BURSOR & FISHER, P.A.
Sarah N. Westcot (State Bar No. 264916)
701 Brickell Avenue, Suite 1420
Miami, FL 33131
Telephone: (305) 330-5512
E-mail: swestcot@bursor.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KRISTEN LOCKHART, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CRUMBL, LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Kristen Lockhart ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant Crumbl, LLC ("Crumbl" or "Defendant") for violating the California Invasion of Privacy Act ("CIPA").

2. Crumbl owns and operates the website, www.crumblcookies.com (the "Website"), through which Crumbl sells its signature cookies.

3. Unbeknownst to Plaintiff and consumers visiting the Website, Crumbl knowingly and willfully assists a third party, Stripe, Inc. ("Stripe"), with intercepting confidential communications that contain consumers' sensitive information.

4. Stripe is one of the world's largest payment processing companies. However, unlike its competitors, Stripe engages in the surreptitious interception and collection of sensitive information, including consumers mouse movements and clicks, keystrokes, IP address, geolocation, and financial information. Stripe accomplishes this, in part, by embedding wiretaps in the computer code of its merchant clients' websites. These wiretaps function by installing tracking cookies on consumers' web browsers the moment they enter one of Stripe's merchant clients' websites.

5. Crumbl assisted Stripe in installing these wiretaps on its Website, which continue to track consumers online activity as they navigate through other websites.

6. Plaintiff brings this action for damages and other legal and equitable remedies resulting from Defendant's violation of the CIPA.

PARTIES

7. Plaintiff Kristen Lockhart is, and has been at all relevant times, a citizen of California who resides in Antioch, California.

8. Ms. Lockhart made several purchases through Crumbl's Website, most recently in approximately June 2023. However, Ms. Lockhart was unaware of Defendant's conduct alleged herein until August 2023.

9. Immediately upon entering the Website, Crumbl assisted Stripe with installing the Stripe.js software onto Plaintiff's web browser without her knowledge or consent. When purchasing Crumbl's signature cookies on the Website, Ms. Lockhart entered her credit card information to complete the transaction.

10. When entering her credit card information on the Website, Ms. Lockhart reasonably expected that Crumbl would keep this information private and not disclose it to third parties. However, Crumbl disclosed such information to a third party, Stripe, without Ms. Lockhart's knowledge or consent. Stripe also continued monitoring Ms. Lockhart's online activity through the Stripe.js software long after her transaction on the Website was completed. This allowed Stripe to intercept additional information, including Ms. Lockhart's IP address and geolocation.

11. Stripe was then able to match this data intercepted from the Website to its existing database to identify Ms. Lockhart as the party completing the transaction.

12. Ms. Lockhart would not have completed a transaction on Crumbl's Website if she knew it was assisting Stripe in intercepting and tracking her sensitive online activity. Similarly, Ms. Lockhart would not have completed a transaction on the Website if she knew that Crumbl was assisting Stripe in monetizing her private information to Stripe's network of merchant customers.

13. Defendant Crumbl, LLC is a Utah limited liability company with its principal place of business at 160 E University Pkwy, Ste G, Orem, Utah 84058. Defendant develops, owns, and operates www.crumblcookies.com, a website that sells Crumbl's signature cookies.

JURISDICTION AND VENUE

14. 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 of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 members of the putative class, and Plaintiff, as well as most members of the proposed class, are citizens of different states than Defendant.

15. This Court has personal jurisdiction over Defendant. First, by integrating the code that allowed a third party to wiretap communications, Crumbl acted intentionally. Second, Crumbl knew that the harm would be felt in California because it received billing and mailing addresses each time a customer completed a purchase. Third, Crumbl expressly aimed its conduct at California because Crumbl, in the regular course of business, sells products through its interactive website and causes those products to be delivered to the forum. More specifically, through the Website, Crumbl sells products to California residents and delivers those products to their home addresses in California. Crumbl also allows customers to pick up their purchases from store locations in California.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in this District.

