BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Alec M. Leslie (*pro hac vice* forthcoming)
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
aleslie@bursor.com

GUCOVSCHI ROZENSHTEYN, PLLC.
Adrian Gucovschi (*pro hac vice* forthcoming)
630 Fifth Avenue, Suite 2000
New York, NY 10111
Telephone: (212) 884-4230
Facsimile: (212) 884-4230
E-Mail: adrian@gr-firm.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EFREN RAMOS, individually and on behalf of all other persons similarly situated, Plaintiff, v. THE GAP, INC. Defendant.	Case No. CLASS ACTION **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Efren Ramos ("Plaintiff") brings this class action complaint on behalf of himself and all others similarly situated (the "Class Members") against The GAP, Inc., ("Defendant" or "GAP"). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations specifically pertaining to himself, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action lawsuit brought against Defendant GAP for aiding, agreeing with, employing, or otherwise enabling the wiretapping of electronic communications between Defendant and its clients via emails sent from Defendant's email domain: bananarepublicfactory@email.bananarepublicfacotry.com (the "Emails"). The wiretaps, which are embedded in the Emails, operate without the knowledge or consent of Defendant's email recipients. Defendant contracts with a third party, Bluecore, Inc. ("Bluecore"), to provide the software that runs on the Emails—through URL links embedded within the words and imagery of the Emails (the "Content")—and the corresponding web pages that those recipients are routed to after clicking on the Emails' Content owned by Defendant at https://bananarepublicfactory.gapfactory.com/ (the "Website), thus violating the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631.

2. The electronic communications of users of the Emails and Website are routed through the servers of and are used by Bluecore to, among other things, secretly observe and record the interactions of Defendant's customers when they open and/or click on the Content of the Emails and the landing pages of Defendant's Website in real-time. The nature of Bluecore's licensing agreement with Defendant is such that Defendant "aids, agrees with, employs, or conspires" to permit Bluecore to read, attempt to read, and/or use the communications of Plaintiff and the Website's users without their consent, thus violating the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631.

3. Plaintiff brings this action on behalf of all persons who received Defendant's Emails, and whose electronic communications with those Emails were intercepted or recorded by

Bluecore.

THE PARTIES

4. Plaintiff Efren Ramos is a California resident and citizen who resides in Alameda County, California. Mr. Ramos received and interacted with Defendant's Emails on multiple occasions from his computer while in California. One such instance was in or about March 2023. When Mr. Ramos opened the Emails, Bluecore intercepted, in real-time, the time, date, device type, geolocation (and other information attributed to Mr. Ramos's online activity) as well as his engagement with the Email's content—including his clicks on URL links embedded within the Emails' Content. Upon clicking on the Email's Content, Bluecore continued to intercept Mr. Ramos's communications throughout the web pages that he was directed to on Defendant's Website. Mr. Ramos was unaware at the time that his engagement with the Emails, the Website, and other electronic communications were being intercepted in real-time by Bluecore, nor did Mr. Ramos consent to the same.

5. Defendant The GAP, Inc., is a Delaware corporation with its principal place of business at Two Folsom Street San Francisco, CA 94105. Defendant develops, owns, and operates the email domain bananarepublicfactory@email.bananarepublicfacotry.com, as well as the Website https://bananarepublicfactory.gapfactory.com/, both of which Bluecore intercepts when Defendant's subscribers access the Emails and Website throughout California. Defendant sends an average of over 7 emails per week to its subscribers—twice the average amount of emails sent by other e-commerce companies.[1]

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005 ("CAFA"), because this case is a class action where the aggregate claims for all members of the proposed class are in excess of $5,000,000.00, exclusive of interests and costs, there are over 100 members of the putative class,

[1] https://www.mailcharts.com/companies/banana-republic-factory-email-marketing (last accessed August 30, 2023).

and Plaintiff, as well as most members of the proposed class, is a citizen of a state different from Defendant.

7. This Court has general jurisdiction over Defendant because Defendant maintains its principal place of business within this District.

