damage that resulted
2 from those acts, and to conduct an accounting and refund the advertisers affected by the
3 fraudulently-generated clicks.

4 **Count 2: 18 U.S.C. § 1030(a)(5)(A)**

5 **Against Vertro and Doe Defendants**

6 77. Microsoft incorporates and realleges each and every allegation contained in
7 paragraphs 1 to 70 of this Complaint.

8 78. Between January 20 and February 4, 2009 Vertro purchased traffic from the
9 Doe Defendants and sold it to RedOrbit and Ralls. This traffic generated clicks on
10 advertisements on RedOrbit.com. This traffic was generated by Doe Defendants through the use
11 of malware or other fraudulent means. On information and belief, Vertro and Doe Defendants
12 knew of the fraudulent origin of the traffic that Vertro was purchasing and reselling to RedOrbit.
13 On information and belief, Vertro and Doe Defendants knew the traffic would generate fraudulent
14 clicks on advertisements on RedOrbit.com, and Vertro took deliberate steps to increase the click-
15 through rate on advertisements on RedOrbit.com.

16 79. The fraudulent clicks on advertisements on RedOrbit.com caused the
17 transmission of fraudulent data to Microsoft's adCenter computers, thereby impairing the
18 integrity and availability of data, the systems that rely on that data, and the information related to
19 that data. On information and belief, Vertro and Doe Defendants knew the fraudulent data would
20 be transmitted to Microsoft's adCenter computers, knew it would cause damage to those
21 computers, intended it to cause damage to those computers, and intended for it to result in
22 payment to RedOrbit for the fraudulent clicks. The transmission of fraudulent data to adCenter
23 computers was done without authorization or in excess of authorized access to those computers.

24 80. On information and belief, Vertro and Doe Defendants acted knowingly and
25 intentionally. The acts of Vertro and Doe Defendants violated 18 U.S.C. §1030(a)(5)(A).

26 81. The Defendants caused loss in excess of \$5000 to Microsoft in an amount to be
27 proven at trial in that adCenter operations were disrupted; the integrity of the data used by
28 adCenter systems was impaired; Microsoft's reputation and the reputation of adCenter were

1 damaged; and Microsoft expended considerable resources to investigate and police the
2 Defendants' fraudulent acts, to conduct a damage assessment, to repair the damage that resulted
3 from those acts, and to conduct an accounting and refund the advertisers affected by the
4 fraudulently-generated clicks.

5 **CLAIM II – BREACH OF CONTRACT**

6 **Against RedOrbit, Inc.**

7 82. Microsoft realleges and incorporates by this reference each and every
8 allegation set forth in paragraphs 1 through 63 above.

9 83. RedOrbit agreed to use the pre-release version of the Microsoft adCenter
10 Publisher online advertising service technology (the "Service"). By installing, accessing, and
11 otherwise using the Service, RedOrbit consented to the terms of the Agreement.

12 84. Under the terms of the Agreement, RedOrbit was contractually prohibited from
13 engaging in certain acts.

14 85. Microsoft performed all conditions, covenants, and promises required to be
15 performed by Microsoft in accordance with the terms and conditions of the Agreement, except
16 those that Microsoft was prevented or legally excused from performing and those to which its
17 performance was waived.

18 86. Between September 2008 and February 2009, RedOrbit purchased traffic that
19 generated impressions and/or clicks on advertisements on its website. The traffic RedOrbit
20 purchased was generated through the use of malware. On information and belief, RedOrbit knew
21 of the fraudulent origin of the traffic it was purchasing. It therefore breached the contract,
22 including by "directly or indirectly generat[ing] impressions or clicks on an [sic] Ads, or
23 authoriz[ing] or encourag[ing] others to do so, through [] automated, deceptive, fraudulent or
24 other invalid means."

