UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

TIMOTHY ARNDT, *individually and on behalf of all others similarly situated*, Plaintiff, v. GOVERNMENT EMPLOYEES INSURANCE COMPANY, Defendant.	Case No. **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Timothy Arndt brings this class action against Defendant Government Employees Insurance Company ("Geico") and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation on conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. "Since the advent of online behavioral advertising ('OBA') in the late 1990s, businesses have become increasingly adept at tracking users visiting their websites." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 111 (W.D. Pa. 2019) (citations omitted). This case involves one of the most egregious examples of such consumer tracking and Internet privacy violations.

2. Plaintiff brings this case as a class action under the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. 5701, *et seq.* ("WESCA") and the Maryland Wiretapping and Electronic Surveillance Act, Md. Code. Ann., Cts. & Jud. Proc. § 10-401 ("MWESA"). The case stems from Defendant's unlawful procurement of the interception of

Plaintiff's and Class members' electronic communications through the use of third party "session replay" spyware that allowed Defendant to surreptitiously watch and record Plaintiff's and the Class members' communications when they filled out online forms requesting quotes from Defendant.

3. As discussed in detail below, Defendant procured and utilized "session replay" spyware from third party Session Replay Providers, namely Quantum Metric, who contemporaneously intercepted Plaintiff's and the Class members' electronic computer-to-computer data communications with Defendant's website, including every interaction they had with the online forms, their mouse movements and clicks when selecting answers to personal questions, and keystrokes and PII inputted into the website form answers like their gender identity, accident history, and social security number. Defendant facilitated a third party's interception, recording, processing and storage of electronic communications created through the online forms filled out by Plaintiff and the Class members, as well as everything Plaintiff and the Class members did on those form pages.

4. Defendant knowingly and intentionally procured undisclosed third parties to intercept 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' rights to be free of intrusion upon their private affairs and to control information concerning their person under WESCA and the MWESA.

5. The third party "session replay" spyware procured and utilized by Defendant is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer software that allows the Session Replay Provider to contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive incoming electronic communications to

Defendant's website. Plaintiff's and the Class members' electronic communications are then interpreted, reproduced, and stored at Defendant's behest using outside vendor(s)'s services and can later be viewed and utilized by Defendant as a session replay, which is essentially a video-like formulation of a Class member's entire visit to Defendant's website, including all of their actions.

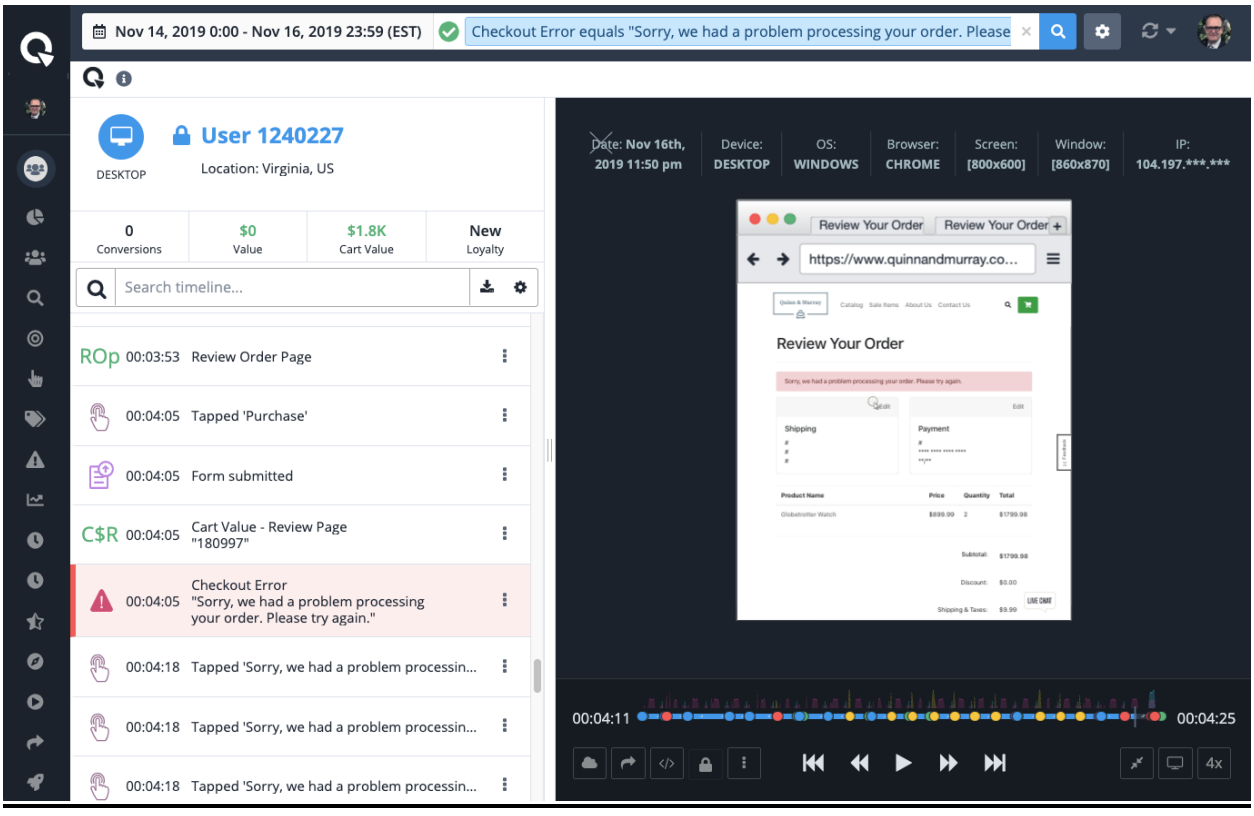
6. "Technological advances[,]" such as Defendant's use of session replay technology, "provide 'access to a category of information otherwise unknowable' and 'implicate privacy concerns' in a manner different from traditional intrusions as a 'ride on horseback' is different from 'a flight to the moon.'" *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)).