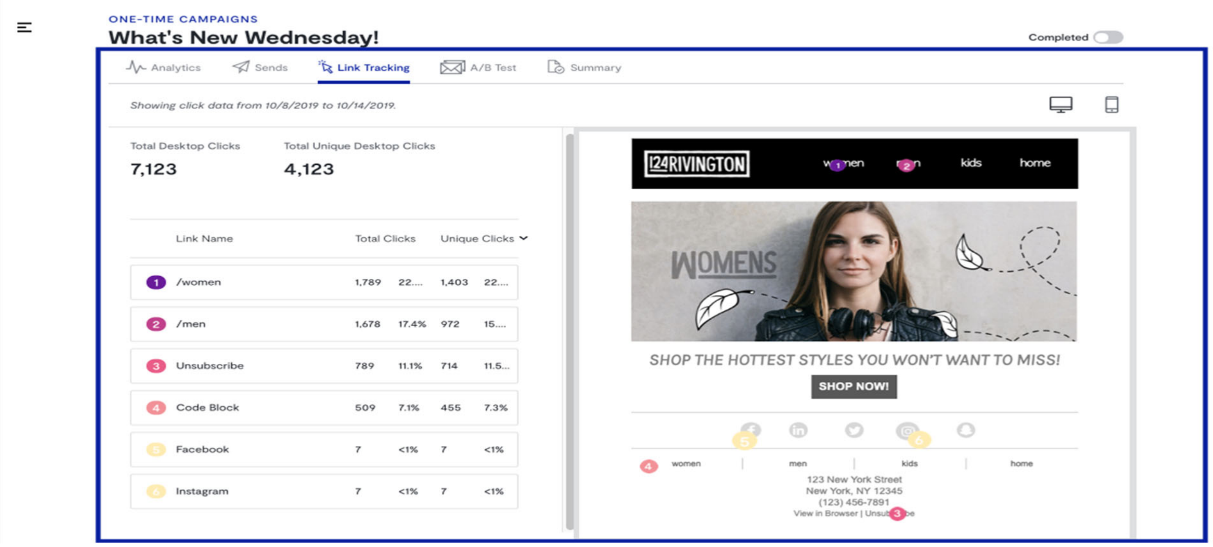
8. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because Defendant resides in this District.

FACTUAL BACKGROUND

I. Overview Of Bluecore's Wiretaps

9. Bluecore develops, owns, and licenses email tracking software for e-commerce businesses. Bluecore's software helps companies optimize their email marketing campaigns by tracking and analyzing their email performance, segmenting and personalizing emails to their audience, and automating their email workflows.

10. One of Bluecore's features is its email link tracking software. Bluecore's link tracking software "provides [clients] with a detailed view of how customers are engaging with [their] email templates…[to] improve email performance going forward."[2]



What's New Wednesday!

Showing click data from 10/8/2019 to 10/14/2019.

