UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

CASE NO.: _____

CINNAMON SMITH, an Illinois resident, ALISON PAIGE, a Massachusetts resident, MARRCHELLE TANZYMORE, a Maryland resident, and CAROLYN SMITH, a Missouri resident, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

JURY TRIAL DEMANDED

TIKTOK INC., a California corporation, and BYTEDANCE INC., a Delaware corporation,

Defendants.
_____/

CLASS ACTION COMPLAINT

Plaintiffs Cinnamon Smith ("Cinnamon Smith"), Alison Paige ("Paige"), Marrchelle Tanzymore ("Tanzymore"), and Carolyn Smith ("Carolyn Smith") (collectively, "Plaintiffs") bring this class action against Defendants TikTok Inc. ("TikTok") and ByteDance Inc. ("ByteDance") (collectively, "Defendants"), and alleges, based upon personal knowledge as to themselves and their own acts and experiences, and on information and belief as to all other matters based upon, *inter alia*, the investigation of counsel, as follows:

INTRODUCTION

1. This is a class action brought by citizens of Illinois and three other states against the California-based corporations Tik Tok and ByteDance (which were and are controlled and largely owned by the same individual in China, Yiming Zhang), for intercepting the electronic communications of users of the TikTok app when they link to third-party websites in the TikTok

app. Defendants employ JavaScript computer code ("Session Replay Code") to track users' every move as they browse the Internet from within the TikTok app. As users browse a third-party website from within the TikTok app, they do so via TikTok's in-app web browser (with no option to use the mobile phone's default web browser), and the Session Replay Code intercepts and records the user's electronic communications. These communications encompass their keystrokes, clicks, scrolling and swiping finger movements, text being entered into an information field or text box (even when never sent to the website), and/or other electronic communications as they occur in real time ("Website Communications").

2. Session Replay Code goes far beyond the expectations of ordinary users of the Internet of the data they might be offering to companies. According to a Princeton University study: "The extent of the data collected 'far exceeds user expectations,' including recording what you type into a text box before you submit it, 'all without any visual indication to the user.'"[1]

3. Moreover, the third-party websites did not consent in any way that private communications from visitors to those websites be intercepted by TikTok, just because the visitor happens to link to the website from within the TikTok app.

4. The use of Session Replay Code is not tolerated by some of the largest tech companies. In 2019, Apple warned app developers using Session Replay Code that they were required to disclose this type of tracking and recording to their users, or they would be 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 visual indication when recording, logging, or otherwise making a record of user activity."[2]

---

[1] Nitasha Tiku, "The Dark Side of 'Replay Sessions' That Record Your Every Move Online," *Wired*, available at https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/ (last visited Jan. 9, 2023).

[2] https://techcrunch.com/2019/02/07/apple-glassbox-apps/ (last visited Jan. 9, 2023).

5. Defendants' conduct directly violates the Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.* (the "FWA"), the Massachusetts Wiretap Act, Mass. Gen. Laws Ann. 272 § 99 (the "Massachusetts Act"), the Maryland Wiretap Act, Md. Cts. & Jud. Pro. §§ 10-401 *et seq.* (the "Maryland Act"), and the Missouri Wiretap Act, Mo. Stat. §§ 542.400 *et seq.* (the "Missouri Act"), which statutes each bar the interception and recording of private communications without prior consent of all parties to the conversation.

6. Plaintiff brings this action individually and on behalf of a class of every person in the United States whose Website Communications were intercepted through Defendants' use of Session Replay Code in the TikTok app via TikTok's in-app web browser within the applicable statute of limitations, and seeks all civil remedies provided under the cause of action, including but not limited to actual, statutory, liquidated, punitive damages, disgorgement, and attorneys' fees and costs.

PARTIES

7. Plaintiff Cinnamon Smith is, and at all times relevant hereto was, a natural person and a permanent resident of the state of Illinois. She is 30 years old, and has resided in Chicago, Illinois for more than 15 years. Cinnamon Smith downloaded the TikTok app in or around 2020 and uses it almost every day. At least once a week and often more, while using the TikTok app, Cinnamon Smith clicks on links to external, third-party websites causing her to use TikTok's in-app web browser. For example, in December 2022, from her home in Chicago, Illinois, she visited www.fashionnova.com via a link in an advertisement on the TikTok app, and scrolled around the website to look at additional products.