7. 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[.]" *See Contentsquare Acquires Clicktale to Create the Definite Global Leader in Experience Analytics*, available at www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html (last accessed May 10, 2021) (emphasis supplied). This CEO further admitted 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***." *Id*. (emphasis supplied).

8. Unlike typical website analytics services that provide aggregate statistics, the third party session replay technology utilized by Defendant is intended to record and capture electronic communications on Defendant's website and then process those communications to create a playback of individual browsing sessions, as if someone is looking over a Class members' shoulder when visiting Defendant's website. The technology also permits companies like Defendant to view the interactions of visitors on their website in real-time.

9. The following screenshot provides an example of a typical recording of a visit to a website captured utilizing session replay software, which includes mouse movements, keystrokes and clicks, search terms, content viewed, and personal information inputted by the website visitor:

QUANTUM METRIC:



10. The purported use of session replay technology is to monitor and discover broken website features. However, the extent and detail of the data collected by Defendant's Session Replay Provider for users of the technology, such as Defendant, far exceeds the stated purpose and Plaintiff's and the Class members' reasonable expectations (and any potential consent they may have provided) when visiting websites like Defendant's. The technology not only allows the recording and viewing of a visitor's detailed electronic communications with a website, but also allows the user and Session Replay Provider to create a detailed, historical profile for each visitor to the site. Indeed, in an ongoing patent dispute, a well-known session replay provider openly admitted that this type of technology is utilized by companies like Defendant to make a profit: **"[the] software computes billions of touch and mouse movements and transforms this knowledge into profitable actions that increase engagement, reduce operational costs, and maximize conversion rates (i.e., the percentage of users who take desired actions on a website, such as purchasing a product offered for sale)**." *Content Square SAS v. Quantum Metric, Inc.,* Case No. 1:20-cv-00832-LPS, Compl. at ¶8, [DE 1] (D. Del. Jun. 22, 2020) (emphasis supplied).

11. Moreover, the collection and storage of page content may cause sensitive information inputted into the website form and other personal information displayed on a page to leak to additional third parties. This may expose website visitors to identity theft, online scams, and other unwanted behavior.

12. Indeed, the news is replete with examples of the dangers of Session Replay Code. For example, in 2019, the App Analyst, a mobile expert who writes about his analyses of popular apps, found that Air Canada's iPhone app wasn't properly masking the session replays they were

sent, exposing unencrypted credit card data and password information.[1] This discovery was made just weeks after Air Canada said its app had a data breach, exposing 20,000 profiles.[2]

13. Further, multiple companies have removed Session Replay Code from websites after it was discovered the Session Replay Code captured highly sensitive information. For instance, in 2017, Walgreens stopped sharing data with a Session Replay Provider after it was discovered that the Session Replay Provider gained access to website visitors' sensitive information.[3] Indeed, despite Walgreens' extensive use of manual redactions for displayed and inputted data, the Session Replay Provider still gained access to full names of website visitors, their medical conditions, and their prescriptions.[4]

14. Following the Walgreens incident, Bonobos, a men's clothing retailer, announced that it was eliminating data sharing with a Session Replay Provider after it was discovered that the Session Replay Provider captured credit card details, including the cardholder's name and billing address, and the card's number, expiration, and security code from the Bonobos' website.[5]

15. In 2019, Apple warned application developers using session replay technology that they were required to disclose such tracking and recording to their users, or face being immediately removed from the Apple Store: "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

---

[1] Zach Whittaker, *Many Popular iPhone Apps Secretly Record Your Screen Without Asking*, TechCrunch (Feb. 6, 2019), https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/.
[2] *Id.*
[3] Nitasha Tiku, *The Dark Side of 'Replay Sessions' That Record Your Every Move Online*, WIRED (Nov. 16, 2017), https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/.
[4] Englehardt, *supra* note 17.
[5] Tiku, *supra* note 25.

visual indication when recording, logging, or otherwise making a record of user activity." https://techcrunch.com/2019/02/07/apple-glassbox-apps/ (last visited November 15, 2021).

16. Consistent with Apple's concerns, countless articles have been written about the privacy implications of recording user interactions during a visit to a website, including the following examples:

(a) ***The Dark Side of 'Replay Sessions' That Record Your Every Move Online***, located at https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/ (last visited Nov. 14, 2022);

(b) ***Session-Replay Scripts Disrupt Online Privacy in a Big Way***, located at https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/ (last visited Nov. 14, 2022);

(c) ***Are Session Recording Tools a Risk to Internet Privacy?***, located at https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/ (last visited Nov. 14, 2022);

(d) ***Session Replay is a Major Threat to Privacy on the Web***, located at https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720 (last visited Nov. 14, 2022);

(e) ***Session Replay Scripts Could be Leaking Sensitive Data***, located at https://medium.com/searchencrypt/session-replay-scripts-could-be-leaking-sensitive-data-5433364b2161 (last visited Nov. 14, 2022);

(f) ***Website Owners can Monitor Your Every Scroll and Click***, located at https://www.digitalinformationworld.com/2020/02/top-brands-and-websites-can-monitor-your-every-scroll-and-click.html (last visited Nov. 14, 2022); and

(g) ***Sites Using Session Replay Scripts Leak Sensitive User Data***, located at https://www.helpnetsecurity.com/2017/11/20/session-replay-data-leak (last visited Nov. 14, 2022).