Total Desktop Clicks 7,123

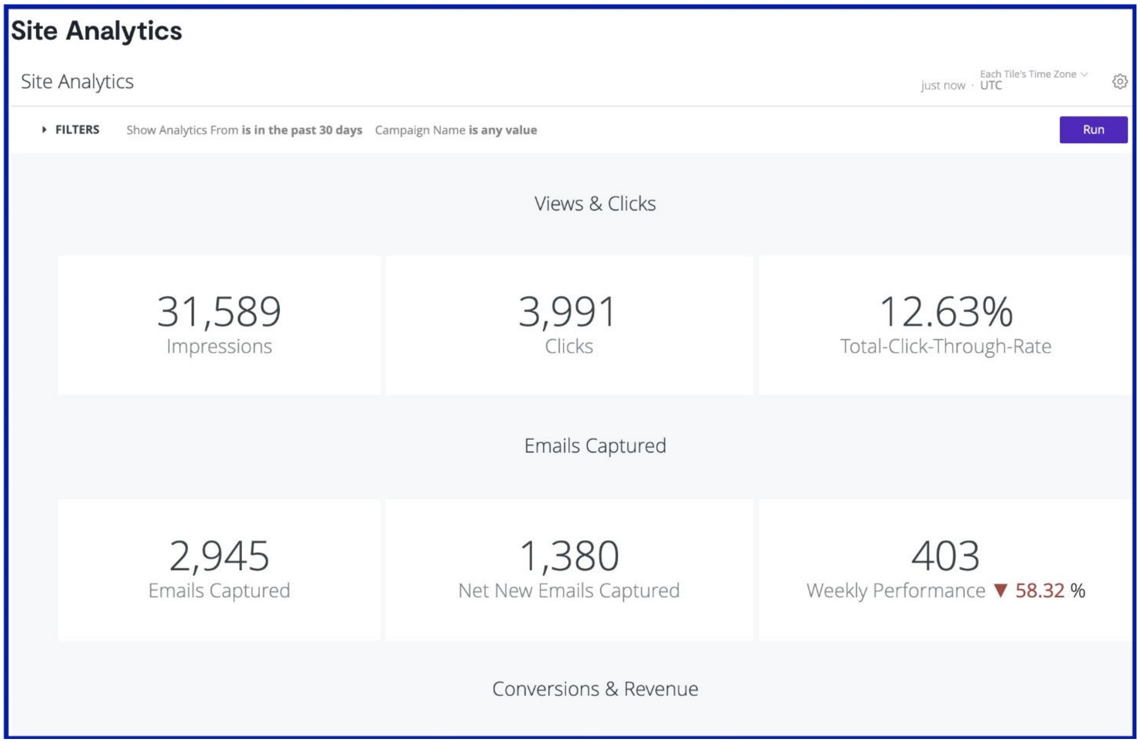
Total Unique Desktop Clicks 4,123

	Link Name	Total Clicks		Unique Clicks	
1	/women	1,789	22....	1,403	22....
2	/men	1,678	17.4%	972	15....
3	Unsubscribe	789	11.1%	714	11.5...
4	Code Block	509	7.1%	455	7.3%
5	Facebook	7	<1%	7	<1%
6	Instagram	7	<1%	7	<1%

123 New York Street
New York, NY 12345
(123) 456-7891

[2] https://help.bluecore.com/en/articles/3616045-link-tracking (last accessed August 30, 2023).

11. To accomplish this task, Bluecore embeds an invisible URL link within the clickable images and words included in the body of an email.[3] These invisible URL links are unique to each recipient of an email campaign—allowing Bluecore to correlate email behavior with its intended recipients. When the recipient of an email clicks on a trackable URL link, the customers are directed to Bluecore's servers, permitting Bluecore to capture a large amount of data, such as the recipient's email address as well as email open rates, and content click rates.[4]



Site Analytics

Site Analytics

just now · Each Tile's Time Zone UTC

FILTERS Show Analytics From **is in the past 30 days** Campaign Name **is any value**

Views & Clicks

31,589 Impressions

3,991 Clicks

12.63% Total-Click-Through-Rate

Emails Captured

2,945 Emails Captured

1,380 Net New Emails Captured

403 Weekly Performance ▼ 58.32 %

Conversions & Revenue

12. After aggregating and analyzing this data, the recipient is finally directed to the final destination—*i.e.*, the clickable part of the email he was interested in visiting.

13. The end landing webpage, however, does not end Bluecore's involvement in the process. After a subscriber ends up on the landing page of a website (*e.g.*, the product catalog displayed in an email), Bluecore uses JavaScript and other persistent cookies installed in the

[3] https://help.bluecore.com/en/articles/4580017-email-visual-template-editor-navigation-and-images (last accessed August 30, 2023).

[4] https://help.bluecore.com/en/articles/4038356-bluecore-site-analytics (last accessed August 30, 2023).

hosting website to monitor customers throughout their purchase journey.[5] Having done so, Bluecore unifies all of the previous anonymous visits of those customers to the hosting website to create a comprehensive user profile—including their interests, purchase intent, and other personal information. With this information in hand, Bluecore then deploys its proprietary algorithm to send personalized emails—such as when a customer abandons a website after placing a product in a purchasing cart.[6]

14. To summarize, Bluecore embeds hidden URL links within the clickable images and words of an email (*i.e.*, it's content). When a user clicks on the content of the email to be directed to a particular webpage within a website (*e.g.*, a specific shirt showcased in the email), Bluecore immediately intercepts the communication and gathers valuable data (including the email address of the subscriber as well as his or her device type, geolocation, IP address and the part of the email he or she clicked on). In addition, Bluecore aggregates this data with the user's previous anonymous visits to the website (linked to the device used to open the email) to create a highly detailed personal profile of that customer—all of this without their knowledge or consent.

15. Bluecore maintains a symbiotic relationship with its clients. Beyond providing the services described above for a fee, Bluecore further enhances its own software capabilities (and thereby attracts new clients) by aggregating the data from its clients' customers: "Bluecore's retail data model processes 500M products and attributes, 5B shopper identities, and 300B behaviors — all of which change and grow as powerful predictive models analyze data for best results."[7] Bluecore also periodically issues industry reports based on the data it processes on behalf of its clients "[i]n the 2022 Retail Ecommerce Benchmark Report, Bluecore analyzed over 35 billion campaigns and shopper data from global ecommerce brands to demonstrate how shoppers are influenced throughout their lifecycle."[8]

[5] https://help.bluecore.com/en/articles/3917362-bluecore-site-targeting-rules (last accessed August 30, 2023).

[6] https://www.bluecore.com/blog/types-triggered-emails/ (last accessed August 30, 2023).