8. Plaintiff Paige is, and at all times relevant hereto was, a natural person and a permanent resident of the state of Massachusetts. She is 57 years old, and has resided in Woburn,

Massachusetts since 2013. Paige downloaded the TikTok app in or around 2021 and has used it almost every day since about September 2022. At least once a week and often more, while using the TikTok app, Paige clicks on links to external, third-party websites causing her to use TikTok's in-app web browser. For example, from her home in Woburn, Massachusetts, she routinely visits websites from within the TikTok app and inputs personal financial information into those websites in order enter into lotteries.

9. Plaintiff Tanzymore is, and at all times relevant hereto was, a natural person and a permanent resident of the state of Maryland. She is 39 years old, and has resided in Baltimore, Maryland her entire life. Tanzymore downloaded the TikTok app in or around 2021 and uses it almost every day. At least once a week and often more, while using the TikTok app, Tanzymore clicks on links to external, third-party websites causing her to use TikTok's in-app web browser. For example, from her home in Baltimore, Maryland, she routinely links to websites of social media influencers from within the TikTok app and scrolls around on those websites to look at additional products.

10. Plaintiff Carolyn Smith is, and at all times relevant hereto was, a natural person and a permanent resident of the state of Missouri. She is 55 years old, and has resided in Kansas City, Missouri her entire life. Carolyn Smith downloaded the TikTok app in or around August 2021 and uses it almost every day. At least once a week and often more, while using the TikTok app, Carolyn Smith clicks on links to external, third-party websites causing her to use TikTok's in-app web browser. For example, in or around August 2021, from her home in Kansas City, Missouri, she visited www.shapermint.com via a link in an advertisement on the TikTok app, and accessed and input personal financial information into that website in order to purchase a product.

11. Defendant TikTok is, and at all times relevant hereto was, a corporation organized and validly existing under the laws of California with its principal place of business in Culver City, California. It is a wholly owned subsidiary of TikTok, LLC.

12. Defendant ByteDance is, and at all times relevant hereto was, a corporation organized and validly existing under the laws of Delaware with its principal place of business in Mountain View, California. Upon information and belief, ByteDance is involved in development of the TikTok app, including research and development of software for the TikTok app.

13. At all relevant times, Defendants have shared offices in Silicon Valley and at 5800 Bristol Parkway, Culver City, California, and have also shared employees. Employees frequently have both a TikTok and a ByteDance email address, and executives often have roles at both companies. For example, in April 2021, it was announced that Shou Zi Chew, the CFO of ByteDance, would concurrently take on the role of CEO of TikTok.[3] TikTok's "Head of HR, Americas & Global Functions, GBS," Kate Barney, is apparently also ByteDance's "Head of HR, US & Europe, Monetization."[4]

14. The ByteDance US Applicant Privacy Notice provided to prospective employees represents Defendants as a single entity: "ByteDance ('we' or 'us') has prepare this Applicant Privacy Notice ('Notice') for applicants to roles with ByteDance . . . references to 'ByteDance' comprises the following U.S. entities: ByteDance Inc., TikTok Inc., and any US incorporate affiliates."[5]

---

[3] Molly Schuetz, *ByteDance's Shouzi Chew Named New TikTok CEO*, FORTUNE (Apr. 30, 2021), available at https://fortune.com/2021/04/30/new-tiktok-ceo-bytedance-shouzi-chew/.

[4] https://www.linkedin.com/in/katemcfarlinbarney/ (last visited Jan. 9, 2023).

[5] *ByteDance US Applicant Privacy Notice*, available at https://sf16-sg.tiktokcdn.com/obj/eden-sg/ha_lm_lswvlw/ljhwZthlaukjlkulzlp/portal/static/ByteDance_US_Applicant_Privacy_Notice.pdf (last visited Jan. 9, 2023).

15. On information and belief, Defendants do not operate as independent corporate entities, but instead function as satellite offices of the China-headquartered company Beijing Douyin Information Service Co. Ltd. a/k/a ByteDance Technology Co. Ltd. ("Beijing ByteDance"). Defendants operate with little independence and are constantly monitored by Chinese management.

