

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

FAN MILLS, individually and on behalf of all
others similarly situated,

Plaintiff,

v.

SAKS.COM LLC,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Fan Mills, individually and on behalf of all others similarly situated, as set forth herein, alleges as follows:

NATURE OF THE ACTION

1. This is a class action on behalf of persons in the State of Arizona that opened emails sent to them by Defendant Saks.com LLC (“Defendant” or “Saks”) for Defendant’s violations of Arizona’s Telephone, Utility and Communication Service Records Act, A.R.S. § 44-1376 *et seq.*
2. Defendant is the self-described “leading name in luxury fashion.”¹ To maximize sales, Defendant solicits customers to sign up for its email list.
3. Plaintiff and Class members are subscribers to Defendant’s email list.

¹ Saks Fifth Avenue, *Saks Fifth Avenue Announces Expansion of the Fifth Avenue Club*, PR NEWswire (Jun. 1, 2023), <https://www.prnewswire.com/news-releases/saks-fifth-avenue-announces-expansion-of-the-fifth-avenue-club-301839651.html>

4. Defendant embeds trackers within its emails. These trackers record whether and when subscribers open and read their messages. Defendant never received subscribers' consent to collect this information.

5. By failing to receive consent from Plaintiff and Class members, Defendant is violating Arizona's Telephone, Utility and Communication Service Records Act, a statute that prohibits procuring or attempting to procure the communication service records of email recipients without their authorization.

THE PARTIES

6. Plaintiff Fan Mills is a resident of Arizona, residing in Phoenix, Arizona. Within the past two years, Plaintiff has received promotional emails from Defendant.

7. From 2017 to October 2023, Plaintiff frequently opened emails from Defendant to review promotional materials. Plaintiff most recently opened one of Defendant's emails in October 2023.

8. Each time Plaintiff opened an email from Defendant, Defendant procured information identifying her and disclosing when she opened and read the email.

9. Defendant never received consent from Plaintiff to procure her private email records.

10. Defendant Saks.com LLC is a Delaware corporation with its principal place of business in New York, New York.

JURISDICTION AND VENUE

11. The 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, and there are over 100 members of the putative class, and Plaintiffs, as well as most members of the proposed class, are citizens of different states than Defendant.

12. The Court has personal jurisdiction over Defendant because Defendant is domiciled in the State of New York.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this District.

FACTS SUPPORTING PLAINTIFF'S CLAIM

A. The HP Spying Scandal and A.R.S. § 44-1376

14. In 2001, Hewlett-Packard “embark[ed] on one of the largest and most difficult mergers in American business history.”² Spearheaded by then-CEO Carly Fiorina, HP sought to acquire a rival company, Compaq, Inc., in a deal valued at \$25 billion.³

15. “Widely considered one of the worst tech mergers in history,”⁴ the economic fallout from the acquisition began immediately.⁵ By 2004, “Hewlett-Packard’s stock had dropped below seventeen dollars, from a high of more than sixty dollars, in 2000.”⁶ Industry insiders took note, with a “consensus” believing that “the new HP, the tech industry’s most sprawling conglomerate,

² Michael Malone, *The H-P-Compaq Mess Isn't All Carly's Doing*, WALL. ST. J. (May 21, 2002), <https://www.wsj.com/articles/SB1021933260918245440>.

³ Andrew Ross Sorkin, *Hewlett-Packard in Deal to Buy Compaq for \$25 Billion in Stock*, N.Y. TIMES (Sept. 4, 2001), <https://www.nytimes.com/2001/09/04/business/hewlett-packard-in-deal-to-buy-compaq-for-25-billion-in-stock.html>.

⁴ PCMag Staff, *The Biggest Tech Mergers and Acquisitions of All Time*, PCMAG (Apr. 12, 2021), <https://www.pcmag.com/news/the-biggest-tech-mergers-and-acquisitions-of-all-time>.