FACTUAL BACKGROUND

17. Each year, Americans spend more than $1 trillion on the internet, a figure that only continues to grow. [1] Despite this explosion in ecommerce, online retailers routinely fail to protect consumers' personal information, a failure that has reached "epidemic" levels[2] and shows no signs of slowing down.[3] Indeed, more than half of all Americans have suffered from a data breach,[4] costing each one an average of $146.[5] From these hacks, only fraudsters benefit, with identity thieves buying and selling personal information "by the millions" through illicit, online

[1] John Koetsier, *E-Commerce Retail Passed $1 Trillion For the First Time Ever*, FORBES (Jan. 28, 2023), https://www.forbes.com/sites/johnkoetsier/2023/01/28/e-commerce-retail-just-passed-1-trillion-for-the-first-time-ever/?sh=3191f5a836df.

[2] Apple, Report: 2.6 billion personal records compromised by data breaches in past two years – underscoring need for end-to-end encryption (Dec. 7, 2023), https://www.apple.com/newsroom/2023/12/report-2-point-6-billion-records-compromised-by-data-breaches-in-past-two-years/.

[3] Yves Audebert, Why authentication is good medicine for today's data breach epidemic (June 6, 2023), https://www.securitymagazine.com/articles/99443-why-authentication-is-good-medicine-for-todays-data-breach-epidemic.

[4] Kenneth Olmstead, et. al., *1. Americans' experiences with data security*, Pew Research Center (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security/

[5] IBM Security, Cost of a data breach Report (2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

marketplaces.[6] There is such a glut of supply, in fact, that prices are relatively low; banking information costs around $100, for example, while credit card information costs as low as $10.[7]

18. Despite these concerns, online retailers, like Crumbl, intentionally assist third parties in intercepting information that is sensitive and confidential. When completing a transaction, for example, a consumer often conveys details about her credit card and mailing address. Undoubtedly, consumers expect this information to be private and used only for the purposes of completing the transaction.

19. However, merchants, like Crumbl, assist third parties in intercepting this sensitive information to protect themselves from fraudulent transactions.

20. Once that information is received, third parties dissect it for inferences, taking anything they can glean and retooling it into products that they can sell to other customers.

21. As an industry, online retailers have failed to protect consumers' personal information. Not only have they failed to protect that information, but they have also shared it voluntarily and intentionally, without obtaining consumer consent to do so.

22. Consumers in California have a right to know if private companies intend on sharing their sensitive information with third parties. Such disclosures are typically contained in a privacy policy on a company's website.

23. In fact, California law requires companies to "conspicuously post" their privacy policies. *See* Cal. Bus. & Prof. Code §§ 22575–79. As California courts have held, a notice is conspicuous if a reasonably prudent person would have seen it.

24. Such policies are crucial so that consumers are aware of what companies are doing with their sensitive information.

---

[6] NordVPN, Analyzing 4 million payment card details found on the dark web, https://nordvpn.com/research-lab/payment-card-details-theft/.

[7] Ryan Smith, *Revealed – how much is personal information worth on the dark web?*, Ins. Bus. Mag. (May 1, 2023), https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx#:~:text=Online%20banking%20login%20information%20costs,be%20purchased%20for%20about%20%241%2C000.

25. As stated by California Attorney General Xavier Becerra, "California consumers have the right to know, the right to delete, and the right to opt-out of the sale of the personal information collected by businesses."

26. This does not stop some companies, like Crumbl, from assisting third parties, like Stripe, in intercepting consumers' sensitive information without their knowledge or consent.

Stripe's Payment Processing Services

27. Stripe offers merchants an online payment processing platform which merchants can integrate into their website for the purported purpose of processing consumer purchases.[8]

28. However, Stripe does not merely process transactions. Instead, Stripe intercepts and indefinitely stores consumer PII and financial information into its fraud prevention network.

29. Stripe accomplishes this through two of its products, Stripe Elements and Stripe Radar.

30. Stripe Elements is Stripe's flagship payment process offering. In order to function, Stripe requires merchants, including Defendant, to integrate Stripe's software code into their websites. This enables Stripe to display payment forms and process payments consumers make on merchants' website.

31. However, Stripe does far more than facilitate payments. When merchants, like Defendant, integrate the Stripe.js code onto their website, the code allows Stripe to intercept communications consumers reasonably believe will be sent directly to the merchant.