16. On information and belief, Beijing ByteDance makes key strategic decisions for Defendants, including regarding the TikTok app, and Defendants are tasked with executing such decisions. Beijing ByteDance's level of involvement is in TikTok's operations has been described by former employees as "so blurry as to be non-existent."[6] Moreover, U.S. employees of Defendants in California are expected to work during Chinese business hours to be available to Beijing-based employees Beijing ByteDance.[7] For example, one former project manager who posted a YouTube video entitled "Why I Just Quit My Product Manager Job at TikTok" stated she was expected to regularly attend late-night "Beijing meetings," and to submit a last-minute product proposal regarding the TikTok app for approval to the "Beijing team," even after it had already been approved by U.S. management.[8]

17. The close relationship between Beijing ByteDance and Defendants encompasses the former's ready access to any and all of U.S. users' data acquired through their use of the TikTok app.[9]

---

[6] Salvador Rodriguez, *TikTok Insiders Say Social Media Company is Tightly Controlled by Chinese Parent ByteDance*, CNBC (June 25, 2021), available at https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html.

[7] ByteDance, *LinkedIn Interviews ByteDance: How ByteDance Builds Its Global Employer Brand*, YOUTUBE, https://www.youtube.com/watch?v=Epp_TN52fSU.

[8] Chloe Shih, *Why I Just Quit My Product Manager Job at TikTok*, YOUTUBE, https://www.youtube.com/watch?v=pkDXV2g_i7Y.

[9] *See id*.

18. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer and/or alter ego of the other Defendant, and each Defendant acted in the course and scope of such agency, partnership and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of the other Defendant and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted and/or participated in the acts or transactions of the other Defendant.

19. At all relevant times, and in connection with the matters alleged herein, Defendants were controlled and largely owned by the same person, China-based founder Zhang Yiming, and constitute a single enterprise with a unity of interest.

JURISDICTION AND VENUE

20. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it is brought under the laws of the United States, *i.e.* the Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.* This Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367.

21. The Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because the members of the putative class are of diverse citizenship from Defendants, there are more than 100 members of the putative class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of costs and interest.

22. The Court has personal jurisdiction over Defendants because they (i) transact business in Illinois; (ii) have substantial aggregate contacts with Illinois; (iii) engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in Illinois; and (iv) purposely availed themselves of the laws of Illinois.

23. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events, omissions, and acts giving rise to the claim occurred in this District. Moreover, Plaintiff Cinnamon Smith resides in this District.

FACTUAL ALLEGATIONS

24. The TikTop app debuted in the United States in September 2018 (as a successor to the Musical.ly app after ByteDance purchased Musical.ly, Inc.). One month thereafter, it had surpassed Facebook, Instagram, YouTube, and SnapChat in monthly installations, and had more than one billion downloads.[10] In 2020, the year of the COVID-19 lockdowns, it was the second most downloaded iPhone app.[11] In 2021, it was the most popular app in the United States,[12] and had 1.2 billion active users globally in the fourth quarter of that year.[13]

25. While TikTok is most widely known for user-created dance, comedy, or lip-synching videos, the variety of content that can be created and viewed on TikTok is virtually limitless—if you can imagine it, it likely exists on TikTok. The content on the TikTop app is aimed at perpetuating its users' dopamine (*i.e.*, the neurotransmitter released in the brain to give a sense of reward or accomplishment), typically with videos less than one minute long. Just as with a slot machine at a casino, users can find themselves scrolling the TikTop app for hours without realizing it, awash in a dopamine rush.

---

[10] Dan Hughes, *The Rapid Rise of TikTok*, Digital Marketing Institute (Aug. 26, 2019), https://digitalmarketinginstitute.com/blog/the-rapid-rise-of-tiktok (last visited Jan. 9, 2023).

[11] Werner Geyser, *TikTok Statistics—63 TikTok Stats You Need to Know [2022 Update]*, Influencer Marketing Hub (updated Aug. 1, 2022), https://influencermarketinghub.com/tiktok-stats/ (last visited Jan. 9, 2023).

[12] *Id*.

[13] Mansoor Iqbal, *TikTok Revenue and Usage Statistics (2022),* Business of Apps (Nov. 11, 2022), https://www.businessofapps.com/data/tik-tok-statistics/#:~:text=TikTok%20generated%20an%20estimated%20%244.6%20billion%20revenue%20in,Is%20accessed%20by%20over%20600%20million%20users%20daily (last visited Jan. 9, 2023).