⁵ Mike Musgrove, *HP Posts \$2 Billion Loss in First Full Quarter with Compaq*, WASH. POST (Aug. 28, 2002), <https://www.washingtonpost.com/archive/business/2002/08/28/hp-posts-2-billion-loss-in-first-full-quarter-with-compaq/2486859a-b55c-4247-9f0a-cb1d839b68d8/>.

⁶ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007), <https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

ha[d] lost its focus and [was] being squeezed between two formidable rivals with much clearer business models, Dell and IBM.”⁷

16. In January 2005, a few days before HP’s annual retreat, two board members, Patricia Dunn and George Keyworth, met with Fiorina to discuss their concerns about the company’s direction.⁸ Fiorina sought to placate Dunn and Keyworth, “agree[ing] to tear up her agenda for the board’s strategy retreat ... and focus instead on the directors’ concerns.”⁹ But shortly after the retreat, “a reporter for the *Wall Street Journal*, Pui-Wing Tam, called to confirm details that Tam had learned about the retreat, including assertions that Fiorina had lost the confidence of the board and that operating responsibilities would soon be shifted away from her.”¹⁰ “Clearly, someone at the retreat, which was attended only by board members and top executives, had leaked proprietary information.”¹¹

17. Fiorina responded with fury. After “call[ing] the board members together on the phone,” Fiorina “dressed them down for giving details of the meeting.”¹² But that response only further inflamed tensions between Fiorina and the board, and less than two weeks after the retreat, the board met again, this time without Fiorina, and voted to dismiss her.¹³

⁷ The Economist Staff, *Losing the HP way*, THE ECONOMIST (Aug. 19, 2004), <https://www.economist.com/business/2004/08/19/losing-the-hp-way>.

⁸ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007), <https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

⁹ Alan Murray, H-P Board Clash Over Leaks Triggers Angry Resignation, WALL ST. J. (Sept. 6, 2006), <https://www.wsj.com/articles/SB115749453036454340>.

¹⁰ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007), <https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

¹¹ *Id.*

¹² Alan Murray, H-P Board Clash Over Leaks Triggers Angry Resignation, WALL ST. J. (Sept. 6, 2006), <https://www.wsj.com/articles/SB115749453036454340>.

¹³ *Id.*

18. Despite Fiorina’s departure, board members remained perturbed by the disclosures to the press, and so when elevating Patricia Dunn to nonexecutive chairwoman and tasking her with choosing Fiorina’s successor, the board also provided Dunn with another mandate: “stop the board leaks.”¹⁴

19. Dunn promptly initiated an investigation, code-naming it “Project Kona.”¹⁵ But before Project Kona could get off the ground, another, more damaging leak came to light.¹⁶ In the months after Fiorina’s removal, Dunn selected Mike Hurd, a CEO at a competitor company, to serve as HP’s new CEO.¹⁷ But before the board could make an announcement, a reporter from *Business Week* reached out, asking for comment on Hurd’s selection.¹⁸ Because Hurd had not yet left the other company, revealing his candidacy before he resigned could potentially derail the process.¹⁹ Although Hurd would go on to become HP’s CEO without issue, the new disclosure added urgency to determining who was behind the leaks.²⁰ For Dunn, Project Kona was the way to find out.²¹

20. To staff Project Kona, Dunn turned to a security manager at HP, Kevin Huska, who, in turn, “referred Dunn to an outside investigator named Ronald R. DeLia, whose firm, Security Outsourcing Solutions, based in Boston, had been under contract to Hewlett-Packard for some ten years.”²² Throughout the summer of 2005, Dunn received regular updates from DeLia, including

¹⁴ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007), <https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

one call where he “revealed that his investigators had obtained private phone records of reporters.”²³ DeLia received these records through “pretexting,” which, in his own words, “involved investigators requesting information from [telephone] operators orally, over the phone, pretending to be someone else if necessary.”²⁴ Notwithstanding this invasion of privacy, Project Kona failed to pinpoint a leaker, and as the year winded down, so too did the investigation.²⁵