17. In sum, Defendant procured the interception of the electronic communications of Plaintiff and the Class members through their visits to its website and filling of the online quote forms, causing them injuries, including violations of their substantive legal privacy rights under WESCA and the MWESA, invasion of their privacy, intrusion upon their seclusion, unlawful dissemination of their private information, interference with their right to control their personal information, and potential exposure of their private information.

18. Through this action, Plaintiff seeks damages authorized by WESCA and the MWESA and on behalf of himself and the Class members, defined below, and any other available legal or equitable remedies to which they are entitled.

PARTIES

19. Plaintiff is, and at all times relevant hereto was, a natural person and a permanent resident of the State of Pennsylvania.

20. Defendant is, and at all times relevant hereto was, a corporation duly organized and validly existing under the laws of Nebraska and maintains its corporate headquarters in Chevy Chase, Maryland. Defendant is therefore a citizen of Nebraska and Maryland.

JURISDICTION, VENUE AND STANDING

21. This Court has personal jurisdiction over Defendant because Defendant is a citizen of Nebraska and Maryland, rendering it at home in this State.

22. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because at least one member of the putative class, including Plaintiff, is a citizen of Pennsylvania, and

Defendant is a citizen of Nebraska and Maryland, thus CAFA's minimal diversity requirement is met. Additionally, Plaintiff seeks, at minimum, $1,000.00 in damages for each violation, which, when aggregated among a proposed class of over 5,000, exceeds the $5,000,000 threshold for federal court jurisdiction under the Class Action Fairness Act ("CAFA").

23. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) because Defendant is deemed to reside in any judicial district in which it is subject to personal jurisdiction, and because a substantial part of the events or omissions giving rise to the claim occurred in this District.

24. Plaintiff has Article III standing to maintain this action because he suffered a cognizable and particularized injury as a result of Defendant's violations of WESCA and the MWESA, and because he is not requesting an advisory opinion from this Court. Thus, Plaintiff has a sufficient stake in a justiciable controversy and seeks to obtain judicial resolution of that controversy. At common law, Defendant's conduct would amount to an invasion of privacy, such as intrusion upon seclusion, of which the intrusion itself is sufficient injury for standing. *See Campbell v. Facebook, Inc*., 951 F.3d 1106, 1111 (9th Cir. 2020) ("Under the privacy torts that form the backdrop for these modern [wiretapping] statutes, the intrusion itself makes the defendant subject to liability… Thus, historical practice provides [] support… for the conclusion that a wiretapping plaintiff need not allege any further harm to have standing"); *see also Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 423, (2013) (the "interception of a private [communication] amounts to an injury that is 'concrete and particularized'.").

FACTS

25. Defendant owns and operates the following website and subdomains therein: geico.com. Through its website and subdomains, Defendant solicits consumers to enter into agreements for the provision of its insurance services.

26. Plaintiff most recently visited Defendant's website on or about January of 2023.

27. During this visit, Plaintiff filled out an online auto insurance quote form.

28. While filling out this form, Plaintiff was required to communicate his personal information with Defendant's website including, but not limited to:

> 1) his zip code; 2) name; 3) birthdate; 4) address; 5) the type of car he had; 6) whether he owned, financed, or leased his vehicle; 7) whether his vehicle was used primarily to commute, for pleasure, or for business; 8) details on his commuting; 9) his approximate annual mileage; 10) the length of time he owned his car; 11) his gender identity; 12) his marital status; 13) his social security number; 14) whether he owned or rented his home; 15) details about his current insurance; 16) whether he was licensed before age 29 in the US or Canada; 17) his highest level of education; 18) whether he had government or military affiliations; 19) his spouse's name and personal details; 20) his accident and traffic history; 21) group affiliations such as alumni associations; and 22) his email and phone number.

29. Plaintiff was in Pennsylvania during his visit to Defendant's website.

30. During his visit to the website and completion of the online form, Plaintiff, through his computer and/or mobile device, transmitted substantive information via electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website.[6] The commands were sent as messages instructing Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff. By way of example, when filling out

[6] These communications occur through the Hypertext Transfer Protocol ("HTTP"). HTTP works as a request-response protocol between a user and a server as the user navigates a website. A GET request is used to request data from a specified source. A POST request is used to send data to a server. *See HTTP Request Methods,* located at https://www.w3schools.com/tags/ref_httpmethods.asp (last visited November 16, 2022).