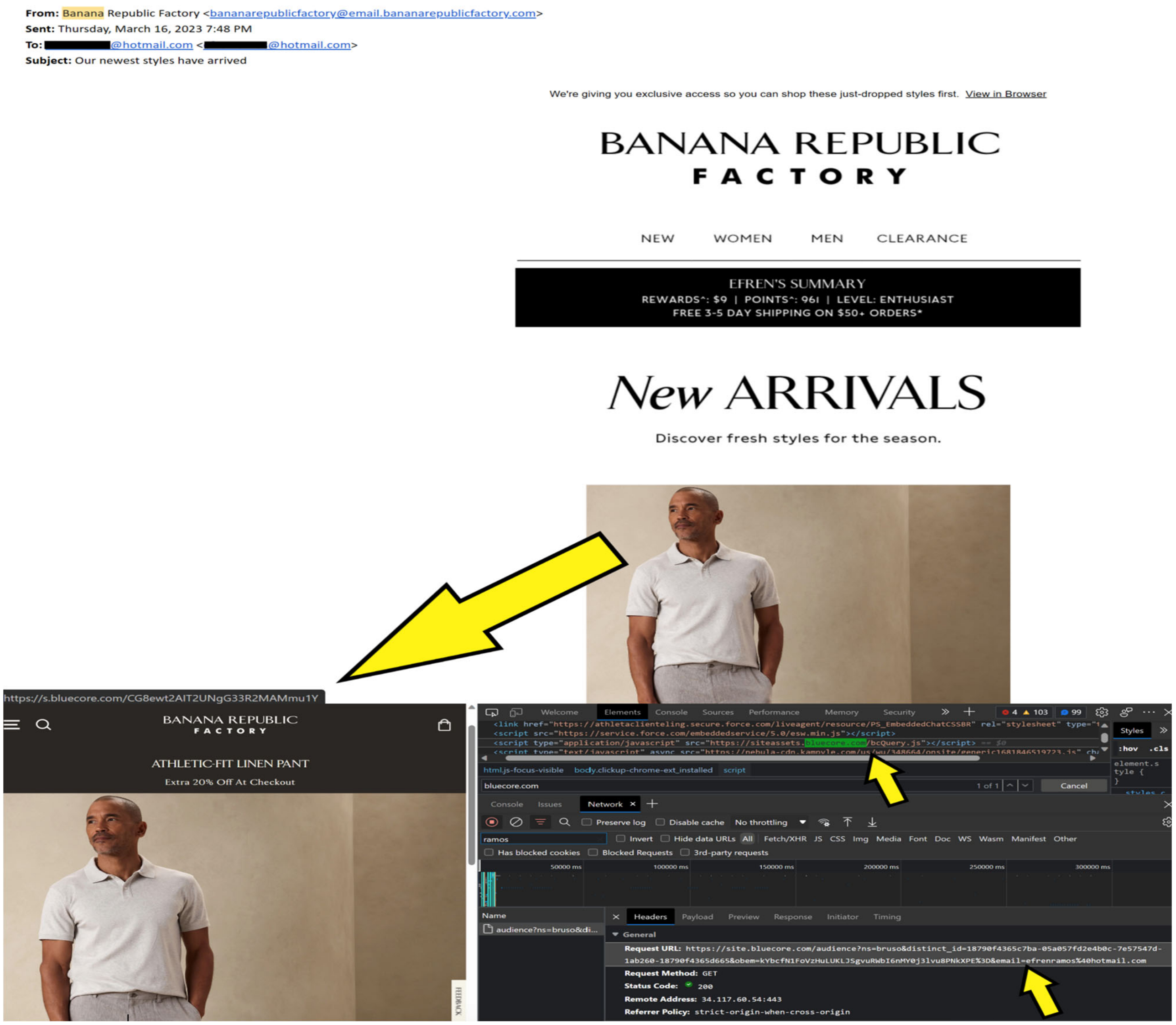
[7] https://www.bluecore.com/solutions/increase-repeat-purchases/ (last accessed August 30, 2023).

[8] https://www.bluecore.com/resources/bluecore-2022-retail-ecommerce-benchmark-report/ (last accessed August 30, 2023).

II. GAP Enables the Interception of Communications On its Emails and Website, Including Plaintiff's

16. Defendant owns and operates the email domain bananarepublicfactory@email.bananarepublicfacotry.com (the "Email") as well as the https://bananarepublicfactory.gapfactory.com/, website (the "Website").