21. Then, in January 2006, a reporter from CNET, Dawn Kawamoto, published an “inside account of the company’s retreat, held two weeks earlier.”²⁶ The substance of the article was innocuous, but at HP, “the story was met with alarm.”²⁷ In response to the leak, “[a] new investigation was immediately launched, which Dunn called Kona II.”²⁸ HP’s general counsel, Ann Baskins, “asked an employment lawyer at the company, Kevin Hunsaker, to head the renewed investigation.”²⁹ “With Hunsaker in day-to-day charge, the investigators undertook their mission with extraordinary zeal,” pretexting phone companies to obtain records for reporters, directors, and employees.³⁰

22. In addition to pretexting, the investigators also took a new approach.³¹ Posing as a disgruntled employee, they emailed Kawamoto with the promise of revealing damaging information about the company.³² Unbeknownst to Kawamoto, the investigators utilized “ReadNotify,” a tracker that, once embedded into an email, allowed them to “track the path [the]

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

message takes, including whether [the] recipient opens the message.”³³ “[A] technique also employed by some e-mail marketers,”³⁴ the investigators hoped that Kawamoto would “forward the e-mail to her source,” thereby revealing who had leaked the confidential information.³⁵

23. ReadNotify failed to yield results, with Kawamoto declining to forward the email.³⁶ But this time around, after combing through the phone records, investigators discovered that a board member, George Keyworth, had a short conversation with Kawamoto right before the article was published.³⁷ After the revelation, the board confronted Keyworth, who admitted to having lunch with the reporter and “say[ing] some nice things about Mike Hurd.”³⁸ The board responded by voting on a motion to request Keyworth’s resignation.³⁹ After the motion passed, a board member who dissented, Mark Perkins, quit in protest.⁴⁰ Keyworth, for his part, refused to step aside, “saying the shareholders had elected him, and he felt the punishment was out of proportion to the offense.”⁴¹

24. Perkins did not go quietly.⁴² After resigning from the board, Perkins retained a lawyer, Viet Denh, who “contacted the S.E.C., the U.S. Attorney’s offices in Manhattan and San Francisco, the California Attorney General, the F.C.C., and the F.T.C.”⁴³

³³ Robert McMillan, *HP’s e-mail tracer in widespread use*, COMPUTERWORLD (Oct. 10, 2006), <https://www.computerworld.com/article/2820287/hp-s-e-mail-tracer-in-widespread-use.html>

³⁴ *Id.*

³⁵ Joris Evers, *How HP bugged e-mail*, CNET (Sept. 29, 2006), <https://www.cnet.com/news/privacy/how-hp-bugged-e-mail/>.

³⁶ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007), <https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

25. Once HP's tactics were made public, the reaction was swift and overwhelming. In September 2006, Congress held a hearing on the scandal, asking Dunn and other witnesses to answer two questions: "Exactly what did they know about the use of pretexting," and "[w]hat did they know about planting spyware on an email to a journalist."⁴⁴ The witnesses verified that investigators employed both methods to gather evidence, but they maintained that their conduct was lawful.⁴⁵ Throughout the hearing, members of Congress called for a law that would prohibit these practices, with one member remarking that "[t]he growing market for personal information is enormous, and many of us have seen this, and that is why we need to pass legislation to stop this."⁴⁶ When another member asked Dunn whether it "strike[s] you as a permissible tactic to use, attaching a tracking device onto an e-mail," Dunn replied, "[i]t is kind of surprising that it is legal, isn't it?"⁴⁷ Still another member lamented that email trackers were "equivalent to going through the mail in my mailbox."⁴⁸

26. Six days after the hearing, the California Attorney General indicted Dunn, Hunsaker, DeLia, and two private investigators involved in both iterations of Project Kona.⁴⁹ A few months after that, Congress passed the Telephone Records and Privacy Protection Act of 2006, a law that criminalizes "knowingly and intentionally obtain[ing], or attempt[ing] to obtain, confidential phone records information of a covered entity, by making false or fraudulent

⁴⁴ Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 109th Cong. 45 (2006), <https://www.govinfo.gov/content/pkg/CHRG-109hhr31472/html/CHRG-109hhr31472.htm>.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007), <https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

statements or representations to an employee of a covered entity.” 18 U.S.C. § 1039(a)(1). That law, as the text suggests, only prohibits pretexting, not the use of email trackers.

