IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

JACOB SWAIM, individually and on behalf of all others similarly situated, Plaintiff, v. BPS DIRECT, L.L.C. d/b/a BASS PRO SHOPS, Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

COMPLAINT - CLASS ACTION

Plaintiff Jacob Swaim ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant BPS Direct, L.L.C. d/b/a Bass Pro Shops ("Defendant" or "BPS"), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against BPS for wiretapping the electronic communications of visitors to its website, www.basspro.com. BPS procures third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code ("Session Replay Code") on Defendant's website, which then deploys on each website visitor's internet browser for the purpose of watching, intercepting, and recording the website visitor's electronic communications with the BPS website, including their mouse movements, clicks, keystrokes (such as substantive information being entered into an information field or text box), URLs of web pages visited, and other electronic communications in real-time ("Website Communications"). These

third-party vendors (collectively, "Session Replay Providers") create and deploy the Session Replay Code at Defendant's request.

2. After intercepting and capturing the Website Communications, Defendant and the Session Replay Providers use those Website Communications to view in real-time website visitors' entire visit to www.basspro.com. The Session Replay Providers watch the user's behavior while visiting the website and share it with Defendant for analysis. Defendant's procurement of the Session Replay Providers to secretly deploy the Session Replay Code results is the electronic equivalent of "looking over the shoulder" of each visitor to the www.basspro.com website for the entire duration of their website interaction.

3. Defendant's conduct violates the Florida Security of Communications Act ("FSCA"), Fla. Stat. § 934.03, *et. seq*., which is modeled after the Federal Wiretap Act, 18 U.S.C. §§ 2511, *et. seq.,* and constitutes an invasion of the privacy rights of website visitors.

4. The case arises from Defendant's unlawful interception of Plaintiff's and Class members' electronic communications that allow Defendant to watch and record Plaintiff's and the Class members' visits to its website.

5. Businesses have become increasingly adept at tracking users visiting their websites – without their knowledge or consent.

6. The FSCA was enacted in 1969. In 1988, the statute was amended to "extend the protection provided oral communications to communications using new technologies, such as cellular phones, voice mail and computer-to-computer data transfer."[1]

[1]1988 Summary of General Legislation, available at FlSumGenLeg1988.pdf (http://library.law.fsu.edu/Digital-Collections/FLSumGenLeg/FlSumGenLeg1988.pdf) (last accessed Oct. 4, 2022).

7. The amendment to the FSCA was modeled after an amendment to the Federal Wiretap Act, which was amended in 1986 by Title I of the Electronic Communications Privacy Act to extend data and electronic transmissions the same protection already afforded to oral and wire communications. Congress' intent in amending the Federal Wiretap Act is instructive when applying the FSCA.

8. The Wiretap Act was amended by Congress in 1986 because of dramatic changes in telecommunications technologies. [2] Accordingly, in defining "electronic communications[,]" under the Wiretap Act Congress "intended to cover a broad range of communication activities that affect interstate or foreign commerce.... As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire). Communications consisting solely of data, for example, would be electronic communications."[3]

9. Defendant utilized "session replay" code to watch in real-time and intercept Plaintiff's and the Class members' electronic computer-to- computer data communications with Defendant's website, including how they interacted with the website, their mouse movements and clicks, keystrokes, search terms, information they input into the website, and pages and content viewed while visiting the website. Defendant watched, intercepted, stored, and recorded electronic communications regarding the webpages visited by Plaintiff and the Class members, as well as everything Plaintiff and the Class members did on those pages (e.g., what they searched for, what

[2] Sen. Rep. No. 99541, at 1 (1986) available at www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99- 541-1986.pdf.
[3] Hse. Rep. No. 99-647, at 35 (1986) available at www.justice.gov/sites/default/files/jmd/legacy/2013/10/16/houserept-99- 647-1986.pdf.

they looked at, the information they inputted, and what they clicked on), even though that information may never have been submitted by Plaintiffs and Class members.