32. Consumers are unaware that Stripe is even involved in the purchasing process, as Stripe Elements enables merchants to customize payment fields to match the merchants existing website. This allows the Stripe Elements payment forms to appear as though they are generated by the merchant itself.

33. Millions of merchants have integrated Stripe's code onto their websites, allowing Stripe to amass an incredible amount of sensitive consumer data including PII and consumer

[8] https://www.stripe.com.

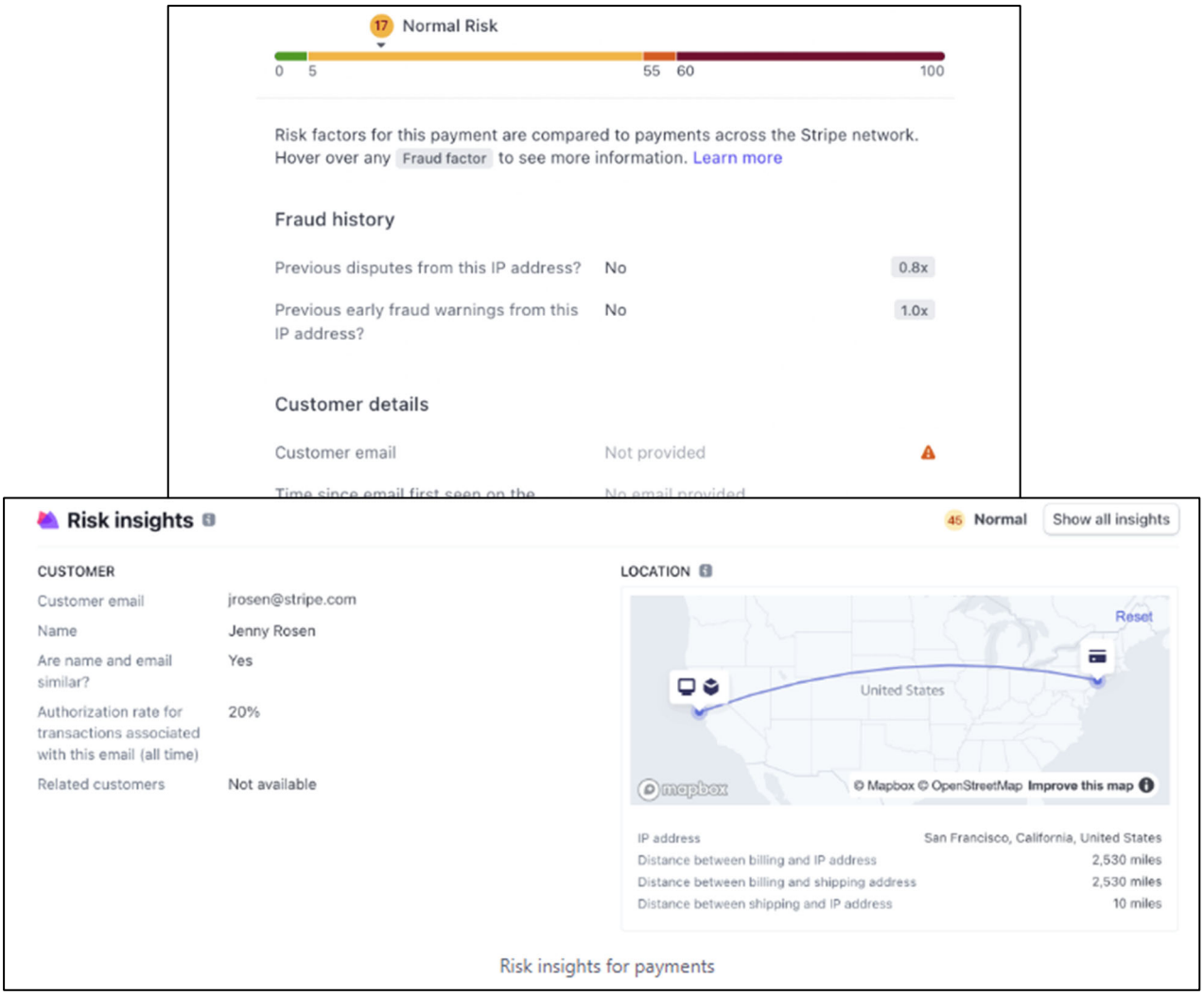
financial information. Stripe leverages this personal consumer data to assess the risk associated with particular consumers and their transactions.