25 87. The fraudulently generated clicks injured Microsoft in an amount to be proven
26 at trial in that adCenter operations were disrupted; the integrity of the data used by adCenter
27 systems was impaired; Microsoft's reputation and the reputation of adCenter were damaged; and
28 Microsoft expended considerable resources to investigate and police the Defendants' fraudulent

1 acts, to conduct a damage assessment, to repair the damage that resulted from those acts, and to
2 conduct an accounting and refund the advertisers affected by the fraudulently-generated clicks.

3 88. Microsoft has been injured by RedOrbit's breaches of the applicable terms and
4 conditions in an amount to be proven at trial.

5 **CLAIM III –TORTIOUS INTERFERENCE WITH EXISTING**

6 **CONTRACTUAL RELATIONS**

7 **Count 1, Under Washington Law**

8 **Against Ralls and Doe Defendants**

9 89. Microsoft realleges and incorporates by this reference each and every
10 allegation set forth in paragraphs 1 through 70 above.

11 90. During the period of Ralls and Doe Defendants' fraudulent acts, Microsoft was
12 a party to contracts with multiple Advertisers. Those contracts required the Advertisers to pay
13 Microsoft based on the number of valid clicks reported on advertisements placed on
14 RedOrbit.com.

15 91. On information and belief, Ralls and Doe Defendants were aware of those
16 contracts, and willfully and intentionally interfered with them by generating and transmitting to
17 Microsoft fraudulent click data, knowing that the data would cause Microsoft to charge the
18 Advertisers' accounts for the fraudulent clicks.

19 92. Ralls and Doe Defendants' interference with the contracts was the direct and
20 proximate cause of damage to Microsoft in an amount to be proven at trial. In particular, Ralls
21 and Doe Defendants' acts damaged Microsoft in that adCenter operations were disrupted; the
22 integrity of the data used by adCenter systems was impaired; Microsoft's reputation and the
23 reputation of adCenter were damaged; Microsoft expended considerable resources to investigate
24 and police the fraudulent acts of Ralls and Doe Defendants, to conduct a damage assessment, to
25 repair the damage that resulted from those acts, and to conduct an accounting and refund the
26 advertisers affected by the fraudulently-generated clicks; and Microsoft's business with the
27 Advertisers was harmed.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Count 2, Under Texas Law

Against RedOrbit

93. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 70 above.

94. During the period of RedOrbit’s fraudulent acts, Microsoft was a party to contracts with multiple Advertisers. Those contracts required the Advertisers to pay Microsoft based on the number of valid clicks reported on advertisements placed on RedOrbit.com.

95. On information and belief, RedOrbit was aware of those contracts, and willfully and intentionally interfered with them by fraudulently and maliciously generating and transmitting to Microsoft fraudulent click data, knowing that the data would cause Microsoft to charge the Advertisers’ accounts for the fraudulent clicks.

96. RedOrbit’s interference with the contracts was the direct and proximate cause of damage to Microsoft in an amount to be proven at trial. In particular, RedOrbit’s acts damaged Microsoft in that adCenter operations were disrupted; the integrity of the data used by adCenter systems was impaired; Microsoft’s reputation and the reputation of adCenter were damaged; Microsoft expended considerable resources to investigate and police RedOrbit’s fraudulent acts, to conduct a damage assessment, to repair the damage that resulted from those acts, and to conduct an accounting and refund the advertisers affected by the fraudulently-generated clicks; and Microsoft's business with the Advertisers was harmed.

CLAIM IV – TRESPASS TO CHATTELS

Count 1, Under Washington Law

Against Ralls and Doe Defendants

97. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 70 above.

98. On information and belief, Microsoft alleges that Ralls and Doe Defendants interfered with Microsoft’s use of adCenter by using its servers for improper purposes; by generating and communicating fraudulent data to it during the January 20-February 4, 2009 click-

1 surge; and by causing Microsoft to store and process the fraudulent data, to debit the accounts of
2 Advertisers for the fraudulent clicks, and to credit the account of RedOrbit.