10. Defendant watched and intercepted the electronic communications at issue without the knowledge or prior consent of Plaintiff or the Class members. Defendant did so for its own financial gain and in violation of Plaintiff's and the Class members' substantive legal privacy rights under the FSCA and Florida common law.

11. To be clear, the "session replay" code that Defendant uses is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer software, a type of device or apparatus if you will, that allows Defendant to contemporaneously watch, intercept, capture, read, observe, re-route, forward, redirect, and receive incoming electronic communications to its website. In addition, Plaintiff's and the Class members' electronic communications are then stored by Defendant using an outside vendor's services, which enables the electronic communications to be viewed again and again and utilized by Defendant to create a session replay, which is essentially a video of a Class member's entire visit to Defendant's website.

12. The technology permits companies like Defendant to view the interactions of visitors on their website in live real-time.

13. The session replay tool is purportedly used to identify broken website features.

14. Defendant does not use session replay for its purported use – as a commonplace analytics tool to improve Plaintiff's and Class members' respective browsing experiences.

15. The extent and detail of the data collected by Defendant far exceeds the stated purpose and Plaintiff's and the Class members' expectations when visiting websites, including Defendant's. The technology not only allows the recording and viewing of the content of Plaintiff's

electronic communications with the website, but also allows the user (Defendant) to create a detailed profile for each visitor to the site – to which Plaintiff and Class members did not consent.

16. The CEO of a major "session replay" software company - while discussing the merger of his company with another "session replay" provider - publicly exposed why companies like Defendant engage in recording visitors to their websites: "The combination of Clicktale and Contentsquare heralds an unprecedented goldmine of digital data that enables companies to interpret and predict the impact of any digital element — including user experience, content, price, reviews and product - - on visitor behavior[.]"[4] This CEO confessed that "this unique data can be used to activate custom digital experiences in the moment via an ecosystem of over 50 martech partners. With a global community of customers and partners, we are accelerating the interpretation of human behavior online and shaping a future of addictive customer experiences."[5]

17. This viewing, collection and storage of page content may cause sensitive information and other personal information displayed on a page to leak to third parties. This exposes website visitors to identity theft, online scams, and other unwanted behavior.

18. Plaintiff brings this action individually and on behalf of a class of all Florida citizens whose Website Communications were watched in real-time and intercepted through Defendant's procurement and use of Session Replay Code embedded on the webpages of www.basspro.com causing them injuries, including violations of their substantive legal privacy rights under the FSCA, invasion of their privacy and exposure of their private information.

---

[4] *See* Contentsquare Acquires Clicktale to Create the Definite Global Leader in Experience Analytics, available at https://www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html; (last accessed Oct. 4, 2022).

[5] *Id.*

19. Plaintiff and Class members seek all civil remedies provided under the causes of action listed below, including but not limited to compensatory, statutory, punitive damages, and attorneys' fees and costs.

20. Plaintiff and Class members seek injunctive relief that will halt Defendant's ongoing unlawful conduct.

PARTIES

21. Plaintiff Jacob Swaim is a citizen of the State of Florida, and at all times relevant to this action, resided and was domiciled in Palm Beach County, Florida. Plaintiff is a citizen of Florida.

22. Defendant BPS Direct, L.L.C. is a limited liability company organized under the laws of Delaware, and its principal place of business is located in Springfield, Missouri. Defendant is a citizen of Missouri.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) 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 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

24. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Florida. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Florida while they were located within Florida. At all relevant times, Defendant knew that its practices would directly result in the real-time viewing and collecting of information from

Florida citizens while those citizens browse www.basspro.com. Defendant chose to avail itself of the business opportunities of marketing and selling its goods in Florida and viewing real-time data from website visit sessions initiated by Floridians while located in Florida, and the claims alleged herein arise from those activities.