34. This risk assessment service offered by Stripe involves the creation of consumer profiles. Using the PII and financial data it has amassed, Stripe assigns a "risk score" to assist merchants, like Crumbl, in determining whether a transaction is likely to be fraudulent.[9]

35. These risk management services are designed to protect merchants, rather than consumers, from fraud.

36. For example, Stripe allows merchants to access its network-wide insights to detect fraud, as shown in Figures 1 and 2:

Figures 1 and 2:



[9] https://docs.stripe.com/radar/risk-evaluation.

37. As shown in Figures 1 and 2, the information compiled by Stripe includes at minimum consumers names, email addresses, delivery addresses, IP address, and geolocation.

38. However, Stripe also collects and indefinitely stores information as consumers navigate through a merchant's website, include the consumer's mouse movements and clicks, keystrokes, name of the consumer's bank or credit card issuer, whether the consumer had sufficient funds for a transaction, and whether the consumer later disputed a charge to their card.

39. This database of consumer data collected and stored by Stripe allows Stripe to identify consumers across devices, networks, and identities and share this information with the merchants paying Stripe for its risk management services.

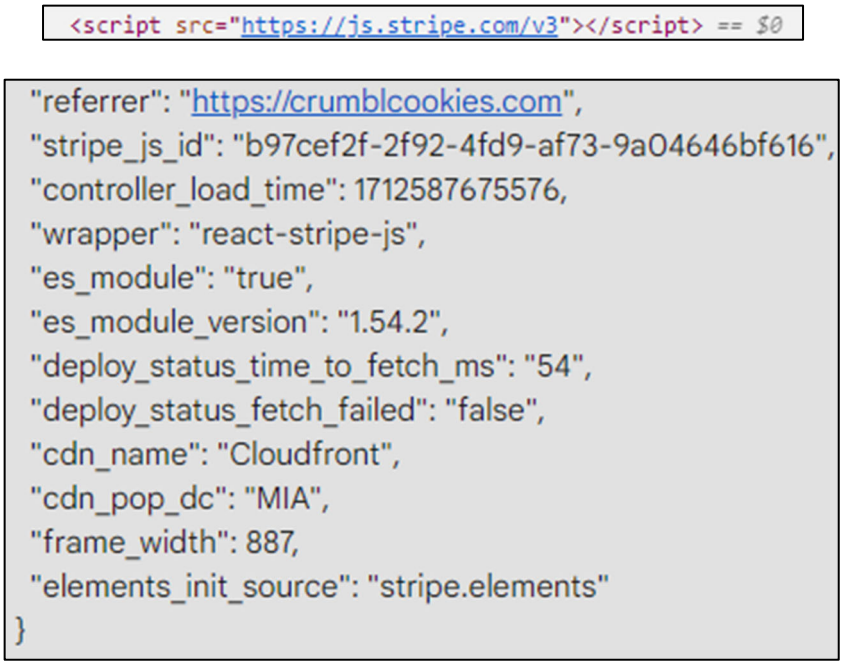
40. Stripe has monetized the collection of personal consumer data, including PII and financial information. Without the collection and storage of this information, Stripe would be unable to sell its risk assessment products to merchants for financial gain.

Defendant's Use of Stripe's Services

41. Consumers visit Defendant's Website to make online purchases for its signature Crumbl cookies.

42. Defendant integrated the Stripe.js code on its Website to track consumer purchasing behaviors and process customer transactions. This code is embedded on a consumer's browser the moment they enter the Website and tracks them as they navigate to other webpages, as shown in Figures 3 and 4.