3 99. As a result of the interference of Ralls and Doe Defendants with Microsoft's
4 use of adCenter, Microsoft was harmed in an amount to be proven at trial. In particular, adCenter
5 operations were disrupted; Microsoft was deprived of the use of its property; the integrity of the
6 data used by adCenter systems was impaired; Microsoft's reputation and the reputation of
7 adCenter were damaged; and Microsoft expended considerable resources to investigate and police
8 the fraudulent acts of Ralls and Doe Defendants, to conduct a damage assessment, to repair the
9 damage that resulted from those acts, and to conduct an accounting and refund the Advertisers
10 affected by the fraudulently-generated clicks.

11 **Count 2, under Texas Law**

12 **Against RedOrbit**

13 100. Microsoft realleges and incorporates by this reference each and every
14 allegation set forth in paragraphs 1 through 70 above.

15 101. On information and belief, Microsoft alleges that RedOrbit interfered with
16 Microsoft's use of adCenter by using its servers for improper purposes; and by fraudulently and
17 maliciously generating and communicating fraudulent data to it during the January 20-February 4,
18 2009 click-surge; and by causing Microsoft to store and process the fraudulent data, to debit the
19 accounts of Advertisers for the fraudulent clicks, and to credit the account of RedOrbit.

20 102. As a result of the interference of RedOrbit with Microsoft's use of adCenter,
21 Microsoft was harmed in an amount to be proven at trial. In particular, adCenter operations were
22 disrupted; the integrity of the data used by adCenter systems was impaired; Microsoft was
23 deprived of the use of its property; Microsoft's reputation and the reputation of adCenter were
24 damaged; and Microsoft expended considerable resources to investigate and police the fraudulent
25 acts of RedOrbit, to conduct a damage assessment, to repair the damage that resulted from those
26 acts, and to conduct an accounting and refund the advertisers affected by the fraudulently-
27 generated clicks.

1
2 **Count 3, under Washington Law**

3 **Against Vertro and Doe Defendants**

4 103. Microsoft realleges and incorporates by this reference each and every
5 allegation set forth in paragraphs 1 through 70 above.

6 104. On information and belief, Microsoft alleges that Vertro and Doe Defendants
7 interfered with Microsoft's use of adCenter by causing fraudulent data to be generated and
8 communicated to Microsoft during the January 20-February 4, 2009 click-surge; and by causing
9 Microsoft to store and process the fraudulent data, to debit the accounts of Advertisers for the
10 fraudulent clicks, and to credit the account of RedOrbit.

11 105. As a result of the interference of Vertro and Doe Defendants with Microsoft's
12 use of adCenter, Microsoft was harmed in an amount to be proven at trial. In particular, adCenter
13 operations were disrupted; Microsoft was deprived of the use of its property; the integrity of the
14 data used by adCenter systems was impaired; Microsoft's reputation and the reputation of
15 adCenter were damaged; and Microsoft expended considerable resources to investigate and police
16 the fraudulent acts of Vertro and Doe Defendants, to conduct a damage assessment, to repair the
17 damage that resulted from those acts, and to conduct an accounting and refund the Advertisers
18 affected by the fraudulently-generated clicks.

19
20 **CLAIM V -- WASHINGTON CONSUMER PROTECTION ACT**

21 (Wash. Rev. Code §§ 19.86.020 *et seq.*)

22 **Count 1**

23 **Against Ralls and Doe Defendants for acts between September 2008 and August 2010**

24 106. Microsoft realleges and incorporates by this reference each and every
25 allegation set forth in paragraphs 1 through 70 above.

26 107. Beginning no later than December 2008 and continuing at least through August
27 2010, Ralls and Doe Defendants each engaged in one or more of a series of deceptive acts and
28 practices that included installing, or causing to be installed, malware on end-user computers; by

1 means of that malware “hijacking” the end-users’ browsers; forcing the hijacked browsers to
2 automatically navigate to RedOrbit.com webpages; and prominently displaying advertisements
3 for Microsoft’s products on those webpages. Ralls and Doe Defendants’ acts had the capacity to
4 deceive a substantial portion of the public, as, on information and belief, the malware was widely
5 disseminated using surreptitious techniques to infect vulnerable end-user computers.

