**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF DELAWARE**

| | |
|---|---|
| BERT GLASER, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>GOOGLE INC., a Delaware Corporation,<br><br>Defendant. | Civil Action No. _____<br><br>**CLASS ACTION COMPLAINT FOR:**<br><br>1. Violation of Federal Wiretap Act, 18 U.S.C. § 2511 AND<br><br>2. Violation of Stored Electronic Communication Act,18 U.S.C. § 2701; AND<br><br>3. Violation of Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030<br><br>**JURY DEMAND** |

Plaintiff Bert Glaser ("Plaintiff"), on behalf of himself and a class of all others similarly situated, by and through his undersigned attorneys, brings this action against Defendant Google Inc. ("Google" or "Defendant"), and in support thereof alleges as follows:

## NATURE OF THE ACTION

1. Plaintiff brings this action on behalf of himself and the entire class of similarly situated users of Apple's Safari web browser and Microsoft's Internet Explorer web browser whose default privacy settings were intentionally and surreptitiously circumvented and whose private internet communications were knowingly intercepted by Google without the user's knowledge or consent.

2. Safari and Internet Explorer are the only web browsers configured to block advertisers and other third parties from using "cookies" to track a user's web-browsing activities by default. However, Google intentionally circumvented the default privacy settings of these web browsers and tricked the browsers to allow the installation of tracking cookies by Google's third-party advertising service, DoubleClick.

3. Google's actions violated the Federal Wiretap Act, the Stored Electronic Communication Act, and the Federal Computer Fraud and Abuse Act. Through this action, Plaintiff seeks declaratory and injunctive relief to prevent further violations by Google and statutory damages and other relief on behalf of himself and the entire class as provided under these statutes.

## JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the action arises under federal statutes, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the "Wiretap Act"), the Stored Electronic Communication Act, 18 U.S.C. § 2701 ("SECA") and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"). Subject matter jurisdiction also exists pursuant to 28 U.S.C. § 1332(d) ("CAFA") because the citizenship of the parties is diverse, there are more than 100 class members, and the amount in controversy exceeds $5,000,000.

5. This Court has personal jurisdiction over Google because Google is incorporated under the laws of the State of Delaware.

6. Venue is proper in this District because Google conducts business in this District.

## THE PARTIES

7. Plaintiff Bert Glaser is an adult domiciled in the State of Maryland. Plaintiff owns an Apple iPhone that uses the Safari web browser and a desktop computer and laptop that use the Internet Explorer web browser. Plaintiff has never changed the default privacy settings for the web browsers on these devices. For at least the last year, Plaintiff has regularly used the web browsers on these devices to access various websites displaying Google advertising content, including the websites for *The New York Times* and *The Washington Post*.

8. Defendant Google is a Delaware corporation based in Mountain View, California. Google is an internet company that provides a broad array of desktop, mobile and online products and services, including web-based search tools and advertising services.

## FACTUAL BACKGROUND

### Safari and Internet Explorer Are Configured To Block Third-Party Tracking Cookies

9. Safari is a web browser developed by Apple. Safari is installed on every Mac computer, iPhone, iPod Touch, and iPad. Safari is the most common web browser among mobile phone and tablet users.

10. Internet Explorer is a web browser developed by Microsoft. Internet Explorer is installed on most desktop and laptop computers that use the Windows operating system. Internet Explorer is the most common web browser among desktop and laptop computer users.

11. Unlike other popular web browsers, including Google Chrome and Mozilla Firefox, both Safari and Internet Explorer are configured to block most third-party advertising cookies and other tracking cookies by default. A cookie is a small text file that a website places on a user's device in order to identify the user and gather information about the user's internet activities. A first-party cookie is placed by the website the user is visiting. First-party cookies are generally used to enhance the user's experience by saving the user's login information or preferences at that first-party website. A third-party cookie is placed by a different website from the one the user is visiting. Although third-party cookies may be used for other purposes, they are most commonly used for advertising-related tracking.

12. It is clear that the explicit purpose of third-party cookie blocking features is to prevent advertisers and other third parties from secretly monitoring a user's web-browsing activities. For instance, Apple's promotional materials expressly advertise Safari's default

cookie blocking feature as a benefit of using Safari, stating: "Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari only accepts cookies from the current domain."

13. Although Safari and Internet Explorer block most third-party tracking, they do allow third-party cookies to be installed in certain limited situations. For instance, Safari makes an exception for third-party websites that Safari users interact with in some way. Thus, Safari permits third-party cookies to be placed on a user's device if the user clicks an advertisement that a third-party website has displayed on the first-party website the user is visiting. Safari also allows cookies from third-party websites when a user submits a form to the third-party website.