27. After Congress enacted the TRPA, the Arizona legislature went a step further, passing a law that addressed *both* methods used by HP’s investigators. Like the federal law, this new Arizona law prohibits any person from procuring or conspiring with another to procure “a telephone record” of residents without consent. But, in addition, the new law also prohibits procurement of any “communication service record” (including email records) of “any resident of this state without the authorization of the customer to whom the record pertains, or by fraudulent, deceptive, or false means.” Ariz. Rev. Stat. Ann. § 44-1376.01. And while Congress declined to include a private right of action in the federal law, the Arizona legislature allowed residents to pursue civil remedies. Ariz. Rev. Stat. Ann. § 44-1376.04(2).

B. Email Pixels

28. Not much has changed between 2008 and today. Despite Arizona law prohibiting the practice, companies still embed trackers within emails without first obtaining consumers’ consent. Indeed, “[a] 2018 Princeton study on email tracking tested over 12,000 emails from 900 senders offering mailing list subscriptions and found that 70% contained trackers.”⁵⁰

29. These trackers, known as “spy pixels,” enable companies to learn information about the email transfer, including when and where the email was opened.

⁵⁰ Mikael Berner, *The Business of Email Tracking: What To Know About Spy Pixels In Your Inbox*, FORBES (Jun 9, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/06/09/the-business-of-email-tracking-what-to-know-about-spy-pixels-in-your-inbox/?sh=2084ee793fec>.

30. A spy pixel is typically a 1x1 (one pixel high by one pixel long) image. “The spy pixel is so small it is basically impossible to see with the naked eye.”⁵¹

31. To activate a spy pixel, recipients need only to open the email.

C. Defendant’s Spy Pixel Tracking

32. Defendant uses “richrelevance,” an email tracking system offered by Algonomy, a “customer data and analytics platform.”⁵² This can be seen in a snippet of the HTML code in one of Defendant’s emails.

```

```

33. At a minimum, this tracker permits Defendant to procure information including information about when and whether a customer opens and reads an email.

34. Defendant incorporates richrelevance into its emails so it can “[m]ap individual shopper behavior with granular segmentation to drive personalized campaigns.”⁵³

35. Defendant also uses its own spy pixel to track when customers open their emails. That tracker records the email address, the subject of the email, and when the email is opened and read.

⁵¹ Becky Willeke, *Spy pixels are hiding in your emails; so what can you do about it?*, FOX 2 NOW (Mar. 15, 2021), <https://fox2now.com/news/tech-talk/spy-pixels-are-hiding-in-your-emails-so-what-can-you-do-about-it/>.

⁵² Algonomy, <https://algonomy.com/>.

⁵³ Algonomy, *Personalized Marketing and Customer Journeys*, (Nov. 17, 2023), <https://algonomy.com/omnichannel-personalization/marketing-personalization/>.

36. Defendant embedded spy tracking pixels in marketing emails Defendant sent to Plaintiff. Defendant utilized a tracking system to determine the time and place their marketing emails were opened.

37. Plaintiff was unaware that tracking pixels were embedded in the emails. Defendant never received consent from Plaintiff and Class Members to use these spy pixels.

CLASS ACTION ALLEGATIONS

38. Plaintiff seeks to represent a class (the “Class”) defined as: All persons in the State of Arizona who have opened a marketing email containing a tracking pixel from Defendant.

39. Excluded from the Class are Defendant, its subsidiaries, affiliates, officers, directors, assigns and successors, and any entity in which it has a controlling interest, and the Judge to whom this case is assigned and any member of his or her immediate family.

40. 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 hundreds of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but will 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 and third-party retailers and vendors.