25. Defendant also knows that many users visit and interact with Defendant's websites while they are physically present in Florida. Both desktop and mobile versions of Defendant's website allow a user to search for nearby stores by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Defendant is continuously made aware that its website is being visited by people located in Florida, and that such website visitors are being wiretapped in violation of Florida statutory and common law.

26. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

27. The "world's most valuable resource is no longer oil, but data."[6]

28. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data

[6] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

(*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[7] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[8]

29. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[9]

30. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[10] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[11]

31. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license

[7] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (updated Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.
[8] *Id.*
[9] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.
[10] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.
[11] *Id.* at 25.

number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[12]

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

32. Consumers are skeptical and wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[13]

33. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[14] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[15]

34. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

35. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing

---

[12] *Id.*

[13] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

[14] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[15] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[16]

36. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[17]

37. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[18]

C. How Session Replay Code Works.

38. Session Replay Code, such as that implemented on www.basspro.com, enables website operators to view in real—time, record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by watching and recording website visitors "as they click, scroll, type or navigate across different web pages."[19]

39. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of

---

[16] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017),. https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/

[17] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/.

[18] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[19] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to watch and capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.[20] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[21]

40. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by allowing the user to watch the browser by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

41. The types of events watched and captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, substantive text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a later reconstruction of a user's visit accurately, the Session Replay Code must be capable of watching and capturing these events at hyper-frequent intervals, often

[20] *Id.*

[21] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

just milliseconds apart. Events are typically contemporaneously accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

42. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

43. A website operator can view the browser's activity contemporaneously and the events from a user session are recorded by a Session Replay Code, so that a website operator can also later view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[22]

44. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be watched in real-time and captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[23]

45. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter"

[22] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
[23] *Id.*

button on the website, the Session Replay Code allows it to be viewed in real-time and causes the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

46. Session Replay Code does not necessarily anonymize user sessions, either.

47. First, if a user's entry of personally identifying information is captured in an event response, that data will be viewed and become known and visible to both the Session Replay Provider and the website owner.

48. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

49. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[24]

50. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

51. When a user eventually identifies him or herself to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited,

[24] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Oct. 4, 2022).

including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

52. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[25] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [ ] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[26]

53. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[27] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[28]

---

[25] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

[26] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

[27] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.

[28] *Id.*

D. Defendant Secretly Wiretaps Its Website Visitors' Electronic Communications.

54. Defendant owns and operates the website www.basspro.com. Defendant is an online and brick-and-mortar retailer for outdoor products, such as hunting gear and apparel, and camping equipment.

55. However, unbeknownst to Plaintiff and the millions of individuals perusing Defendant's products online, Defendant intentionally procures and embeds various Session Replay Codes from Session Replay Providers on its website to watch, track and analyze website user interactions with www.basspro.com.

56. One such Session Replay Provider that Defendant procures is Microsoft.

57. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.[29]

58. Defendant's procurement and use of Microsoft's tool, the Clarity's Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, is a wiretap in violation Florida statutory and common law.

E. Plaintiff and Class Members' Experience.

59. During the past year, Plaintiff has visited www.basspro.com several times a week.

60. Plaintiff visited the website on his computer while in Florida.

61. During his visits to the website, Plaintiff, through his computer and/or mobile device, transmitted electronic communications in the form of instructions to Defendant's computer

[29] Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity, (last visited Oct. 4, 2022).

servers utilized to operate the website. The commands were sent as messages instructing Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff. The communications sent by Plaintiff to Defendant's servers included, but were not limited to, the following actions taken by Plaintiff while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff, pages and content viewed by Plaintiff, scroll movements, and copy and paste actions.

62. Defendant responded to Plaintiff's electronic communications by supplying - through its website - the information requested by Plaintiff. This series of requests and responses — whether online or over the phone — constitutes electronic communication under the FSCA.

63. While visiting Defendant's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.basspro.com.

64. Unknown to Plaintiff, Defendant procures and embeds Session Replay Code on its website.

65. During the website visits, Plaintiff's Website Communications were watched in real-time and captured by Session Replay Code and sent to various Session Replay Providers.