17. Defendant enabled, allowed, or otherwise procured Bluecore to intercept communications between Defendant and its Email's recipients and Website's visitors through a contractual arrangement. Defendant procured Bluecore to embed Bluecore's URLs within the imagery and words (*i.e.*, "Content") of the Emails sent to its subscribers, and continued to intercept their interactions after being redirected to the Website:



From: Banana Republic Factory <bananarepublicfactory@email.bananarepublicfactory.com>
Sent: Thursday, March 16, 2023 7:48 PM
To: [redacted]@hotmail.com <[redacted]@hotmail.com>
Subject: Our newest styles have arrived

We're giving you exclusive access so you can shop these just-dropped styles first. View in Browser

BANANA REPUBLIC FACTORY

NEW WOMEN MEN CLEARANCE

EFREN'S SUMMARY
REWARDS^: $9 | POINTS^: 961 | LEVEL: ENTHUSIAST
FREE 3-5 DAY SHIPPING ON $50+ ORDERS*

New ARRIVALS

Discover fresh styles for the season.

https://s.bluecore.com/CG8ewt2AIT2UNgG33R2MAMmu1Y

BANANA REPUBLIC FACTORY

ATHLETIC-FIT LINEN PANT
Extra 20% Off At Checkout

```
<link href="https://athletaclienteling.secure.force.com/liveagent/resource/PS_EmbeddedChatCSSBR" rel="stylesheet" type="t
<script src="https://service.force.com/embeddedservice/5.0/esw.min.js"></script>
<script type="application/javascript" src="https://siteassets.bluecore.com/bcQuery.js"></script> == $0
<script type="text/javascript" async src="https://nebula-cdn.kampyle.com/us/wu/348664/onsite/generic1681846519723.js" cha
```

```
element.s
tyle {
}
```

html.js-focus-visible body.clickup-chrome-ext_installed script

bluecore.com 1 of 1 Cancel

ramos

Name
audience?ns=bruso&di...

General
Request URL: https://site.bluecore.com/audience?ns=bruso&distinct_id=18790f4365c7ba-05a057fd2e4b0c-7e57547d-1ab260-18790f4365d665&obem=kYbcfN1FoVzHuLUKLJSgvuRWbI6nMY0j3lvu8PNkXPE%3D&email=efrenramos%40hotmail.com
Request Method: GET
Status Code: 200
Remote Address: 34.117.60.54:443
Referrer Policy: strict-origin-when-cross-origin

18. Bluecore operates on the Emails and Website in the manner alleged above.

19. Through its Email and Website wiretaps, Bluecore intercepts, at minimum, the following information from all of Defendant's Email recipients and Website visitors:

(a) Emails: the time, place, device, geolocation, email address, and open rates and click rates of Emails (including what part of the Email's Content was clicked on);

(b) Website Sessions: "The timeframe of 30 minutes from the time a visitor lands on a website."

(c) Visits: "A series of customer interactions within your website that takes place across one or more tabs, while one of these are still active."

(d) User Engagement: "Campaign Seen: "A customer has viewed the popup based on the previously configured display criteria."

(e) Date/Time: "The minimum number of minutes the customer has spent on the website. This is calculated with every page load. Time spent can be further filtered by lifetime, session, or visit as explained in the visit frequency conditions."

(f) Campaign Engaged: "A customer has entered the required information into the popup. For email capture Site campaigns, the campaign is engaged with when an email address is entered. For all other Site campaigns, the campaign is engaged with when it's clicked."

(g) Campaign Closed: "A customer has clicked out of or used the close button to dismiss the popup on-site."

(h) Cookie: "Checks for the cookies available in the customer's browser and matches them with the expected value configured in targeting. Only first-party cookies can be targeted here."

(i) Page scrolled: "Configure page scroll by percentage or pixels. Track customers who have scrolled a certain percentage/pixels of the website's page."

(j) Time spent: "Tracks the time the customer has spent on the current page. Curate a better user experience where an offer is not immediately triggered upon the customer's arrival to the site."

(k) User idle time: "Tracks the inactivity of the customer on the page. Display a promotion with this rule if a customer has spent X number of seconds without switching pages or scrolling."

(l) Has intent to leave: "Captures the exit intent of the customer to trigger a specific overlay to reduce page abandonment."

(m)New user: "A customer that is identified for the first time by the Bluecore Site™ JavaScript. Customers will remain in this state only when it's their first ever visit to a website."

(n) Returning user: "A customer who has been identified as a cookie, but Bluecore has not identified an email address to send marketing communications."

(o) Known user: "A customer who Bluecore has identified and the Bluecore Site™ JavaScript has captured an email address."