14. Internet Explorer only permits third-party cookies to be installed if a website presents a "P3P Compact Policy Statement" that describes how the site will use the cookies and pledges to offer users the ability to opt out of having any personal information that might be associated with that cookie shared or used for certain purposes such as tracking.

15. The Platform for Privacy Preferences ("P3P") is a standard format for computer-readable privacy policies published by the World Wide Web Consortium ("W3C") in 2002. The standard includes a P3P full policy format and a P3P compact policy format. The compact policy format is designed to be a shorter version of a full P3P policy that encodes in a computer-readable format only the parts of a privacy policy that relate to cookies. Use of a compact policy is optional for websites that use P3P full policies. However, according to the P3P working group, "if a web site makes compact policy statements it MUST make these statements in good faith."

16. The compact policy is designed to be transmitted in an HTTP header that also contains an HTTP cookie. It takes the form: CP = "POLICY" where POLICY is a series of three-

and four-letter tokens associated with P3P policy elements as defined in the P3P 1.0 Specification. Valid compact policies must have at least five of these elements. For example, the following is a valid P3P compact policy: CP = "NOI NID ADMa OUR IND UNI COM NAV."

17. The P3P specification states, "If an unrecognized token appears in a compact policy, the compact policy has the same semantics as if that token was not present." This means that web browsers should ignore any tokens that appear in a P3P compact policy that are not defined in the P3P specification.

18. Microsoft introduced support for P3P in the Internet Explorer 6 web browser and included functionally identical implementations of P3P in its subsequent Internet Explorer 7, 8, and 9 web browsers. By default, Internet Explorer is set to the "Medium" privacy setting, which (1) blocks third-party cookies that do not have a compact privacy policy, (2) blocks third-party cookies that use personally identifiable information without the user's implicit consent, and (3) restricts first-party cookies that use personally identifiable information without implicit consent.

19. Internet Explorer checks for a P3P compact policy header whenever a website sends a cookie in an HTTP response. If it finds a third-party cookie that is not accompanied by a compact policy, it blocks that cookie. If it finds a first-party cookie that is not accompanied by a compact policy, it prevents that cookie from being transmitted in a third-party context. If it finds an accompanying compact policy, it evaluates that compact policy and blocks the cookie if the compact policy is found to be "unsatisfactory." Internet Explorer considers a cookie to be unsatisfactory if the corresponding compact policy indicates that the cookie is used to collect personally identifiable information and does not allow users a choice in its use. By blocking cookies on the basis of their P3P compact policies, Internet Explorer's default privacy settings allow users "to enjoy the benefits of cookies, while protecting themselves from unsatisfactory

cookies."

20. Internet Explorer treats the representations made in compact policies as truthful statements and makes no attempt to verify the accuracy of the information contained in a compact policy. Thus, if a website with an unsatisfactory privacy policy were to make an untruthful statement and misrepresent its policy as a satisfactory one, it could trick Internet Explorer into allowing its third-party cookie to be set when it would otherwise be blocked.

21. Websites can also trick Internet Explorer into allowing their third-party cookies to be set without making untruthful statements by simply leaving out any compact policy tokens that would lead Internet Explorer to classify the compact policy as unsatisfactory. In fact, an invalid compact policy that contains only a made-up word is classified as satisfactory by Internet Explorer.

**Google Primarily Generates Revenue From Advertising**

22. Although Google is perhaps best known for its search engine and first-party website, google.com, Google offers many other web-based products and services, including third-party advertising services that it provides through its subsidiary, DoubleClick.

23. Like other web advertisers, Google uses cookies to identify users and collect information about their internet usage. Google has a generic advertising cookie that enables DoubleClick to gather information about a user's activities across all of the websites that are part of Google's advertising network. This information includes a unique ID number assigned to the user's browser, IP address, which typically indicates the user's approximate geographic location, the web address of the particular web page the user visited, and the date and time when the user visited the web page. DoubleClick records and pools the information in order to determine the user's interests and place the user into segments that advertisers choose from when they select

the type of people they want to see their advertisements.

24. According to Google, users who do not want to be tracked can opt out of its advertising cookie. In addition, Google has denied that it makes any effort to circumvent tools that are designed to block third-party cookies.

25. The fact that user web-browsing information has real economic value cannot seriously be denied. Indeed, most of Google's profits are derived from advertising. In fact, Google's most recently filed Form 10-K expressly states that it "generate[s] revenue primarily by delivering relevant, cost-effective online advertising." In 2011, Google earned advertising revenues of approximately $36.5 billion. Google currently generates 96% of its revenue through its advertising products.