6 108. On information and belief Ralls and Doe Defendants’ deceptive acts and
7 practices were intended to drive traffic to RedOrbit.com webpages displaying advertisements for
8 Microsoft’s products to increase clicks on those advertisements or impressions of those
9 advertisements, for which RedOrbit would have received payment from Microsoft or an
10 intermediary distributing Microsoft advertisements, and were thus actions taken in commerce.

11 109. These deceptive acts and practices were against the public interest. On
12 information and belief they were committed in the course of Ralls and Doe Defendants’ business;
13 and the acts are part of a generalized course of conduct extending from as early as 2005 to as
14 recently as August 2010; and there are no indications that Ralls or Doe Defendants are likely to
15 cease their actions without a court-ordered injunction.

16 110. Microsoft’s costs increased as a result of the malware-generated traffic causing
17 impressions and/or clicks on advertisements for its products. Microsoft’s goodwill and business
18 reputation were harmed by Ralls and Doe Defendants’ deceptive acts. Users’ browsers were
19 “hijacked” and forced to navigate to RedOrbit.com which prominently displayed Microsoft
20 advertisements. On information and belief, users associate the intrusive, disruptive, and annoying
21 experience of having their browsers hijacked with the Microsoft advertisements they are shown,
22 and this harms Microsoft’s goodwill and business reputation. In addition, on information and
23 belief, users attribute the disruptive experience, not to malware, but to supposed defects in
24 Microsoft products, further damaging Microsoft’s goodwill and business reputation.

25 111. The damage to Microsoft’s goodwill and business reputation are directly
26 caused by these deceptive acts.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Count 2

Against RedOrbit for acts between March 2009 and August 2010

112. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 70 above.

113. Beginning no later than June 2009 and continuing at least through August 2010, RedOrbit engaged in deceptive acts and practices by using malware-generated traffic to force end-users to view advertisements on RedOrbit.com. RedOrbit’s acts had the capacity to deceive a substantial portion of the public, as, on information and belief, the malware was widely disseminated using surreptitious techniques to infect vulnerable end-user computers.

114. On information and belief, RedOrbit’s deceptive acts and practices were intended to drive web traffic to RedOrbit.com webpages displaying Microsoft’s products to increase clicks on those advertisements or impressions of those advertisements for which RedOrbit would have received payment from Microsoft or an intermediary selling Microsoft advertisements, and were thus actions taken in commerce.

115. These deceptive acts and practices were against the public interest. On information and belief they were committed in the course of RedOrbit’s business; the acts are part of a generalized course of conduct extending from at least 2005 to as recently as August 2010; and there are no indications that RedOrbit is likely to cease its actions without a court-ordered injunction.

116. Microsoft’s costs increased as a result of the malware-generated traffic causing impressions and/or clicks on advertisements for its products. Microsoft’s goodwill and business reputation were harmed by RedOrbit’s deceptive acts. Users’ browsers were “hijacked” and forced to navigate to sites prominently displaying Microsoft advertisements. On information and belief users associate the intrusive, disruptive, and annoying experience of having their browsers hijacked with the Microsoft advertisements they are shown, and this harms Microsoft’s goodwill and business reputation. In addition, on information and belief users attribute the disruptive experience, not to malware, but to supposed defects in Microsoft products, further damaging

1 Microsoft's goodwill and business reputation.

2 117. The damage to Microsoft's goodwill and business reputation are directly
3 caused by RedOrbit's deceptive acts.

4 **CLAIM VI -- NEGLIGENCE**

5 **Against Vertro**

6 118. Microsoft realleges and incorporates by this reference each and every
7 allegation set forth in paragraphs 1 through 70 above.