(p) Product Interaction: "New user: A customer that is identified for the first time by the Bluecore Site™ JavaScript. Customers will remain in this state only when it's their first ever visit to a website."[9]

20. Plaintiff and the proposed class members received Defendant's Emails and accessed the Website through their internet browsers while in California. Upon having their browsers access the Emails and Websites in California, their browsers were intercepted by Bluecore's servers through the embedded URLs in the Emails and/or the JavaScript of the Website. Through this technology, Bluecore began tracking Plaintiff and the proposed class members' communications as they interacted with the Emails and the Website.

[9] https://help.bluecore.com/en/articles/3917362-bluecore-site-targeting-rules#url-based (last accessed August 30, 2023).

21. When Plaintiff and the proposed class members accessed Defendant's Emails and visited the Website, the contents of their communications – namely, the pieces of data alleged above – were intercepted in real-time by Bluecore, as procured by Defendant. Bluecore then used that data to create unique identifiers for each website visitor, including Plaintiff, and to target advertisements to Plaintiff and the proposed class members. Bluecore also retained and agglomerated this information to further enhance its proprietary algorithms, and subsequently provide statistical reports and presentations to attract new paying clients.

CLASS ACTION ALLEGATIONS

22. Plaintiff brings this action on behalf of himself and all other similarly situated persons pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), and (b)(3). The putative Class is defined as all persons within California who received and opened an Email from Defendant which caused their device to navigate to Defendant's Website.

23. Plaintiff reserves the right to amend the above class definitions and add additional classes and subclasses as appropriate based on investigation, discovery, and the specific theories of liability.

24. ***Community of Interest***: There is a well-defined community of interest among Class members, and the disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and to the Court.

25. ***Numerosity:*** Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the millions. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant.

26. ***Commonality and Predominance***: Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendant has violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631; and whether

members of Class are entitled to actual and/or statutory damages for the aforementioned violations.

27. ***Typicality.*** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other Class members, accessed Defendant's Emails, visited the Website and had his electronic communications intercepted and disclosed to Bluecore—as enabled by Defendant—through the use of Bluecore's wiretaps.

28. ***Adequacy***. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he is committed to prosecuting this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and his counsel.

29. ***Superiority***: A class action is superior to all other available methods of the fair and efficient adjudication of the claims asserted in this action under Federal Rule of Civil Procedure 23(b)(3) because:

(a) The expense and burden of individual litigation makes it economically unfeasible for members of the Classes to seek to redress their claims other than through the procedure of a class action;

(b) If separate actions were brought by individual members of the Classes, the resulting duplicity of lawsuits would cause members to seek to redress their claims other than through the procedure of a class action; and

(c) Absent a class action, Defendant likely would retain the benefits of its wrongdoing, and there would be a failure of justice.

CAUSES OF ACTION

COUNT I

Violation of the California Invasion of Privacy Act Cal. Penal Code § 631, *et seq.*, ("CIPA")

30. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

31. Section 631(a) of CIPA provides for damages and other relief against any person who "by means of any machine, instrument, contrivance, or in any other manner," did any of the following:

a. Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;

Or

b. Willfully and without the consent of all parties to the communication,or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

Or

c. Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained;

Or

d. Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

32. Section 631(a) of the CIPA is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

33. Bluecore’s tracking software (*i.e.*, the Email’s URLs and Website’s Javascript) is a “machine, instrument, contrivance, or … other manner” used to engage in the prohibited conduct at issue here.

34. At all relevant times, by using Bluecore’s tracking software, Bluecore intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiff and the Class members, on the one hand, and Defendant, on the other, without consent.

35. The information that Defendant Bombora collected by using the URL trackers in the Emails, as procured by Defendant, constitutes the “content” of Plaintiff’s and the Class members’ communications with the Emails and Website and arises to the level of common law invasion of privacy.

36. Specifically, the Bluecore tracking software read with specificity the Emails sent by Defendant which Plaintiff and the Class members read and replied to by clicking on the URL link embedded within the content of the Emails. In addition, after intercepting the URLs in the Emails, Bluecore’s tracking software continued to track Plaintiff and the Class members' communication with the Website, as explained in greater detail above.