26. In February 2012, Google began soliciting participants for its "Screenwise Trends" market research panel, which promises to give users gift cards worth as much as $25 for every three months that they allow Google to track their web-browsing activities.

**Jonathan Mayer Reveals That Google Has Been Intentionally Circumventing Safari's Cookie Blocking Feature And Tracking The Internet Activities Of Safari Users**

27. On or about February 17, 2012, Jonathan Mayer, a graduate student at Stanford University and blogger for The Center for Internet and Society at Stanford Law School, posted a blog revealing that Google was intentionally circumventing Safari's cookie blocking feature in order to place third-party tracking cookies on Safari users' devices.

28. Specifically, Mayer reported that Google advertisements displayed on non-Google websites contained a code that would "surreptitiously submit a form in an invisible iframe and place trackable cookies in Safari." Mayer explained that, when Safari users visited a webpage containing Google advertising content, Google's server responded by sending an

invisible form that was then automatically submitted to Google. He further explained that, because Google made it appear as though Safari users were submitting a form to Google, Safari permitted Google to install cookies on their devices, which, in turn, allowed the Google advertising cookie to be installed by DoubleClick.

29. Mayer also reported that he confirmed that Google's advertising cookie was enabled after the Safari web browser was used to access the website for *The New York Times.*

### *The Wall Street Journal* Independently Verifies That Google Has Been Tracking The Internet Usage of Safari Users

30. The same day that Mayer reported his findings, *The Wall Street Journal* published an article indicating that its technical advisor, Ashkan Soltani, had independently confirmed Mayer's results.

31. Consistent with Mayer's findings, the article concluded that: "Google added coding to some of its ads that made Safari think that a person was submitting an invisible form to Google. Safari would then let Google install a cookie on the phone or computer." Noting that "Safari, the most widely used browser on mobile devices, is designed to block such tracking by default," the article agreed that Google had been "bypassing the privacy settings of millions of [Safari users]" and "tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked" by using a "special computer code that tricks Apple's Safari Web-browsing software into letting them monitor many users."

32. According to the article, Soltani surveyed the top 100 most popular websites and found that the Google code was embedded in advertisements displayed on numerous sites that are part of Google's advertising network, including the website for *The New York Times.* The article stated that there was no indication that these sites were aware of Google's code.

**Google Admits That It Bypassed Safari's Cookie Blocking Feature, But Unconvincingly Claims Any Tracking Of Safari Users Was Inadvertent**

33. Google responded to the article in *The Wall Street Journal* by admitting that it intentionally bypassed Safari's third-party cookie blocking feature, but claiming that it only did so to enable web socialization features and that the placement of the Google advertising cookie was inadvertent. Specifically, Google's Senior Vice President of Communications and Policy, Rachel Whetstone, released the following statement:

> The Journal mischaracterizes what happened and why. We used known Safari functionality to provide features that signed-in Google users had enabled. It's important to stress that these advertising cookies do not collect personal information.
>
> Unlike other major browsers, Apple's Safari browser blocks third-party cookies by default. However, Safari enables many web features for its users that rely on third parties and third-party cookies, such as "Like" buttons. Last year, we began using this functionality to enable features for signed-in Google users on Safari who had opted to see personalized ads and other content–such as the ability to "+1" things that interest them.
>
> To enable these features, we created a temporary communication link between Safari browsers and Google's servers, so that we could ascertain whether Safari users were also signed into Google, and had opted for this type of personalization. But we designed this so that the information passing between the user's Safari browser and Google's servers was anonymous–effectively creating a barrier between their personal information and the web content they browse.
>
> However, the Safari browser contained functionality that then enabled other Google advertising cookies to be set on the browser. We didn't anticipate that this would happen, and we have now started removing these advertising cookies from Safari browsers. It's important to stress that, just as on other browsers, these advertising cookies do not collect personal information.

34. On February 21, 2012, Jonathan Mayer posted another blog refuting Google's claims. Among other things, Mayer noted that he "never saw an ad with the +1 button" in his testing and that, to the contrary, "[t]he circumvention behaviors occurred in ordinary-looking ads." Mayer also pointed out that "Google's circumvention was not necessary to make the +1

button clickable." Finally, Mayer observed that "Google held an advantage over its advertising competitors that did not track Safari browsers," that this "advantage may have resulted in profit," and that "Google ha[d] not yet publicized an estimate of its income from tracking Safari browsers."