8 119. Vertro's failure to ensure that the traffic it purchased and resold was
9 reasonably and tolerably free of malware generated clicks created the reasonably foreseeable risk
10 of monetary, operational, and reputational injury to online advertisers, and operators – like
11 Microsoft – of online advertising platforms. On information and belief, Vertro knew that click-
12 traffic sold to RedOrbit would be used to generate clicks on advertisements placed on
13 RedOrbit.com through Microsoft's adCenter platform.

14 120. Vertro therefore had a duty to exercise reasonable care to prevent the risk of
15 such injury from taking effect.

16 121. Vertro breached that duty by failing to exercise reasonable care to ensure that
17 the online traffic that it aggregated and resold was free of malware generated clicks.

18 122. Vertro's breach of that duty was the proximate cause of Microsoft's injury as
19 each fraudulent click that Vertro sold to RedOrbit that resulted in a click on an advertisement
20 placed by adCenter on RedOrbit.com caused fraudulent data to be sent to Microsoft's adCenter
21 servers, and forced Microsoft to reimburse advertisers for the fraudulent clicks.

22 123. Microsoft's damages are legally compensable. As a result of Vertro's breach
23 of duty, Microsoft was harmed in an amount to be proven at trial. In particular, adCenter
24 operations were disrupted; the integrity of the data used by adCenter systems was impaired;
25 Microsoft was deprived of the use of its property; Microsoft's reputation and the reputation of
26 adCenter were damaged; and Microsoft expended considerable resources to investigate and police
27 the negligent acts of Vertro, to conduct a damage assessment, to repair the damage that resulted
28 from those acts, and to conduct an accounting and refund the advertisers affected by the

1 fraudulently-generated clicks.

2 **PRAYER FOR RELIEF**

3 WHEREFORE, Microsoft prays for Judgment against the Defendants as follows:

4 1. For temporary and permanent injunctive relief against the Defendants, and that the
5 Defendants, their officers, agents, representatives, servants, employees, attorneys, successors and
6 assignees, and all others in active concert or participation with the Defendants, be enjoined and
7 restrained from continuing to violate the laws alleged herein; and be enjoined and restrained from
8 assisting, aiding, or abetting any other person or business entity in engaging in or performing any
9 of such;

10 2. For actual damages, in an amount to be proven at trial and treble damages as
11 appropriate;

12 3. For disgorgement of the Defendants' ill-gotten profits;

13 4. For attorneys' fees and costs;

14 5. For exemplary and punitive damages, and

15 6. For such other or additional relief as is just and proper.

16 **Jury Trial Demanded**

17 //
18 //
19 //
20 //

21 Dated: December 10, 2010.

22 Respectfully submitted,

23 ORRICK HERRINGTON & SUTCLIFFE LLP

24 By: /s/ Mark Parris
25 Mark Parris (Bar No. 13870)
mparris@orrick.com
26 Jeffrey Cox (Bar No. 37534)
jcox@orrick.com
27 701 Fifth Avenue, Suite 5600
Seattle, WA 98104
28 Telephone: (206) 839-4300

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I. Neel Chatterjee (Pro Hac Vice)
nchatterjee@orrick.com
Gabriel M. Ramsey (Pro Hac Vice)
gramsey@orrick.com
ORRICK HERRINGTON & SUTCLIFFE
LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

Attorneys for Plaintiff
MICROSOFT CORPORATION

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I certify that on December 10, 2010, the foregoing FIRST AMENDED COMPLAINT was electronically filed with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the service list below.

Parker C Folse, III, pfolse@susmangodfrey.com

Ian B Crosby, icrosby@susmangodfrey.com

s/ Heather Bond _____

EXHIBIT A

Microsoft adCenter Publisher Pre-Release License and Service Agreement

This is an agreement between you and Microsoft Corporation (located at One Microsoft Way, Redmond, WA 98052-6399) regarding your use of the pre-release version of the Microsoft adCenter Publisher online advertising service technology and service and any associated documentation, software code or other materials made available by Microsoft (collectively referred to in this agreement as the "**Service**"). Through the Service you will receive advertisements ("**Ads**") for display on your websites and Microsoft will pay you based upon the performance of the Ads on your websites.