Figures 3 and 4:

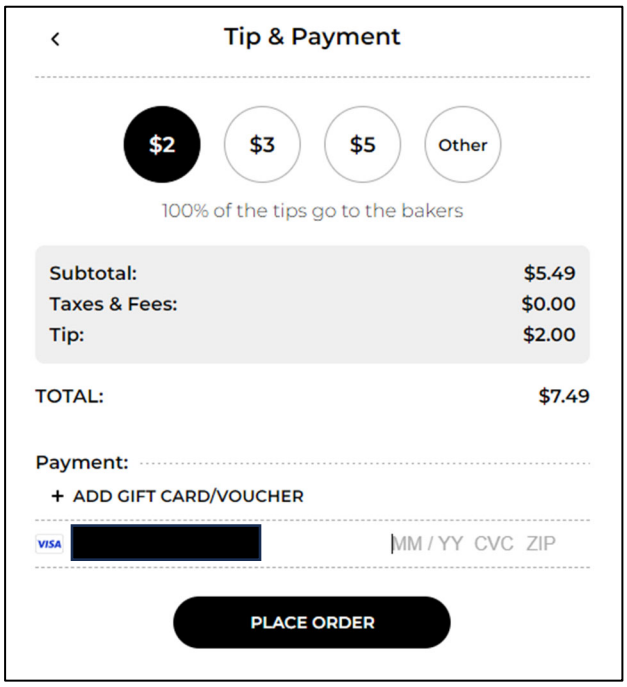


43. This code allows Stripe to surreptitiously intercept sensitive information, including a consumer's mouse movements and clicks, keystrokes, IP address, and geolocation.

44. Defendant's Website does not include any identifying information or identification to alert consumers that their transactions are being processed by a third party.

45. Specifically, there is no branding on the payment screens indicating that Stripe is involved, and consumers cannot tell that Stripe is obtaining or storing sensitive information, including financial information.

Figure 5:



46. Consumers never consent, nor are they alerted, that the Stripe.js code is being embedded on their browser upon entering the Website.

47. During the checkout process, Stripe's code allows it to intercept additional information, including card issuer information, payment method, credit card numbers, credit card cvc, credit card expiration date, and zip code.

Figure 6:

48. During the checkout process, there is no privacy policy that alerts consumers that their sensitive information is being shared with and indefinitely stored by a third party.

49. Consequently, consumers think they are only sending their sensitive information to Crumbl to facilitate their purchases.

50. However, unbeknownst to consumers, Crumbl assists Stripe in intercepting and indefinitely storing this sensitive information.

51. Also unbeknownst to consumers, Crumble assists Stripe in monetizing this consumer information by allowing Stripe to incorporate its consumers' data into Stripe's database, which in turn allows Stripe to market its fraud prevention services (utilizing this data) to other merchants.

52. At no time are consumers informed nor do consumers consent to their sensitive information being disclosed or monetized in this manner.

53. Additionally, the Stripe.js code remains on a consumers browser after they complete their purchase on Defendant's Website, allowing Stripe to intercept more information as consumers make other online purchases from other merchants utilizing Stripe's product offerings.

CLASS ALLEGATIONS

54. **Class Definition**: Plaintiff seeks to represent a class of similarly situated individuals defined as all persons in California who made a purchase from Defendant's website, www.crumblcookies.com (the "Class").

55. Subject to additional information obtained through further investigation and discovery, the above-described Class may be modified or narrowed as appropriate, including through the use of multi-state subclasses.

56. **Numerosity (Fed. R. Civ. P. 23(a)(1))**: At this time, Plaintiff does not know the exact number of members of the Class. However, given the popularity of Defendant's website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

57. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2), 23(b)(3))**: There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

(a) whether Defendant collected Plaintiff's and the Class's PII;

(b) whether Defendant collected Plaintiff's and the Class's financial information;

(c) whether Defendant unlawfully disclosed and continues to disclose its users' PII and financial information in violation of the CIPA;

(d) whether Defendant's disclosures were committed knowingly;

(e) whether Defendant disclosed Plaintiff's and the Class's PII and financial information without consent;

(f) whether Defendant intentionally recorded Plaintiff and Class members' communications under the CIPA; and

(g) whether Plaintiff and Class members' PII and financial information are content under the CIPA.

58. **Typicality (Fed. R. Civ. P. 23(a)(3))**: Plaintiff's claims are typical of those of the Class because Plaintiff, like all members of the Class, placed an order on Defendant's Website and had her sensitive information collected and disclosed by Defendant, and had her communications recorded by Defendant, without her consent.