**Microsoft Discloses That Google Also Bypassed Internet Explorer's Privacy Settings**

35. After initially using the publicity surrounding Google's breach of Safari's cookie blocking feature as an opportunity to tout Internet Explorer's superior privacy protection, on or about February 20, 2012, Dean Hachamovitch, Microsoft's Corporate Vice President of Internet Explorer, posted a blog acknowledging that Google also circumvented Internet Explorer's privacy settings.

36. According to Hachamovitch's blog post, "Google [wa]s employing similar methods (to what it employed with Safari) to get around the default privacy protections in IE and track IE users with cookies." Hachamovitch explained that "IE blocks third-party cookies unless the site presents a P3P Compact Policy Statement indicating how the site will use the cookie and that the site's use does not include tracking the user. Google's P3P policy causes Internet Explorer to accept Google's cookies even though the policy does not state Google's intent." Hachamovitch further explained that "Google sends a P3P policy that fails to inform the browser about Google's use of cookies and user information. Google's P3P policy is actually a statement that it is not a P3P policy. It's intended for humans to read even though P3P policies are designed for browsers to 'read.' P3P-compliant browsers interpret Google's policy as indicating that the cookie will not be used for any tracking purpose or any purpose at all. By sending this text, Google bypasses the cookie protection and enables its third-party cookies to be allowed rather than blocked."

**Google Admits That It Intentionally Circumvented Internet Explorer's Privacy Settings**

37. In response to Microsoft's disclosure, Whetstone issued a statement admitting that Google intentionally circumvented Internet Explorer's privacy settings, but claiming that "it is impractical to comply with [P3P] while providing modern web functionality."

38. According to Whetstone's statement, Google had "been open about [its] approach" and "[t]oday the Microsoft policy is widely non-operational." Whetstone cited a September 10, 2010 technical report published by researchers at Carnegie Mellon University, titled "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens." This report describes a research study in which the authors collected compact policies from 33,139 websites and found errors in 11,176 compact policies on 4,696 domains, including 11 of the 50 most-visited websites. Importantly, Whetstone's statement omits the fact that the Carnegie Mellon study ultimately concluded that these websites were "misrepresenting their privacy practices, thus misleading users and rendering privacy protection tools ineffective."

39. Indeed, in response to the publicity surrounding Google's breach of the Safari cookie blocking feature, Dr. Lorrie Faith Cranor, one of the authors of the report, posted a blog stating: "The excuse everyone uses to justify this circumvention is that P3P is dead and IE breaks the cool things they want to do on their website, so therefore it is ok to circumvent browser privacy controls. There is a long painful history associated with P3P … and I will be the first to admit that P3P is on life support at best right now. But despite that, Microsoft is still using it as part of their default cookie settings that the vast majority of IE users depend on. So, if you don't like P3P, how about asking Microsoft to take P3P out of their browser? Or how about

going back to the W3C [] and asking them to declare it dead? I suspect nobody wants to do that because it might call into question the effectiveness of industry self-regulation on privacy. W3C is currently hard at work on a new privacy standard called Do Not Track (DNT) which the industry is currently rallying around. Once the spotlights are off and companies have to live with the standard they created and discover that it prevents them from doing what they want to do, will they declare it dead as well and feel justified in circumventing it too?"

**The Public is Outraged By Google's Conduct**

40. Following publication of the article in *The Wall Street Journal*, the Electronic Frontier Foundation ("EFF"), a non-profit organization that promotes digital privacy rights on behalf of consumers and the general public, released a statement explaining that Google exploited "a small hole in Safari's privacy protections" that "[u]nfortunately had the effect of completely undoing all of Safari's protections against doubleclick.net." EFF also noted that, while Google was actively circumventing Safari's cookie blocking feature, Google's website contained the following language affirmatively advising Safari users that Safari's default privacy settings would prevent Google from tracking their web-browsing activities: "While we don't yet have a Safari version of the Google advertising cookie opt-out plugin, Safari is set by default to block all third party cookies. If you have not changed those settings, this option effectively accomplished the same thing as setting the opt-out cookie."

41. In addition, Consumer Watchdog, a non-profit consumer advocacy organization, sent a letter to the Chairman of the Federal Trade Commission ("FTC") asking that the FTC take "immediate action" because Google had "violated people's online privacy choices and falsely advised them about how to make opt-out choices." Consumer Watchdog cited the language from Google's website advising Safari users that they could rely on Safari's default privacy settings to

avoid being tracked by Google's advertising cookie and complained that "the advice was false," "Google was lying," and Google "was in fact circumventing the privacy choice and setting DoubleClick tracking cookies." Consumer Watchdog also asserted that Google "[c]learly [] knows that it was wrong" because, after Google's conduct became public, "it changed its advice page" and "remov[ed] the specific references to Safari." In addition, Consumer Watchdog pointed out that Google's actions violated the terms of an existing Consent Decree with the FTC that prohibits Google from misrepresenting "the extent to which [it] maintains and protects the privacy and confidentiality" of user information, "including, but not limited to, misrepresentations related to: (1) [t]he purposes for which it collects and uses information, and (2) the extent to which consumers may exercise control over collection, use, or disclosure of covered information."