This agreement applies to any updates, supplements or support services for the Service, unless other terms accompany those items. If so, those other terms apply.

By installing, accessing or otherwise using the Service, you accept the terms of this agreement. If you do not agree to the terms of this agreement, do not install, access or use the Service.

If you comply with this agreement, you have the rights below.

1. **PARTICIPATION.** Your participation in the Service is subject to Microsoft's prior approval, your compliance with this agreement and Microsoft's published policies for the Service available at <http://www.adcenterpublisher.com>. To participate, you must be at least 18 years old and must set up an account at <http://beta.pubcenter.microsoft.com> by providing all of the required registration information. You must keep this account information up to date, accurate, and secure. You may not barter, trade, or otherwise exchange your account and you may not maintain more than one account. You must protect any passwords or other credentials associated with your account(s) for the Service, and take full responsibility for any use of the account(s) under your password.
2. **USE OF THE SERVICE.** Under the terms of this agreement, you may access and use the Service in accordance with Microsoft's technical requirements for the purpose of receiving Microsoft's advertising services and that you have registered to participate in this Service ("Your Websites"), subject to Microsoft's prior review and approval of Your Websites. As part of the Service, Microsoft may provide you with account access to online reporting systems to view and use a variety of online reports for Your Websites' use of the Service. You may use such reports solely for your internal business purposes.

If you receive any feedback, comments, or complaints about any Ads delivered by the Service, you agree to forward the same to Microsoft.

This agreement only gives you some rights to access and use the Service. Microsoft reserves all other rights. You may use the Service only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Service that allow you to use it only in certain ways. You may not rent, lease, sublicense, or lend the Service or any of its components.

3. **YOUR WEBSITES.** You must ensure that Your Websites that access the Service comply with Microsoft's then-current published editorial policies for the Service. Such policies are currently available [here](#). You must indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to Your Websites, other than claims caused by the

Service.

4. PROHIBITIONS. You may not

- work around any technical limitations in the Service or introduce or use any device, software, or routine that interferes or attempts to interfere with the operation of the Service or otherwise attempt to access the Service in any manner other than those authorized by Microsoft;
- access the Service from any websites or other locations, other than Your Websites that have been approved by Microsoft;
- Cache, store, copy, distribute, or redirect any Ads delivered by the Service;
- directly or indirectly generate impressions or clicks on an Ads, or authorize or encourage others to do so, through any automated, deceptive, fraudulent or other invalid means;
- Edit, modify, filter, obscure, or reorder any Ads (including their associated links) supplied by the Service; or
- Frame, minimize, remove, redirect, delay or otherwise inhibit or modify the display of any web page accessed by the links included with an Ad.

5. USER DATA. Nothing in this agreement or the Service provides for the collection or transfer of any personally identifiable information ("PII") of internet users between the parties. You must maintain a prominent online privacy policy for Your Websites. This privacy policy, at a minimum, must include: (a) a full, accurate and clear disclosure regarding the placement, use and reading of cookies and related technologies, and Your collection and use of data in relation to activity by users on the Your Websites; (b) Your use of Microsoft (and others, if applicable) for advertising services for the Your Websites; and (c) a disclosure that users may choose to not participate in Microsoft's (and others', if applicable) personalized advertising services, along with a link to a Microsoft-specified web address (and other web sites, if applicable) where the end user may "opt out" of such personalized advertising services.

6. CONFIDENTIALITY. The Service, including its user interface (including reporting interface), features, performance (e.g., click-through rates, eCPM, or other performance statistics provided to you by Microsoft) and documentation, is confidential and proprietary to Microsoft and its suppliers. For five years after the provision of the Service to you or its commercial release, whichever is first, you may not disclose confidential information to third parties. Your duty to protect confidential information survives this Agreement. You may disclose confidential information in response to a judicial or governmental order. You must first give written notice to Microsoft to allow it to seek a protective order or otherwise protect the information. Confidential information does not include information that

- becomes publicly known through no wrongful act;
- you received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
- you developed independently.