37. Furthermore, Bluecore provided this aggregated data to Defendant to enable it to learn deep insights, or otherwise enrich, its unknown user base, as explained in greater detail above. Bluecore’s tracking software and contractual arrangements also permitted Defendant to track its known, and unknown, userbase after they logged off the Website while those users browsed their emails. *Davis v. Facebook, Inc. (In re Facebook Inc. Internet Tracking Litig.)*, 956 F.3d 589, 605-608 (9th Cir. 2020) (sustaining a common law invasion of privacy under California law and CIPA § 631(a) claim where the plaintiffs alleged that Facebook collected “a full-string detailed URL, which contains the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested…[which] Facebook then correlates [] with the user ID, time stamp, browser settings and even the type of browser used.”) (emphasis added); *see also In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at *36-37 (N.D. Cal. Dec. 22, 2022) (finding that the plaintiffs established a likelihood

of success in their Wiretap and CIPA § 631(a) claims when Facebook tracked "descriptive URLs…[that] include both the 'path' and the 'query string'" that led to a particular webpage after a user clicked on a log in button on the website) (emphasis added); *see also In re Google RTB Consumer Priv. Litig.*, No. 21-cv-2155- YGR, 2022 U.S. Dist. LEXIS 115023, 2022 WL 2165489, at *10 (N.D. Cal. June 13, 2022) (sustaining a ECPA Wiretap Act and CIPA § 631(a) claims against Google for disclosing to advertisers the "content" of the plaintiffs communications when navigating to particular websites, including the referrer URL that caused navigation to the website).

38. Defendant aided, agreed with, and conspired with Bluecore to implement Bluecore's technology and to accomplish the wrongful wiretapping of the recipients of the Emails and visitors of the Website. In addition, Defendant employed Bluecore to accomplish its own wrongful wiretapping of the offline activity of its Website visitors, as detailed herein.

39. Plaintiff and the Class members did not consent to any of Defendant's actions in implementing the wiretaps. Plaintiff and the Class members did not consent to Bluecore's access, interception, reading, learning, recording, and collection of Plaintiff's and the Class members' electronic communications.

40. As a result of Defendant's violations of Section 632 of CIPA, Plaintiff and the Class members are entitled to damages, statutory damages, punitive damages, injunctive and declaratory relief, and attorney's fees and costs pursuant to Cal. Penal Code § 637.2.

COUNT II
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 635, *et seq.*, ("CIPA")

41. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

42. Section 635 of CIPA provides for damages and other relief against any person who:

> a. Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for

> eavesdropping upon the communication of another;
>
> *Or*
>
> b. any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones;
>
> c. between a cellular radio telephone and a landline telephone in violation of Section 632.5;
>
> *Or*
>
> d. communications between cordless telephones or between a cordless telephone and alandline telephone in violation of Section 632.6.

43. At all relevant times, by implementing the Bluecore wiretaps, Defendant intentionally manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished a wiretap device that is primarily or exclusively designed or intended for eavesdropping and intercepting the communication of another.

44. Bluecore's software code is a "device" that is "primarily or exclusively designed" for eavesdropping and intercepting communications. That is, the Bluecore Email URLs and Website Javascript trackers are designed to intercept and gather the contents of electronic communications, including Plaintiff and the Class members' replies to Defendant's Emails and subsequent visits to the Website; as well as their offline activity outside of the Website.

45. Plaintiff and the Class members did not consent to any of Defendant's actions in implementing the Bluecore wiretaps detailed herein.

46. As a result of Defendant's violations of Section 635 of CIPA, Plaintiff and the Class members are entitled to damages, statutory damages, punitive damages, injunctive and declaratory relief, and attorney's fees and costs pursuant to Cal. Penal Code § 637.2.

COUNT III
Statutory Larceny
Cal. Penal Code § §§ 484 and 496
(On Behalf of Plaintiff and the Class)

47. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

48. Cal. Penal Code § 496(a) prohibits the obtaining of property "in any manner constituting theft."

49. Cal. Penal Code § 484 defines theft and provides:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

50. Cal. Penal Code § 484 thus defines "theft" to include obtaining property by false pretense.

51. Under California law, personal information constitutes property for the purpose of Cal. Penal Code § 496(a). *Calhoun v. Google LLC*, No. 20-CV-05146-LHK, 2021 U.S. Dist. LEXIS 54107, at *60-62 (N.D. Cal. Mar. 17, 2021) (collecting cases).

52. Cal. Civ. Code § 1798.140, defines personal information as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement."

53. The data that Defendant enabled Bluecore to collect from the computers of Plaintiff and the Class members—by implementing and using Bluecore's wiretaps on the Emails

and Website—was aggregated to create consumer profiles, and their interactions with Defendant's Emails and Website constitutes personal information.

54. Defendant intentionally designed and implemented the Bluecore wiretaps unbeknownst to Plaintiff the Class members whose computers were thus deceived into providing personal information to Defendant.