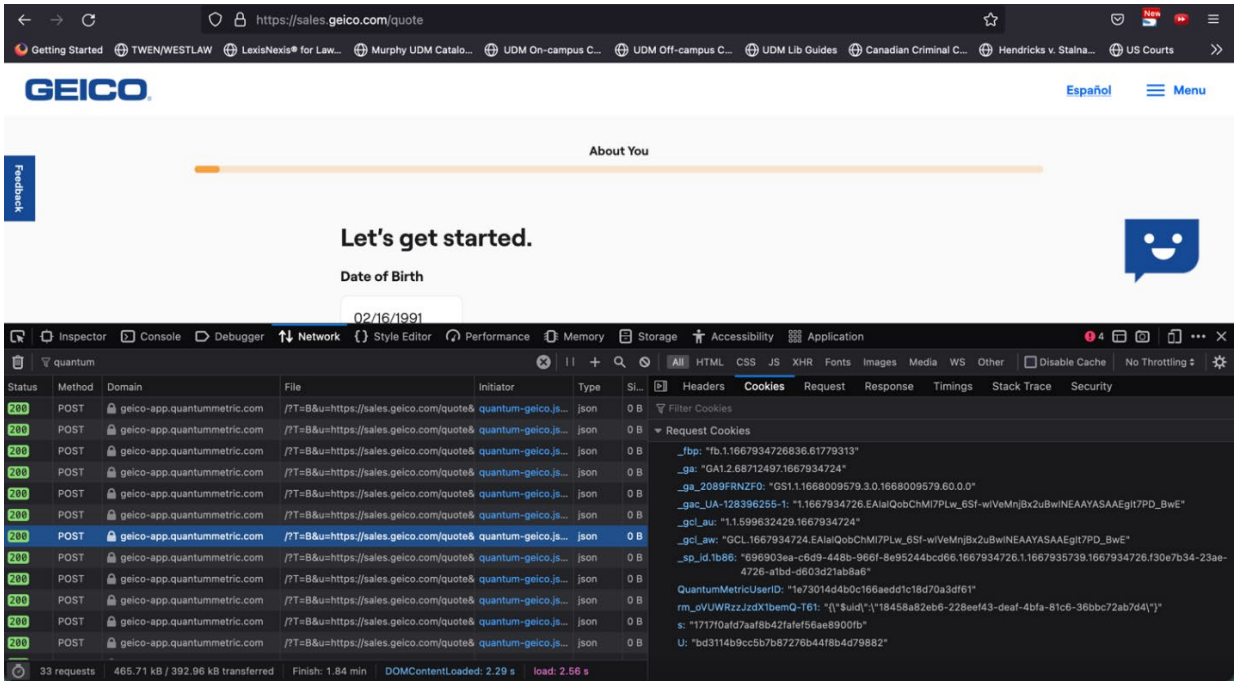
his online insurance quote form, Plaintiff was asked his gender. Plaintiff clicked the selection for "male". This interaction caused an electronic communication to be sent conveying that Plaintiff had clicked and selected that option and substantively expressed the message that he identified as male, which triggered the online form to proceed to the next question. This process applied with the same force for all of the personal information communicated by Plaintiff through his interactions with the online quote form, whether by clicking a selection (like home rental, gender identity, or highest level of education) or by inputting information via keystrokes (like his and his spouse's names and his social security number).

31. The communications sent by Plaintiff to Defendant's (and unknowingly to the Session Replay Provider(s)'s) servers included, but were not limited to, the following actions taken by Plaintiff while filing out the online quote form: mouse clicks and selections of form questions answers, keystrokes, information and PII inputted and communicated by Plaintiff, and copy and paste actions.

32. Defendant responded to Plaintiff's electronic communications by processing and supplying – through its website – the information inputted and requested by Plaintiff. *See Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 U.S. Dist. LEXIS 186955, at *3 (N.D. Cal. Oct. 23, 2019) ("This series of requests and responses — whether online or over the phone — is communication."); *see also Popa v. Harriet Carter Gifts, Inc*., No. 21-2203, 2022 U.S. App. LEXIS 28799 (3d Cir. Oct. 18, 2022).

33. At virtually the same moment that Plaintiff sent communications to Defendant's servers, the session replay software procured by Defendant instantaneously created a duplicate request-and-response communication for each of Plaintiff's actions and answers to the form's questions and routed these communications from Plaintiff to the Session Replay Provider's

servers. The following screenshot reflects the intercepting HTTP request-response sequence on Defendant's website outlined above:



34. Plaintiff reasonably expected that his visit to Defendant's website would be private and that Defendant would not have procured a third party that was tracking, recording, and/or watching Plaintiff as he browsed, interacted with the website, and filled out the personal details he communicated through the online insurance quote form, particularly because Plaintiff was not presented with any type of pop-up disclosure or consent form alerting Plaintiff that his visit to the website was being recorded by Defendant through a third party.

35. In fact, on the first page of Defendant's form is a message that states "**Your info is important to us!** We'll never share your information." Accordingly, Plaintiff reasonably believed that he was interacting privately with Defendant's website, and not that he was being recorded and that those recordings would be captured and transmitted by and to third party servers that Plaintiff was unaware of, where they would be processed and repurposed by that third party, fingerprinting

his digital presence, and could later be watched by Defendant's employees, or worse yet, live while Plaintiff was on the website.

36. Upon information and belief, over at least the past two years, Defendant has had embedded within its website's code and has continuously operated at least one session replay software script[7] that was provided by a third party (a "Session Replay Provider"). The session replay spyware was always active and intercepted every incoming data communication to Defendant's website from the moment they accessed the online quote form.

37. The Session Replay Provider(s) that provided the session replay spyware to Defendant are not a provider of wire or electronic communication services, or an internet service provider.

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

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

40. Defendant's use of session replay spyware through Session Replay Providers to intercept Plaintiff's electronic communications 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's Session Replay Provider(s) indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its website for Defendant's (and its Session Replay Provider's) own benefit.

[7] A script is a sequence of computer software instructions.