66. When visiting www.basspro.com, if a website user looks at product, that information is captured by the Session Replay Codes embedded on the website.

67. And, when you select a store closest to you in order to view inventory and schedule in-store pick-up, that substantive information is viewed and sent to Service Replay Providers.

68. The wiretapping by the Session Replay Codes are ongoing during the visit and intercepts the contents of these communications between Plaintiff and Defendant with instantaneous transmissions to the Session Replay Provider in which only 33 milliseconds were

required to send a packet of event response data, which would indicate everything the website user had just done.

69. The Session Replay Codes operate in the same manner for all putative Class members.

70. Like Plaintiff, each Class member visited www.basspro.com with Session Replay Code embedded in it, and those Session Replay Codes watched and intercepted the Class members' Website Communications with www.basspro.com by sending hyper-frequent logs of those communications to Session Replay Providers.

71. Even if Defendant masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

72. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

73. As a specific example, if a user types a product into Defendant's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Defendant will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

74. Plaintiff reasonably expected that his visits to Defendant's website would be private and that Defendant would not be watching, tracking, and recording Plaintiff as he browsed and interacted with the website, particularly because Plaintiff was never presented with any type of pop-up disclosure or consent form alerting Plaintiff that his visits to the website were being watched and recorded by Defendant. Moreover, he used his own personal device to communicate with the website, was not aware of anyone else present during the communication and presumed his private interactions with Defendant's website were just that – private.

75. Plaintiff reasonably believed that he was interacting privately with Defendant's website, and not that he was being watched and recorded and that those recordings could later be watched again and again by Defendant's employees, or worse yet, live while Plaintiff was on the website.

76. Defendant has had embedded within its website code and has continuously operated at least one session replay script that was provided by a Session Replay Provider. The session replay code is analogous to an electronic or mechanical device or apparatus in that it was always active, watching, intercepting and recording every incoming data communication to Defendant's website the moment Plaintiff or any visitor accessed the site.

77. The Session Replay Providers that provided the session replay code to Defendant are not providers of wire or electronic communication services, or an internet service provider.

78. Defendant is not a provider of wire or electronic communication services, or an internet service provider.

79. Defendant utilized session replay code to intentionally and contemporaneously watch and intercept the substance and content of Plaintiff's electronic communications with Defendant's website, including mouse clicks and movements, keystrokes, search terms, substantive

information inputted by Plaintiff, pages and content viewed by Plaintiff, and scroll movements, and copy and paste actions. In other words, Defendant intercepted, stored, and recorded the webpages visited by Plaintiff, as well as everything Plaintiff did on those pages, what Plaintiff searched for, what Plaintiff looked at, and the information Plaintiff inputted.

80. The Session Replay Providers intentionally utilized by Defendant contemporaneously watched and intercepted the content of electronic computer-to-computer data communications between Plaintiff's computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website - as the communications were transmitted from Plaintiff's computer and/or mobile device to Defendant's computer servers and hardware – and while viewing, copied and sent and/or re-routed the communications to a storage file within the Session Replay Provider(s)' server(s). The intercepted data was transmitted contemporaneously to the Session Replay Provider(s) server(s) as it was sent from Plaintiff's computer and/or mobile device.

81. The session replay code utilized by Defendant acts as an electronic, mechanical or other analogous device or apparatus in that the session replay code monitors, intercepts and records the content of electronic computer-to-computer communications between Plaintiff's computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website.

82. The session replay code utilized by Defendant is not a website cookie, standard analytics tool, tag, web beacon, or other similar technology.

83. The data collected by Defendant identified specific information inputted and content viewed, and thus revealed personalized and sensitive information about Plaintiff's Internet activity and habits.