7. EXPORT RESTRICTIONS. The Service is subject to United States export laws and regulations. You must comply with all domestic and international export laws and

regulations that apply to the Service. These laws include restrictions on destinations, end users and end use. For additional information, see [here](#)

8. **PRE-RELEASE SERVICE.** This Service is a pre-release version. It may not work the way a final version of the Service will. Microsoft may change it, the participation requirements and criteria, and payment models for the final, commercial version. Microsoft also may not release a commercial version.
9. **SUPPORT.** Microsoft is not obligated to provide any technical or other support ("**Support Services**") for Service.
10. **FEEDBACK.** You may have the ability to give additional feedback about the Service to Microsoft. You grant to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also grant to third parties, without charge, any patent rights necessary for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that incorporates your feedback. You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because Microsoft includes your feedback in our software or documentation. These rights survive this agreement.
11. **PAYMENTS.** You will receive a payment based upon the number of valid clicks on Ads from the Service on Your Websites, as measured by Microsoft's systems. Clicks that Microsoft's systems register as coming from IP addresses owned or controlled by you or clicks associated with your violation of this agreement or any of the Program Policies are not valid clicks. Payments will be made based upon then-current payment schedules and are subject then-current minimum payment amounts, both of which are described [here](#). If your earned balance does not exceed the then-current minimum payment amount at the cutoff day for a scheduled payment, those payments will roll over to the next period. **If you receive a payment that was not due to you, we may reverse or seek return of the payment and you agree to cooperate with us in our efforts to do this.**

Microsoft makes no guarantee regarding the number of on Ads from the Service on Your Websites you may expect or the amount of any payments you may receive.

12. **TERM AND TERMINATION.** The term of this Agreement automatically expires on May 1, 2009, but both you and Microsoft reserve the right to terminate your participation in the Service at any time for any reason. Microsoft also reserves the right to discontinue offering the Service or to modify the Service at any time in its sole discretion. If you are dissatisfied with any aspect of the Service at any time, your sole and exclusive remedy is to cease using it. Notwithstanding anything contained in the agreement to the contrary, Microsoft may also, in its sole discretion, terminate or suspend access to the Service to you at any time, in which case this Agreement automatically terminates. Upon the expiration or any termination of this Agreement, you must cease using the Service. This Section and Sections 6, 10, and 14-19 survive termination of this agreement or any discontinuation of the Service. Within ninety (90) days after the end of the calendar month in which this Agreement is terminated, Microsoft will pay you any amounts due to you under Section 11, provided that such amounts are at least \$10.
13. **MODIFICATIONS; NOTICES.** If we change this agreement, then we will give you notice before the change is in force. If you do not agree to these changes, then you must cancel and stop using the Service before the changes are in force. If you do not stop using the

Service, then your use of the Service will continue under the changed agreement. Microsoft may give notices to you, at Microsoft's option, in writing or by electronic mail to any e-mail address provided by you to Microsoft.

14. ENTIRE AGREEMENT. This agreement is the entire agreement with respect to the Service.

15. APPLICABLE LAW. Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

16. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

17. CLAIM MUST BE FILED WITHIN ONE YEAR. Any claim related to this contract or the Service may not be brought unless brought within 1 year. The 1 year period begins on the date when the claim first could be filed. If it is not filed in time, then that claim is permanently barred. This applies to you and your successors. It also applies to us and our successors and assigns.

18. DISCLAIMER OF WARRANTY. The Service is supplied "as-is." You bear the risk of using it. Microsoft gives no express or implied warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this agreement cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

19. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. You can recover from Microsoft and its suppliers only direct damages up to an amount equal to the net amount paid by Microsoft to you under this agreement during the 3 month period immediately preceding the date of the claim. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.

This limitation applies to

- anything related to the Service, Script, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.