41. Defendant's use of session replay spyware to intercept Plaintiff's electronic communications did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's or the Class members' electronic communications with Defendant's website.

42. Upon information and belief, during Plaintiff's visit to Defendant's website, Defendant utilized session replay spyware procured from third parties to intentionally and contemporaneously intercept the substance of Plaintiff's electronic communications with Defendant's website and online quote form, including mouse clicks selecting answers to form questions, keystrokes, information and PII inputted by Plaintiff in response to form questions, and copy and paste actions. In other words, Defendant utilized its Session Replay Provider(s) to intercept, record, process and store electronic communications conveying everything Plaintiff communicated in the online quote form i.e. all the detailed personal information that Plaintiff inputted.

43. The session replay spyware intentionally utilized by Defendant contemporaneously intercepted the 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 copied and sent and/or re-routed the communications to a storage file within the Session Replay Provider(s)'s server(s). The intercepted data communications were transmitted contemporaneously to the Session Replay Provider(s) server(s) as it was sent from Plaintiff's computer and/or mobile device.

44. The relevant facts regarding the full parameters of the communications intercepted and how the interception occurred are solely within the possession and control of Defendant.

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

46. Unlike the harmless collection of an internet protocol address, the data collected by Defendant identified specific information inputted and content viewed (ex. Plaintiff's selected gender identity and social security number), and thus revealed personalized and sensitive information about Plaintiff.

47. The electronic communications intentionally intercepted at Defendant's behest were content generated through Plaintiff's intended use, interaction, and communication with Defendant's website relating to the substance, purport, and/or meaning of Plaintiff's communications with the website quote form, *i.e.*, when Plaintiff clicked and selected "male" as his gender, he was intentionally communicating that he identified as male. These electronic communications stemming from Plaintiff's interactions with the online insurance quote form included conveying highly personal content as described above.

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

49. The session replay spyware utilized by Defendant intercepted, copied, replicated, and sent the data to the Session Replay Provider(s) in a manner that was undetectable by Plaintiff.

50. Plaintiff's electronic data communications were then, processed, interpreted, stored and reproduced by Defendant and/or the Session Replay Provider(s).

51. The electronic data communications were not only intercepted and stored, but was also used by Defendant to create a playback of Plaintiff's visit to the website, displaying the content communicated by Plaintiff during his interactions with the site. Additionally, upon

information and belief, the session replay technology procured by Defendant gave Defendant the ability to view Plaintiff's website visits live in real-time as they were occurring.

52. Defendant's procured interception of Plaintiff's electronic communications allowed Defendant to capture, observe, and divulge Plaintiff's personal details, interests, browsing history, queries, and habits as he interacted with and browsed Defendant's website.

53. Upon information and belief, Defendant similarly procured the interception of the electronic communications of at least 5,000 individuals located in Pennsylvania, Maryland and throughout the United States who visited Defendant's website and completed an online quote form.

54. Defendant utilized third party spyware embedded within its website to intercept the communications at issue.

55. Defendant never alerted or asked Plaintiff or the Class Members for permission to have its Session Replay Provider(s) intercept and record their visits to Defendant's website using "session replay" spyware.

56. Plaintiff and the Class members never consented to interception of their electronic communications by Defendant, it's Session Replay Provider(s) or anyone acting on Defendant's behalf, and they were never given the option to opt out of Defendant's recording.

57. At no point in time did Plaintiff or the Class members provide Defendant, its employees, or agents with consent to intercept their electronic communications using "session replay" spyware.

58. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendant's use of a third party to intercept and record their electronic communications using "session replay" spyware.

59. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendant's use of a third party to intercept and record their visits to Defendant's website using "session replay" spyware.

60. At no point in time did Plaintiff or the Class members impliedly consent to Defendant's use of a third party to intercept and record their electronic communications, as no reasonable person could assume that by communicating with Defendant's website, the substance of those electronic communications would be intercepted, captured, read, observed, re-routed, forwarded, interpreted, reproduced, and stored by an undisclosed third party Session Replay Provider.

61. Plaintiff and the Class members did not have a reasonable opportunity to discover Defendant's unlawful interceptions because Defendant did not disclose the third party interception nor seek consent from Plaintiff and the Class members prior to interception of their communications.

62. Plaintiff and the Class members never clicked or otherwise agreed to any disclosure or consent form authorizing Defendant to use a third party Session Replay Provider to intercept Plaintiff's and the Class members' electronic communications using "session replay" spyware.

63. Defendant's third party session replay spyware 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. In other words, Defendant's unlawful 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 Wesca. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 U.S. App. LEXIS 14951, at *5 (9th Cir. May 31, 2022).

64. In fact, a hyperlink to Defendant's website's privacy policy only misleadingly appears on the insurance quote form after being preceded by the language "we will not share your information". Moreover, Defendant's website and privacy policy failed to explicitly alert or otherwise notify Plaintiff and the Class members that Defendant would be utilizing session replay spyware to facilitate an undisclosed third party's monitoring and recording of their interactions with Defendant's website.

65. Additionally, 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 of use or privacy policy. Indeed, the landing page to Defendant's website not only fails to advise visitors that Defendant is using a third party to intercept their electronic communications, it does not contain any type of conspicuous disclosure regarding Defendant's terms of use or privacy policy. Similarly, the online quote form does not contain language indicating that by completing the form, a user is affirmatively consenting to be bound by Defendant's terms of use or privacy policy.

66. 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 or beginning to complete an online insurance quote form. In other words, Defendant's website does not immediately direct visitors to the sites to the terms of use or privacy policy, and do 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.