84. The electronic communications intentionally watched and intercepted by Defendant was content generated through Plaintiff's intended use, interaction, and communication with Defendant's website relating to the substance and/or meaning of Plaintiff's communications with the website, i.e., mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff, and pages and content clicked on and viewed by Plaintiff. This information is "content" as defined by the FSCA and is not merely record information regarding the characteristics of the message that is generated in the course of the communication, nor is it simply information disclosed in the referer headers. The mere fact that Defendant values this content, monitors, intercepts and records it, confirms these communications are content that convey substance and meaning to Defendant.

85. The electronic communications intentionally intercepted by Defendant were not generated automatically and were not incidental to Plaintiff's communications.

86. The session replay code utilized by Defendant watched, intercepted, copied, replicated, and sent the data in a manner that was undetectable by Plaintiff.

87. The session replay technology utilized by Defendant gave Defendant the ability to view Plaintiff's website visits live in real-time as they were occurring and intercept the content of these electronic communications as they were occurring, which is exactly what Defendant did.

88. These electronic data communications were not only watched in real-time, intercepted contemporaneously with transmission and stored, but could also be used by Defendant to create a video playback of Plaintiff's visit to the website. Defendant's contemporaneous interception of Plaintiff's electronic communications during transmission allowed Defendant to observe, capture, and divulge Plaintiff's personal interests, browsing history, queries, and habits as he interacted with and browsed Defendant's website in real-time.

89. Defendant similarly intercepted the electronic communications of at least thousands of other individuals located in Florida who visited Defendant's website.

90. Defendant did not utilize a telephone or telegraph instrument, equipment, or facility to intercept Plaintiff's and the Class members' electronic communications at issue. Rather, Defendant utilized a code embedded within its website to watch and intercept the communications at issue. By the very nature of its operation, said code is the equivalent of a device or apparatus used to intercept wire or electronic communications.

91. The electronic communications intercepted by Defendant did not originate from an electronic or mechanical device which permits the tracking of the movement of a person or an object.

92. Defendant never alerted or asked Plaintiff or the Class Members for permission to watch, intercept and record their visits to Defendant's website using "session replay" code.

93. Plaintiff and the Class members never consented to being watched or having their electronic communications on Defendant's website intercepted by Defendant or anyone acting on Defendant's behalf, and they were never given the option to opt out of Defendant's surreptitious watching and recording.

94. Plaintiff and the Class members never provided Defendant, its employees, or agents with consent to watch and intercept and record their electronic communications using "session replay" code.

95. Plaintiff and the Class members did not specifically, clearly, and unmistakably consent to Defendant's watching, interception and recording of their electronic communications using "session replay" code.

96. Plaintiff and the Class members did not specifically, clearly, and unmistakably consent to Defendant's interception and recording of their visits to Defendant's website using "session replay" code.

97. Plaintiff and the Class members did not have a reasonable opportunity to discover Defendant's unlawful interceptions because Defendant did not disclose that it was watching their activity, nor did Defendant disclose its interception, nor did it seek consent from Plaintiff and the Class members prior to interception of their communications.

98. Plaintiff and the Class members never clicked or otherwise agreed to any disclosure or consent form authorizing Defendant to watch and intercept Plaintiff's and the Class members' electronic communications using "session replay" code.

99. Defendant intercepted Plaintiff's and the Class members' electronic communications from the moment they landed on Defendant's website, and before they had an opportunity to even consider consenting or agreeing to any privacy or terms of use policy on the website. Defendant's unlawful watching and interception occurred before Plaintiff and the Class members were given an opportunity to review, let alone consent, to any language that Defendant may claim purportedly authorized its violations of the FSCA.

100. Defendant's website failed to explicitly alert or otherwise notify Plaintiff and the Class members that Defendant would be utilizing session replay code to monitor and record their interactions with Defendant's website.

101. Upon immediately landing on Defendant's website, Plaintiff and the Class members were not alerted that by entering the website Defendant would unilaterally attempt to bind them to Defendant's terms and policies or privacy policy. Indeed, the landing page to Defendant's website not only fails to advise visitors that Defendant is intercepting their electronic communications, but

also does not contain any type of conspicuous disclosure regarding Defendant's terms of use or privacy policy.