41. 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:

- a) whether Defendant “[k]nowingly procure[d], attempt[ed] to procure, solicit[ed] or conspire[d] with another to procure a ... communication service record of any resident of this state without the authorization of the customer to whom the record

pertains or by fraudulent, deceptive or false means” in violation of A.R.S. § 44-1376 *et seq.*;

- b) whether Plaintiff’s and the Class’s “communication service records” were procured, sold or received in violation of A.R.S. § 44-1376 *et seq.*
- c) whether Defendant’s conduct violates A.R.S. § 44-1376 *et seq.* or any other applicable laws; and
- d) whether, as a result of Defendant’s misconduct as alleged herein, Plaintiff and Class members are entitled to restitution, injunctive, and/or monetary relief and, if so, the amount and nature of such relief.

42. Plaintiff’s claims are typical of the claims of Class members because Plaintiff, like all Class members, had her communication service records procured, sold, or received by Defendant.

43. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained counsel competent and experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and her counsel.

44. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant’s liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also

presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I
Violation of A.R.S. § 44-1376.01

45. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

46. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

47. Defendant embeds spy pixels in its marketing emails sent to Plaintiff and Class members.

48. The spy pixels are designed to extract "communication service records" related to the delivery of the email the spy pixel is embedded in. This includes, but is not limited to, time logs of email access, associated email addresses, email client type, email path data, IP addresses, and device information.

49. Defendant "procures" Plaintiff's and Class members' "communication service records" because they "obtain by any means, including electronically" Plaintiff and Class member's "communication service records" as defined in A.R.S. § 44-1376.

50. In contravention of A.R.S. § 44-1376.01, Defendant knowingly procures "subscriber information, including name, billing or installation address, length of service, payment method, telephone number, electronic account identification and associated screen names, toll bills

or access logs, records of the path of an electronic communication between the point of origin and the point of delivery and the nature of the communication service provided, such as ... electronic mail ...,” which constitute “communication service records” under A.R.S. § 44-1376, from Plaintiff and Class members.

51. Plaintiff and Class members were never informed by Defendant, and thus never knew, that Defendant would be procuring sensitive information including, but not limited to, time logs of email access, associated email addresses, email client type, email path data, IP addresses, and device information.

52. Plaintiff and Class members never gave lawful consent to Defendant to procure the communication service records.

53. Each time Defendant sent an email containing a spy pixel, Defendant procured a communication service record, thus committing a separate violation of A.R.S. § 44-1376.01.

54. Defendant invaded Plaintiff’s and Class members’ right to privacy by spying on when they opened and read an email. That conduct also intruded upon their seclusion.

55. Accordingly, Plaintiff, individually and on behalf of the proposed Class, prays for the relief set forth by the statute, including actual damages, profits made by Defendant as a result of the violation, \$1,000 for each violation, reasonable attorneys’ fees and other litigation costs reasonably incurred, and such other equitable relief as the court determines to be appropriate.

REQUEST 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 Class under Fed. R. Civ. P 23 and naming Plaintiff as representative of the Class and Plaintiff’s attorneys as Class Counsel to represent the Class members;

- b. For an order declaring that Defendant's conduct, as set out above, violates A.R.S. § 44-1376.01;
- c. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- d. For actual damages or damages of \$1,000.00 for each of Defendant's violations, whichever is more, pursuant to A.R.S. § 44-1376.04;
- e. For damages equal to the sum of any profits Defendant made for each of Defendant's violations, pursuant to A.R.S. § 44-1376.04;
- f. For injunctive and other equitable relief as is necessary to protect the interests of the Class, including, inter alia, an order requiring Defendant to comply with A.R.S. § 44-1376 *et seq.*
- g. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit;
- h. For pre- and post-judgment interest on all amounts awarded, to the extent allowable; and
- i. For such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: November 27, 2023

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ Yitzchak Kopel
Yitzchak Kopel

Yitzchak Kopel
Israel Rosenberg
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: ykopel@bursor.com
irosenberg@bursor.com

Attorneys for Plaintiff

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Saks.com Unlawfully Embeds Spyware in Marketing Emails, Class Action Alleges](#)