67. Upon information and belief, at least one of the purposes of Defendant's procured interception of Plaintiff's and the Class members' electronic communications was to allow Defendant to learn of Plaintiff's and the Class members' personal details, preferences and likes,

which would then be used to market Defendant's services and goods to Plaintiff and the Class members.

68. The surreptitious third party interception of Plaintiff's and the Class members' electronic communications procured by Defendant caused Plaintiff and the Class members harm, including violations of their substantive legal privacy rights under WESCA and the MWESA, invasion of privacy, intrusion upon seclusion, invasion of their rights to control information concerning their person, and/or the exposure of their private information. Indeed, at common law, the intrusion into Plaintiff's and the Class members' private lives is of itself a cognizable injury. 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 ALLEGATIONS

PROPOSED CLASS

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

Nationwide Class:

All natural persons in the United States whose Website Communications were captured in the United States while completing an insurance quote form through the use of Session Replay Code embedded in Defendant's Website without consent.

Pennsylvania Subclass:

All natural persons in the State of Pennsylvania whose Website Communications were captured in the United States while completing an insurance quote form through the use of Session Replay Code embedded in Defendant's Website without consent.

70. Defendant and its employees or agents are excluded from the Class. Plaintiff reserves the right to modify or amend the Class definitions, as appropriate, during the course of this litigation.

NUMEROSITY

71. The Class members are so numerous that individual joinder of all Class members is impracticable. Upon information and belief, Defendant intercepted the electronic communications of over 5,000 individuals. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include notice on Defendant's website, U.S. Mail, electronic mail, Internet postings, and/or published notice.

72. The identities of the Class members are unknown at this time and can be ascertained only through discovery. Identification of the Class members is a matter capable of ministerial determination from Defendant's records kept in connection with its unlawful interceptions.

COMMON QUESTIONS OF LAW AND FACT

73. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are:

(1) Whether Defendant violated WESCA;

(2) Whether Defendant violated the MWESA;

(3) Whether Defendant intercepted or procured another to intercept Plaintiff's and the Class members' electronic communications;

(4) Whether Defendant disclosed to Plaintiff and the Class Members that it was intercepting their electronic communications;

(5) Whether Defendant secured prior consent before intercepting Plaintiff's and the Class members' electronic communications; and

(6) Whether Defendant is liable for damages, and the amount of such damages.

74. The common questions in this case are capable of having common answers. If Plaintiff's claim that Defendant routinely intercepts electronic communications without securing prior consent is accurate, Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

TYPICALITY

75. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

PROTECTING THE INTERESTS OF THE CLASS MEMBERS

76. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and has retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

SUPERIORITY

77. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by the Class are potentially in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendant's wrongful conduct are too small to warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

78. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. For

example, one court might enjoin Defendant from performing the challenged acts, whereas another may not. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

COUNT I
VIOLATIONS OF WESCA
18 Pa. Cons. Stat. 5701, *et seq*.
(On Behalf of Plaintiff and the Pennsylvania Subclass)

79. Plaintiff re-alleges and incorporates the foregoing allegations as if fully set forth herein. For purposes of Count I, and "Class" refers to the Pennsylvania subclass.

80. The Pennsylvania Wiretap and Electronic Surveillance Control Act (the "Act") 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. 18 Pa. Cons. Stat. § 5703.

81. An "intercept[ion]" is the "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device". *See* 18 Pa. Cons. Stat. § 5702.

82. 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. 18 Pa. Cons. Stat. § 5725(a).

83. Defendant procured at least one, and at some time two independent, third party Session Replay Providers to automatically and secretly spy on, and intercept, Defendant's Pennsylvania website visitor's electronic communications with Defendant in real-time.

84. To facilitate this wiretap, Defendant procured and installed its Session Replay Provider(s)'s software code on its website.

85. The session replay software code procured from the Session Replay Provider(s) by Defendant is a sophisticated system capable of capturing, recording, interpreting, reformatting, and processing electronic communications, and is therefore an "electronic, mechanical, or other device" as defined by WESCA. *See* 18 Pa. Cons. Stat. § 5702.

86. The session replayed software code procured from the Session Replay Provider(s) by Defendant is not a "tracking device" because, as stated above, it is a sophisticated system with capabilities well beyond "***only*** the tracking of the movement of a person or object." *See* 18 Pa. Cons. Stat. § 5702.

87. Upon information and belief, Defendant knew that its Session Replay Provider(s) would add the contents of its visitor's private electronic communications, including but not limited to the personal information they communicated in their insurance quote forms, procured through the wiretap, to its back-end database, resulting in the unauthorized disclosure of such information to the Session Replay Provider(s) and risking the further disclosure of that information to others.

88. Defendant intentionally procured the interception of the content of Defendant's website visitors' private electronic communications in real-time, including the detailed personal information they communicated through the online quote form.

89. Plaintiff and the putative class members engaged in electronic communications with Defendant through use of Defendant's website, as their interactions with the website

transferred "signs, signals, writing, images, sounds, data or intelligence" and their interactions were not wire or oral communications, a communication made through a tone-only paging device, or communications from a tracking device. *See* 18 Pa. Cons. Stat. § 5702.

90. Plaintiff and the putative class members had a justified and reasonable expectation under the circumstances that their private electronic communications, including the contents of their personal details as described above, would not be intercepted by and exposed to an undisclosed third party. *See In re Google Inc.*, 806 F.3d 125, 151 (3d Cir. 2015); *see also In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 293-94 (3d Cir. 2016).