102. Plaintiff and the Class members were not immediately required to click on any box or hyperlink containing Defendant's terms of use or privacy policy upon visiting the website or in order to navigate through the website.

103. Plaintiff and the Class members were not placed on notice of Defendant's terms and policies or privacy policy upon immediately visiting the website. Instead, Defendant's terms of use and privacy policy are buried at the bottom of Defendant's website where Plaintiff and the Class members were unable to see them.

104. Defendant does not require visitors to its website to immediately and directly acknowledge that the visitor has read Defendant's terms of use or privacy policy before proceeding to the site. In other words, Defendant's website does not immediately direct visitors to the site to the terms of use or privacy poli and does not require visitors to click on a box to acknowledge that they have reviewed the terms and conditions/policy in order to proceed to the website.

105. There is no cookie banner that Plaintiff and Class members must affirmatively ex out of for it to no longer be visible on the Defendant’s website.

106. Defendant's entire website, including its terms of use and privacy policy, are silent on Defendant's use of “session replay” code to watch, monitor and record Plaintiff's and the Class member's (1) mouse clicks and movements; (2) keystrokes; (3) search terms; (4) substantive information inputted into the website; and (5) pages and content viewed.

107. Defendant's use of a session replay code to intercept Plaintiff's electronic communications in real-time did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's electronic communications with Defendant's website.

108. Defendant's use of session replay code was not instrumental or necessary to the operation or function of Defendant's website or business.

109. Defendant's use of a session replay code to contemporaneously intercept Plaintiff's electronic communications at the time of transmission was not instrumental or necessary to Defendant's provision of any of its goods or services. Rather, the level and detail of information surreptitiously collected by Defendant indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its website, and the information collected was solely for Defendant's own benefit.

110. At least one of the purposes for Defendant to watch and intercept Plaintiff's and the Class members' electronic communications was to allow Defendant to learn of Plaintiff's and the Class members' personal preferences, which would then be used to market Defendant's services and goods to Plaintiff and the Class members.

111. Plaintiff and the Class members had a reasonable expectation of privacy during their visits to Defendant's website, which Defendant violated by intentionally monitoring and intercepting the content of their electronic communications with the website.

112. The purpose of the FSCA is to protect every person’s right to privacy and to prevent the pernicious effect on browsers who would otherwise feel insecure from intrusion into their browsing activity.

113. Defendant's covert monitoring and interception of Plaintiff's and the Class members' electronic communications caused Plaintiff and the Class members harm, including violations of their substantive legal privacy rights under the FSCA, invasion of privacy, invasion of their rights to control information concerning their person, and/or the exposure of their private information. Moreover, Defendant's practices caused harm and a material risk of harm to Plaintiff's

and the Class Members' privacy and interest in controlling their personal information, habits, and preferences.

CLASS ACTION ALLEGATIONS

114. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> All natural persons in Florida who visited www.basspro.com and whose Website Communications were watched and captured in Florida without their consent through the use of Session Replay Code embedded in Defendant's website.

115. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action. Plaintiff reserves the right to modify or amend the Class definitions, as appropriate, during the course of this litigation.

116. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Defendant or the Session Replay Providers.

117. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant procures Session Replay Providers to watch in real time and intercept Defendant's website visitors' Website Communications; (b) whether Defendant intentionally discloses the intercepted Website Communications of its website users; (c) whether Defendant acquires the contents of website users' Website Communications without their consent; (d) whether Defendant's conduct violates the FSCA, Fla. Stat. § 934.03, *et. seq*.; (e) whether Plaintiff and the Class members are entitled to

equitable relief; and (f) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

118. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

119. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the interests of the other members of the Class.

120. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

121. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

122. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through BPS's books and records or the Session Replay Providers' books and records.

COUNT I
Florida Security of Communications Act
Fla. Stat. § 934.03, *et. seq*.