42. The FTC is currently investigating Google's breach of Safari's default privacy settings.

## CLASS ACTION ALLEGATIONS

43. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of a Class of all Safari and Internet Explorer users whose default privacy settings were intentionally and surreptitiously circumvented by Google in order to intercept the users' internet communications without their knowledge or consent. Excluded from the Class are the Court and any of the Court's family members, Defendant, and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest.

44. The members of the Class are so numerous that joinder of all members is impracticable.

45. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class include whether Defendant violated the same federal laws.

46. Plaintiff's claims are typical of the claims of other Class members, as all members of the Class were similarly affected by Defendant's wrongful conduct in violation of federal law as complained of herein.

47. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel that is competent and experienced in class action litigation. Plaintiff has no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members.

48. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

## COUNT I

## VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2511

49. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

50. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the willful interception of any wire, oral, or electronic communication.

51. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire,

oral or electronic communication is intercepted.

52. Defendant circumvented the default privacy setting on Plaintiff's Safari and Internet Explorer web browsers and allowed a tracking cookie to be placed on Plaintiff's mobile phone and computer devices.

53. Neither Plaintiff nor members of the Class consented to or were aware that Google was violating federal law and engaging in this activity.

54. The data that the Google knowingly intercepted are "communications" within the meaning of the Wiretap Act.

55. Google intentionally and willfully placed the tracking cookies on users' mobile phone and computer devices and willfully intercepted the electronic communications of such users.

56. Plaintiff is a person whose electronic communications were intercepted within the meaning of Section 2520.

57. Section 2520 provides for preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and disgorgement of any profits earned by Defendant as a result of the above-described violations.

## COUNT II

## VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT, 18 U.S.C. § 2701

58. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

59. The Stored Electronic Communications Act ("SECA") provides a cause of action against a person who intentionally accesses without authorization a facility through which an

electronic communication service is provide, or who intentionally exceeds an authorization to access that facility, and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in storage in such a system.

60. "Electronic Storage" is defined in the statute to be "any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof."

61. Defendant intentionally placed tracking cookies on users' mobile phone and computer devices that accessed their stored electronic communications without authorization, and thus violated SECA.

62. Plaintiff and other member of the Class were harmed by Defendant's violations, and are entitled to statutory, actual and compensatory damages, injunctive relief, punitive damages, and reasonable attorneys' fees.

## COUNT III

## VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030

63. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

64. Defendant intentionally accessed a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, and by obtaining information from such a protected computer.

65. Defendant knowingly caused the transmission of a program, information, code or command and as a result caused a loss to one or more persons during any one-year period of at least $5,000 in the aggregate.

66. Plaintiff has also suffered a violation of the right of privacy as a result of Defendant's knowing actions.

67. Defendant has thus violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

68. Plaintiff's phone is a "computer" within the meaning of the Act.

69. Defendant's unlawful access to Plaintiff's computers and communications have caused irreparable injury. Unless restrained and enjoined, Defendant may continue to commit such acts. If Plaintiff's remedies at law are not adequate to compensate for these inflicted and threatened injuries, Plaintiff and the Class are entitled to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff respectfully requests that this Court:

A. Determine that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

B. Award compensatory damages, including statutory damages where available, in favor of Plaintiff and the other members of the Class against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from installing software on cell phones that could track the users' information in violation of federal law;

D. Award Plaintiff and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

E. Grant Plaintiff such further relief as the Court deems appropriate.

## JURY TRIAL DEMAND

Plaintiff demands a trial by jury for all issues so triable.

Dated: May 29, 2012

Respectfully submitted,

**STEWARTS LAW US LLP**

By: */s/ David A. Straite*

David A. Straite (DE I.D. #5428)
1201 North Orange Street
Wilmington, DE 19801
Tel: (302) 298-1200
Fax: (302) 298-1222
*dstraite@stewartslaw.com*

**OF COUNSEL:**

**MURPHY P.A.**
William H. "Billy" Murphy, Jr.
Tonya Osborne Baña
One South Street – 23rd Floor
Baltimore, MD 21202
Tel: (410) 539-6500
Fax: (410) 539-6599
*billy.murphy@murphypa.com*
*tonya.bana@murphypa.com*