91. Nonetheless, Defendant employed its Session Replay Provider(s) to intercept the content of Plaintiff's and the putative class members' electronic communications with Defendant.

92. Because the code is secret and encrypted, Plaintiff and the putative class members were not aware that their electronic communications were being intercepted by Defendant's Session Replay Provider(s).

93. Plaintiff and the putative class members did not give prior consent to having their communications intercepted by Defendant or its Session Replay Provider(s).

94. By procuring its Session Replay Provider(s) to intercept, record, interpret, reproduce and store Plaintiff's and the Class members private electronic communications for its own purposes without prior consent, Defendant violated 18 Pa. Cons. Stat. § 5703(1), (2) and (3).

95. At all times pertinent hereto, Defendant's conduct was knowing and intentional.

96. As a result of Defendant's conduct, and pursuant to § 5725 of WESCA Plaintiff and the other members of the putative Class were harmed and are each entitled to actual damages, liquidated damages, punitive damages, reasonable attorneys' fees and costs. 18 Pa. Cons. Stat § 5725(a).

COUNT II
INVASION OF PRIVACY – PENNSYLVANIA INTRUSION UPON SECLUSION
(On behalf of the Pennsylvania Subclass)

97. Plaintiff re-alleges and incorporates the foregoing allegations as if fully set forth herein. For purposes of Count II, and "Class" refers to the Pennsylvania subclass.

98. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

99. Each time Plaintiff and Class members visited Defendant's website on their personal computers and/or mobile devices, Defendant secretly monitored, recorded, and collected their personal data, in real-time, for Defendant's monetary gain and without Plaintiff's and Class members' consent.

100. Plaintiff and Class members' mouse clicks and keystrokes when filling out the online quote forms ("Website Communications"), were all collected by the Session Replay Code that Defendant procured and deployed on its website.

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

102. Because the data collected by the Session Replay Code identifies specific information inputted by visitors to Defendant's website, such as the personal details entered into the quote forms by Plaintiff and the Class members, it reveals personalized and sensitive information about the website visitors' person, including the visitor's internet activity, personal interests, personal details, and habits.

103. Defendant's surreptitious interception of website visitors' Website Communications therefore allowed Defendant to monitor, record, and disclose Plaintiff's and

Class members' internet activity, personal interests, personal details, and habits as they interacted with Defendant's online quote forms in real-time.

104. Upon information and belief, the Session Replay Code embedded on Defendant's website indiscriminately captures the maximum range of data and information, including highly sensitive and personal information displayed by the website.

105. 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 collect, disclose, or use the contents of Website Communications.

106. 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 and utilized for business gain.

107. Defendant intentionally intrude on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

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

109. Defendant deprived Plaintiff and Class members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

110. Plaintiff and Class members were harmed by Defendant's wrongful conduct as Defendant's conduct has caused Plaintiff and the Class frustration, mental anguish and suffering arising from their loss of privacy and confidentiality of their personal information.

111. 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.

112. 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.

113. Further, Defendant (and the Session Replay Provider it facilitated) improperly profited from its invasion of Plaintiff's and Class members' privacy by using Plaintiff's and Class members personal data and information for its economic value and their own commercial gain.

114. Upon information and belief, Defendant derive significant benefit from the content intercepted through its procurement and use of Session Replay Code, by collecting, retaining, and using that data and information to maximize profits through predictive marketing and other targeted advertising practices.

115. The intercepting Session Replay Provider procured by Defendant derives a paramount benefit from the content intercepted through Defendant's procurement and use of session replay code as this data underlies the very services it provides,

116. As a direct and proximate result of 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.

117. Defendant's conduct is ongoing. Defendant continues to unlawfully intercept the Website 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
VIOLATION OF MWESA
Md. Code Ann., Cts. & Jud. Proc. § 10-401, et seq
(On behalf of the Nationwide Class)

118. Plaintiff re-alleges and incorporates the foregoing allegations as if fully set forth herein. For purposes of Count III, and "Class" refers to the Nationwide class.

119. Plaintiff and Class members visited and interacted with Defendant's website from their personal computers and/or mobile devices while Defendant was in Maryland. Because Defendant is at home in Maryland, it is obligated to abide by Maryland law.

120. Unbeknownst to Plaintiff and Class members, Defendant procures and directs Session Replay Providers to embed Session Replay Code on Defendant's website to surreptitiously intercept, monitor and record nearly every interaction visitors have with its website quote forms—including every mouse click and keystroke used to substantively answer the questions in Defendant's forms ("Website Communications")—in real-time.

121. MWESA makes it unlawful for private corporations, like Defendant, to (1) willfully intercept, or procure another to intercept, any wire, oral, or electronic communication; (2) willfully disclose the contents of any wire, oral, or electronic communication,; or (3) willfully 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. Md. Code Ann., Cts. & Jud. Proc. § 10-401(14) & 402(a).

122. Anyone who intercepts, discloses, or uses—or procures another to intercept, disclose, or use—a wire, oral, or electronic communication in violation of the Maryland Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher; (2) punitive damages;

and (3) reasonable attorneys' fees and other litigation costs incurred. Md. Code Ann., Cts. & Jud. Proc. § 10-410(a).

123. The electronic communications of visitors to Defendant's Website—including their interactions with the website in responding to the quote form questions ("Website Communications")—are intentionally intercepted by the Session Replay Code procured and utilized by Defendant in violation of the Maryland Act.