55. Defendant acted in a manner constituting theft and/or false pretense.

56. Defendant stole, took, and/or fraudulently appropriated Plaintiff and the Class members' personal information without their consent.

57. Defendant concealed, aided in the concealing, sold, and/or utilized Plaintiff's and the Class members' personal information that was obtained by Defendant for Defendant's commercial purposes and the financial benefit of Defendant.

58. Defendant knew that Plaintiff's and the Class members' personal information was stolen and/or obtained because Defendant designed or implemented the Bluecore wiretaps that tracked Plaintiff's and the Class members' personal information and operated it in a manner that was concealed and/or withheld from Plaintiff and the Class members.

59. The reasonable and fair market value of the unlawfully obtain personal data can be determined in the marketplace.

COUNT IV
Violation of California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL")

60. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

61. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code § 17200. 409. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

62. Defendant violated the UCL by engaging in unlawful and unfair business acts and practices.

63. Defendant's "unlawful" acts and practices include its violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; California Invasion of Privacy Act, Cal. Penal Code §§ 635, *et seq.*; and California Statutory Larceny, Cal. Penal Code §§ 484 and 496.

64. Defendant's conduct violated the spirit and letter of these laws, which protect property, economic, and privacy interests and prohibit unauthorized disclosure and collection of private communications and personal information.

65. Defendant's "unfair" acts and practices include their violation of property, economic, and privacy interests protected by the: California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 635, *et seq.*; and California Statutory Larceny, Cal. Penal Code §§ 484 and 496.

66. To establish liability under the unfair prong, Plaintiff needs not establish that these statutes were actually violated, although the claims pleaded herein do so.

67. Defendant never obtained Plaintiff's or the Class members' permission to permit Bluecore to intercept or read their communications with the Emails or Website; nor did they permit Defendant to send their personal information to third parties, such as Bluecore, or the general public without their consent. Plaintiff and the Class members thus had no reason to know and could not have anticipated this intrusion into their privacy by the disclosure of their private communications with the Emails or the Website. Defendant acted in concert with Bluecore in violating the privacy expectations of Plaintiff and the Class members. Defendant's conduct was immoral, unethical, oppressive, unscrupulous, and substantially injurious to Plaintiff and the Class members. Further, Defendant's conduct narrowly benefitted its own business interests at the expense of Plaintiff's and the Class members' fundamental privacy interests protected by California's state laws.

68. The wiretaps that Defendant concealed would be, and are, material to reasonable consumers, namely, that rather than not sharing the information contained within the Emails or the Website, that information was in fact shared with third parties, such as Bluecore.

69. Plaintiff has suffered an in-jury-in-fact, including the loss of money and/or property, as a result of Defendant's unfair and/or unlawful practices, to wit, the unauthorized disclosure and taking of his personal information which has value as demonstrated by its use and sale by Defendant. Plaintiff has suffered harm in the form of diminution of the value of his private and personally identifiable data and online activities. Defendant's actions caused damage to and loss of Plaintiff's property right to control the dissemination and use of his personal information and communications.

70. Defendant reaped unjust profits and revenues in violation of the UCL. This includes Defendant's profits and revenues from their targeted marketing campaigns.

71. Defendant's unfair, fraudulent, and unlawful business practices, as enumerated and explained above, were the direct and proximate cause of financial injury to Plaintiff and the Class members. Defendant has unjustly benefitted as a result of its wrongful conduct. Accordingly, Plaintiff and the California Subclass seek an order of this Court that includes, but is not limited to, requiring Defendant to: (a) provide restitution to Plaintiff and the Class members; (b) disgorge all revenues obtained as a result of its violations of the UCL; (c) pay attorneys' fees and costs for Plaintiff and the Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiff as representative of the Class; and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For compensatory, statutory and punitive damages in amounts to be determined by the Court and/or jury;

(d) For prejudgment interest on all amounts awarded;

(e) For an order of restitution and all other forms of equitable monetary relief; and

(f) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable.

Dated: September 13, 2023

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ L. Timothy Fisher*

L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

Joseph I. Marchese (*pro hac vice* forthcoming)
Alec M. Leslie (*pro hac vice* forthcoming)
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
aleslie@bursor.com

GUCOVSCHI ROZENSHTEYN, PLLC.
Adrian Gucovschi (*pro hac vice* forthcoming)
630 Fifth Avenue, Suite 2000
New York, NY 10111
Telephone: (212) 884-4230
Facsimile: (212) 884-4230
E-Mail: adrian@gr-firm.com

Attorneys for Plaintiff