123. Plaintiff incorporates paragraphs 1-122 as if fully set forth herein.

124. Plaintiff brings this claim individually and on behalf of the Class.

125. The FSCA creates civil liability for anyone who "[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Fla. Stat. § 934.03(1)(a).

126. The FSCA creates further liability for anyone who "[i]ntentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection[.]" Fla. Stat. § 934.03(1)(d).

127. Thus, the FSCA prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was

obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. Fla. Stat. § 934.03.

128. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. Fla. Stat. § 934.10.

129. As used in the FSCA, "intercept" means the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Fla. Stat. § 934.02(3).

130. "Contents" when "used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." Fla. Stat. § 934.02(7).

131. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." Fla. Stat. § 934.02(5).

132. Under the FSCA, "contents" includes, but is not limited to, "any information concerning the substance, purport, or meaning of that communication." Fla. Stat. § 934.02(7).

133. The FSCA defines "electronic communication" as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects intrastate, interstate, or foreign commerce [.]" Fla. Stat. §934.02(12).

134. BPS is a person for purposes of the FSCA because it is a corporation.

135. Session Replay Code like that procured by Defendant is a "device" or "apparatus" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the FSCA. Fla. Stat. §934.02(3) and (04). Courts unanimously hold that software constitutes a "device" for purposes of applying wiretap statues. *See, e.g*, *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (accepting that a keylogger software could be considered a device); *Luis v. Zang,* 833 F.3d 619, 630 (6th Cir. 2016) (accepting that a software could be a "device" for the purpose of the Wiretap Act); *In re Carrier IQ, Inc.,* 78 F. Supp. 3d 1051, 1087 (N.D. Cal. 2015) (concluding that a software was an "electronic, mechanical or other device"); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661-62 (E.D. Ten. 2012) (analyzing spyware software as a device under Wiretap Act); *Shefts v. Petrakis*, 2012 U.S. Dist. LEXIS 130542, 2012 WL 4049484, at *8-9 (C.D. Ill. 2012) (analyzing software as a device under the Wiretap Act).

136. Plaintiff's and Class members' intercepted Website Communications constitute the "contents" of electronic communication[s]" within the meaning of the FSCA.

137. Defendant intentionally procures and embeds Session Replay Code on its website to secretly watch and intercept its website visitors' electronic interactions communications with Defendant in real time.

138. Plaintiff's and Class members' electronic communications are watched and intercepted contemporaneously with their transmission.

139. Plaintiff and Class members did not consent to having their Website Communications wiretapped.

140. Defendant violated § 934.03(1)(a) of the FSCA by intentionally intercepting Plaintiff's and the Class members' electronic communications when they visited Defendant's website.

141. Defendant intentionally intercepted Plaintiff's and the Class members' electronic communications without their prior consent.

142. Defendant uses or attempts to use the electronic communications it views and intercepts in order to market its services and goods to Plaintiff and the Class members.

143. Plaintiff and the Class members had a reasonable expectation of privacy during their visits to Defendant's website, which Defendant violated by intentionally monitoring and intercepting their electronic communications with the website.

144. Pursuant to Fla. Stat. § 934.10, Plaintiff and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of $100 a day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

145. BPS' conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
Invasion of Privacy – Intrusion

146. Plaintiff incorporates paragraphs 1-122 as if fully set forth herein.

147. Florida common law recognizes the tort of invasion of privacy, and specifically, intrusion.

148. Plaintiff brings this claim individually and on behalf of the Class.

149. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

150. Plaintiff and Class members did not consent to, authorize, or know about Defendant's intrusion at the time it occurred. Plaintiff and Class members never agreed that Defendant could monitor, intercept, collect or disclose their Website Communications.

151. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information monitored in real-time, intercepted and utilized for business gain.

152. Defendant's conduct constitutes an intentional electronic intrusion on Plaintiff's and Class members' private life, without consent.