59. **Adequacy (Fed. R. Civ. P. 23(a)(4))**: Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation, including litigation concerning the CIPA. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiff nor her counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional representatives to represent the Class, additional claims as may be appropriate, or to amend the definition of the Class to address any steps that Defendant took.

60. **Superiority (Fed. R. Civ. P. 23(b)(3))**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Class is impracticable. Even if every member of the Class could afford to pursue individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action.

CAUSES OF ACTION

COUNT I
Violation of the California Invasion of Privacy Act, Cal. Penal Code § 631

61. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class.

62. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . ." Cal. Penal Code § 630.

63. A person violates California Penal Code § 631(a), if:

> by means of any machine, instrument, or contrivance, or in any other manner, [s/he] 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 [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to 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 [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

64. Further, a person violates § 631(a) if s/he "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" in the preceding paragraph. *Id.*

65. To avoid liability under § 631(a), a defendant must show it had the consent of all parties to a communication.

66. At all relevant times, Defendant aided, agreed with, and conspired with Stripe to track and intercept Plaintiff's and Class Members' internet communications while accessing www.crumblcookies.com. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

67. Defendant, when aiding and assisting Stripe's wiretapping and eavesdropping, intended to help Stripe learn some meaning of the content in the form fields entered by Plaintiff and Class members.

68. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Stripe's payment platform and Stripe.js code fall under the broad catch-all category of "any other manner":

(a) The computer codes and programs Stripe used to track Plaintiff and Class Members' communications while they were navigating www.crumblcookies.com;

(b) Plaintiff's and Class Members' browsers;

(c) Plaintiff's and Class Members' computing and mobile devices;

(d) The computer codes and programs used by Stripe to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit www.crumblcookies.com; and

(e) The plan Stripe carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile

application to visit www.crumblcookies.com.

69. The information that Defendant transmitted using Stripe's payment platform and Strip.js code constituted sensitive and confidential personally identifiable information.

70. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive its customers' sensitive and confidential online communications through www.crumblcookies.com without their consent.

71. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, $5,000 dollars per violation or three times the amount of actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages." Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

COUNT II
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 632

72. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

73. The following items constitute "an electronic amplifying or recording device" under CIPA:

(a) The computer codes and programs Stripe used to track Plaintiff and Class Members' communications while they were navigating www.crumblcookies.com;

(b) Plaintiff's and Class Members' browsers;

(c) Plaintiff's and Class Members' computing and mobile devices;

(d) The computer codes and programs used by Stripe to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit www.crumblcookies.com; and

(e) The plan Stripe carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit www.crumblcookies.com.

74. The data collected on Defendant's website constitutes "confidential communications," as that term is used in Section 632, because Class Members had objectively reasonable expectations of privacy with respect to their PII and financial information.

75. Defendant is liable for aiding and abetting violations of Section 632 by the third-party vendors.

76. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class members have been injured by the violations of Cal. Penal Code § 635, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT III
Invasion Privacy Under California's Constitution

77. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

78. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential online communications; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

79. At all relevant times, by using Stripe's payment platform and computer code to record and communicate consumers' sensitive and confidential online communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

80. Plaintiff and Class Members had a reasonable expectation that their sensitive and confidential online communications, identities, and financial information would remain confidential, and that Defendant would not install wiretaps on www.crumblcookies.com.

81. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' sensitive and confidential online communications.

82. This invasion of privacy was serious in nature, scope, and impact because it related to their sensitive and confidential online communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

83. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

PRAYER FOR RELIEF

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

(a) For an order certifying the Class 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 declaring that Defendant's conduct violates the statutes referenced herein;

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

(d) An award of statutory damages to the extent available;

(e) For punitive damages, as warranted, in an amount to be determined at trial;

(f) For prejudgment interest on all amounts awarded;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

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

JURY TRIAL DEMANDED

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

Dated: May 1, 2024

BURSOR & FISHER, P.A.

By: */s/ Sarah N. Westcot*
Sarah N. Westcot

Sarah N. Westcot (State Bar No. 264916)

701 Brickell Avenue, Suite 1420
Miami, FL 33131
Telephone: (305) 330-5512
E-mail: swestcot@bursor.com

Counsel for Plaintiff

ClassAction.org