124. "Intercept" is defined by the Maryland Act as any "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Md. Code Ann., Cts. & Jud. Proc. § 10-401(10) (emphasis added).

125. "Electronic Communication" is defined as "any 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 photooptical system." Md. Code Ann., Cts. & Jud. Proc. § 10-401(5)(i).

126. "Contents" of an electronic communication are defined broadly to include "any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Code Ann., Cts. & Jud. Proc. § 10-401(4).

127. Plaintiff's and Class Members' intercepted Website Communications constitute the "contents" of "electronic communications" within the meaning of the Maryland Act. Because the data collected by the Session Replay Code identifies specific information inputted by visitors to Defendant's Website who filled out the quote forms, it reveals personalized and sensitive information about the website visitors' internet activity, personal interests, personal details, and habits. As such, Defendant intercept the "content" generated through Plaintiff's and Class Members' intended use, interaction, and electronic communication with Defendant's Website.

128. The Session Replay Code procured and utilized by Defendant is a "device" used for the "acquisition of the contents of [] electronic [] communication[s]" within the meaning of the Maryland Act, because it intercepts, monitors, records, and collects the contents of electronic computer-to-computer communications relayed between the personal computers and/or mobile devices of website visitors and the computer servers and hardware utilized by Defendant to operate its website. Moreover, the Session Replay Code procured and utilized by Defendant alters the operation of the personal computers and/or mobile devices used by website visitors by instructing the hardware components of those physical devices to run the processes that ultimately intercepts the Website Communications and transmits them contemporaneously to the Session Replay Providers. By the very nature of its operation, the Session Replay Code is therefore a "device" used to intercept electronic communications within the meaning the Maryland Act.

129. Defendant violated the Maryland Act by willfully procuring and deploying Session Replay Code on its website to spy on visitors, automatically and secretly, and ***intercept*** the content of Plaintiff's and Class Members' electronic communications with Defendant's Website in real-time.

130. Plaintiff's and Class Members' electronic communications are intercepted contemporaneously with their transmission.

131. The Session Replay Code procured and utilized by Defendant also ***disclose*** the content of Plaintiff's and Class Members' electronic communications to the Session Replay Providers, who could then use the intercepted electronic communications to recreate simulation videos of Plaintiff's and Class Members' entire visits to Defendant's Website.

132. Defendant willfully ***use*** the contents of Plaintiff's and Class Members' electronic communications, knowing that the data and information was obtained through unlawful

interception, for purposes of targeted advertising, marketing, and other unknown revenue generating purposes. The Session Replay Code procured and utilized by Defendant deliberately intercepts, records, and collects the content of Plaintiff's and Class Members' electronic communications with Defendant's Website. Upon information and belief, the data and information intercepted, recorded, and collected is used by Defendant to increase its marketing efficiency, advertising, and outreach efforts, rather than to keep the website operational.

133. Plaintiff and Class Members did not consent to Defendant's surreptitious interception and recording of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at Defendant's Website.

134. Plaintiff and Class Members have been injured by Defendant's conduct alleged herein, which injury includes violations of their privacy and the unknowing loss of control over how their personal information and communications are received, used, or disseminated and by whom. Accordingly, the imposition of statutory damages under the Maryland Act is appropriate here.

135. Pursuant to Md. Code Ann., Cts. & Jud. Proc. § 10-410, Plaintiff and the Class Members seek (1) actual damages, not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

136. Defendant's conduct is ongoing. Defendant continues to procure and utilize Session Replay Code to unlawfully intercept, record, collect, disclose, and use the contents of electronic communications generated by website visitors—including Plaintiff and Class Members—without their prior consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

WHEREFORE, Plaintiff, on behalf of himself and the other members of the Class, prays for the following relief:

a. An order certifying the Nationwide Class and Pennsylvania Subclass and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

b. An award of actual damages, statutory damages, liquidated damages, and/or punitive statutory damages;

c. An award of reasonable attorney's fees and costs;

d. Declaring that Defendants' past conduct was unlawful, as alleged herein;

e. Declaring Defendants' ongoing conduct is unlawful, as alleged herein;

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

g. Such further and other relief the Court deems reasonable and just.

JURY DEMAND

Plaintiff and Class Members hereby demand a trial by jury on all issues so triable.

DOCUMENT PRESERVATION DEMAND

Plaintiff demands that Defendant take affirmative steps to preserve all records, lists, electronic databases or other itemizations associated with the allegations herein, including all records, lists, electronic databases or other itemizations in the possession of any vendors, individuals, and/or companies contracted, hired, or directed by Defendant to assist in sending the alleged communications.

Dated: October 19, 2023

Respectfully Submitted,

/s/ James J. Pizzirusso
James J. Pizzirusso
(Md. Bar No. 20817)
HAUSFELD LLP
888 16th Street N.W.
Suite 300
Washington, D.C. 20006
202.540.7200
jpizzirusso@hausfeld.com

Steven M. Nathan
(Md. Bar No. 30618)
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
646.357.1100
snathan@hausfeld.com

Joseph H. Kanee, Esq.*
MARCUS ZELMAN LLC
701 Cookman Avenue, Suite 300
Asbury Park, New Jersey 07712
Telephone: (732) 695-3282
Fascimile: (732) 298-6256
joseph@marcuszelman.com

Counsel for Plaintiff and Proposed Class

** Pro Hac Vice Forthcoming*

ClassAction.org