153. Plaintiff and Class members reasonably expected to browse on their laptops and mobile devices without "Big Brother" a/k/a Defendant monitoring every move. Defendant electronically intruded into Plaintiff's and Class members' private quarters,

154. By surreptitiously watching and intercepting Plaintiff and the Class members' digital data, Defendant has wrongfully intruded into Plaintiff and the Class members' private quarters, being their digital footprint and computer, and the private use of their computers and/or mobile devices.

155. Defendant's conduct is highly offensive to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

156. Defendant's intrusion is so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency.

157. Plaintiff and Class members were harmed by Defendant's wrongful conduct as Defendant's conduct has caused Plaintiff and the Class members mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

158. Defendant's conduct has needlessly harmed Plaintiff and the Class members by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class members to experience mental anguish, emotional distress, worry, fear, and other harms.

159. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

160. Further, Defendant has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

161. As a direct and proximate result Defendant's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

162. Defendant's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
Invasion of Privacy – Public Disclosure of Private Facts

163. Plaintiff incorporates paragraphs 1-122 as if fully set forth herein.

164. Florida common law recognizes the tort of invasion of privacy, and specifically, public disclosure of private facts.

165. Plaintiff brings this claim individually and on behalf of the Class.

166. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

167. Defendant monitored and collected Plaintiff's and Class members' Website Communications that contained private facts that Plaintiff and Class members wanted kept private.

168. Plaintiff and Class members did not consent to, authorize, or know about Defendant's intrusion at the time it occurred. Plaintiff and Class members never agreed that Defendant could monitor, collect, disclose, utilize or publish their Website Communications.

169. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted, disseminated, and utilized for business gain.

170. Defendant has publicized this information for its own gain.

171. By intercepting Plaintiff's and the Class members' digital data, and utilizing it for marketing purposes, Defendant has wrongfully disclosed the Plaintiff and the Class members' private facts that are not of public concern.

172. Defendant's conduct is highly offensive to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

173. The digital footprint and Website Communications of Plaintiff and the Class members are not of public concern.

174. Plaintiff and Class members were harmed by Defendant's wrongful conduct as Defendant conduct has caused Plaintiff and the Class members mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

175. Defendant's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

176. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

177. Further, Defendant has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

178. As a direct and proximate result Defendant's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

179. Defendant's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT IV
Declaratory and Injunctive Relief

180. Plaintiff incorporates paragraphs 1-122 as if fully set forth herein.

181. Under the FSCA, Plaintiff and the Class members are entitled to "[p]reliminary or equitable or declaratory relief as may be appropriate[.]" Fla. Stat. § 934.10(1)(a).

182. Plaintiff and the Class members seek a declaration that Defendant's use of session replay code as alleged herein violates the FSCA.

183. Pursuant to § 934.10(1)(a), Plaintiff and the Class members seek an injunction prohibiting Defendant from utilizing session replay code to monitor and record visits to its website without first securing consent.

184. Defendant's ongoing and continuing violations have caused, and in the absence of an injunction will continue to cause, harm to Plaintiff and the Class members.

185. Plaintiff and the Class members will suffer irreparable harm if Defendant is permitted to continue its practice of recording website visits utilizing session replay code.

186. The injuries that the Plaintiff and the Class members will suffer if Defendant is not prohibited from continuing to engage in the illegal practices described herein far outweigh the harm that Defendant will suffer if it is enjoined from continuing this conduct.

187. The public interest will be served by an injunction prohibiting Defendant from continuing to engage in the illegal practices described herein.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully request that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: October 5, 2022

Respectfully submitted,

/s/ Jonathan B. Cohen
Jonathan B. Cohen (FL Bar No. 27620)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
3833 Central Ave.
St. Petersburg, FL 33713
Phone: (813) 786-8622
Email: jcohen@milberg.com

MaryBeth V. Gibson *(pro hac vice forthcoming)*
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, Georgia 30305
T: (404) 978-6971 / F: (404) 320-9978
MGibson@TheFinleyFirm.com

ClassAction.org