26. TikTok touts that one in every two "Gen Z" (*i.e.*, the generation aged 18 to 25 as of the date of this filing) TikTok users are likely to purchase a product while using TikTok; that 81% of users use TikTok to discover new products and brands; and that TikTok video ads take up six times more space on the user's screen than traditional "banner ads."[14] In the second quarter of 2021, consumers spent over $500 million in purchases via the TikTok app.[15] One independent study of TikTok's effectiveness for advertisers by consumer insights platform Disqo found that "TikTok users put an average of 8.5% more dollars into their shopping carts" than consumers shopping at those same websites who did not link from TikTok.[16] Moreover, the independent study found that over 50% of respondents 35-54 were using the TikTop app daily: "They become power users just like younger cohorts."[17]

27. In 2021, TikTok generated an estimated $4.6 billion in revenue.[18] The United States is TikTok's largest market outside of China.[19]

28. As stated in a 2017 feature story in *The Economist*, the "world's most valuable resource is no longer oil, but data."[20]

29. TikTok's algorithm, the machine learning software tool used to determine what videos and what advertisements to display on a user's home page or a user's "discover page,"

---

[14] *Get Your Business Discovered on TikTok,* TikTok for Business, https://getstarted.tiktok.com/us-en-v1brand?lang=en&msclkid=9808304b00701c6f2f13532624807b5c (last visited Jan. 9, 2023).
[15] Geyser, *supra* at n.11.
[16] Liu, Ivy, *TikTok's Latest Good News: Its Ads Are Sticky and Rich People Spend a Lot of Time There*, DIGDAY (Sept. 30, 2021), https://digiday.com/media/tiktoks-latest-good-news-its-ads-are-sticky-and-effective-and-rich-people-spend-a-lot-of-time-there/ (last visited Jan. 9, 2023).
[17] *Id.*
[18] Mansoor, *supra* at n.13.
[19] *Id*.
[20] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), available at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

utilizes tracking software to understand a user's interests and habits.[21] This type of accurate targeted advertising, and the big data that powers it, is critical to Defendants' lucrative marketing business model.

30. To drive its business, TikTok presents users with links to third-party websites in two main ways:

(a) through TikTok video advertisements, which appear as normal TikTok videos except that they contain icons identifying them as a sponsored post or an advertisement, and which present users with multiple opportunities to link to a third-party website, *e.g.*, to purchase the advertised product; and

(b) through the profiles of users with more than 1,000 followers, including popular TikTok personalities, businesses or organizations, which have the option to add a link to external websites directly on their profile.

31. In both scenarios, the third-party website is opened via TikTok's in-app browser. Specifically, while a user attempts to access a website by clicking a link while using the TikTok app, the website does not open via the user's default web browser on the mobile device, such as Safari or Google Chrome. Instead, unbeknownst to the user, and without offering the user any option, the link is opened inside the TikTop app, in Defendants' own in-app browser. Thus, the user views the third-party website without leaving the TikTok app.

32. TikTok's in-app browser inserts JavaScript Session Replay Code into the third-party websites that are accessed using the in-app browser. The inserted code intercepts all the details of the TikTok user's use of the in-app browser while it is open, and TikTok tracks and captures all these details as the user interacts with the website.

---

[21] *See, e.g.*, *How TikTok's Algorithm Works: A Fascinating and Disturbing Analysis,* 9 TO 5 MAC (July 28, 2021), https://9to5mac.com/2021/07/28/how-tiktoks-algorithm-works/ (last visited Jan. 9, 2023).

33. Software researcher and blogger Felix Krause recently published a report on the risks of in-app Internet browsers.[22] Of the seven popular apps Krause tested, TikTok was the only app that monitors keystrokes.

34. Specifically, while a user is interacting with the third-party website, TikTok tracks and records all keyboard inputs. It also records every tap on any button, link, image or other website element and logs details about what that element is.[23]

35. Krause created and used a tool called InAppBrowser.com to detect JavaScript commands executed. Krause concluded that "TikTok injects code into third party websites through their in-app browsers that behaves like a keylogger."[24] Anything that user does via TikTok's in-app browser is recorded and stored by Defendants, including what links were clicked, what form fields were filled out (and with what text), how the user scrolled or manipulated images using various finger movements, and what images were viewed. The graphics below show the JavaScript code inserted by Defendants' in-app browser into the Apple iOS operating system and the tool's description of the function of the code. Plaintiff is informed and believes that similar JavaScript Session Replay Code is inserted by Defendants' in-app browser into the Android operating system.

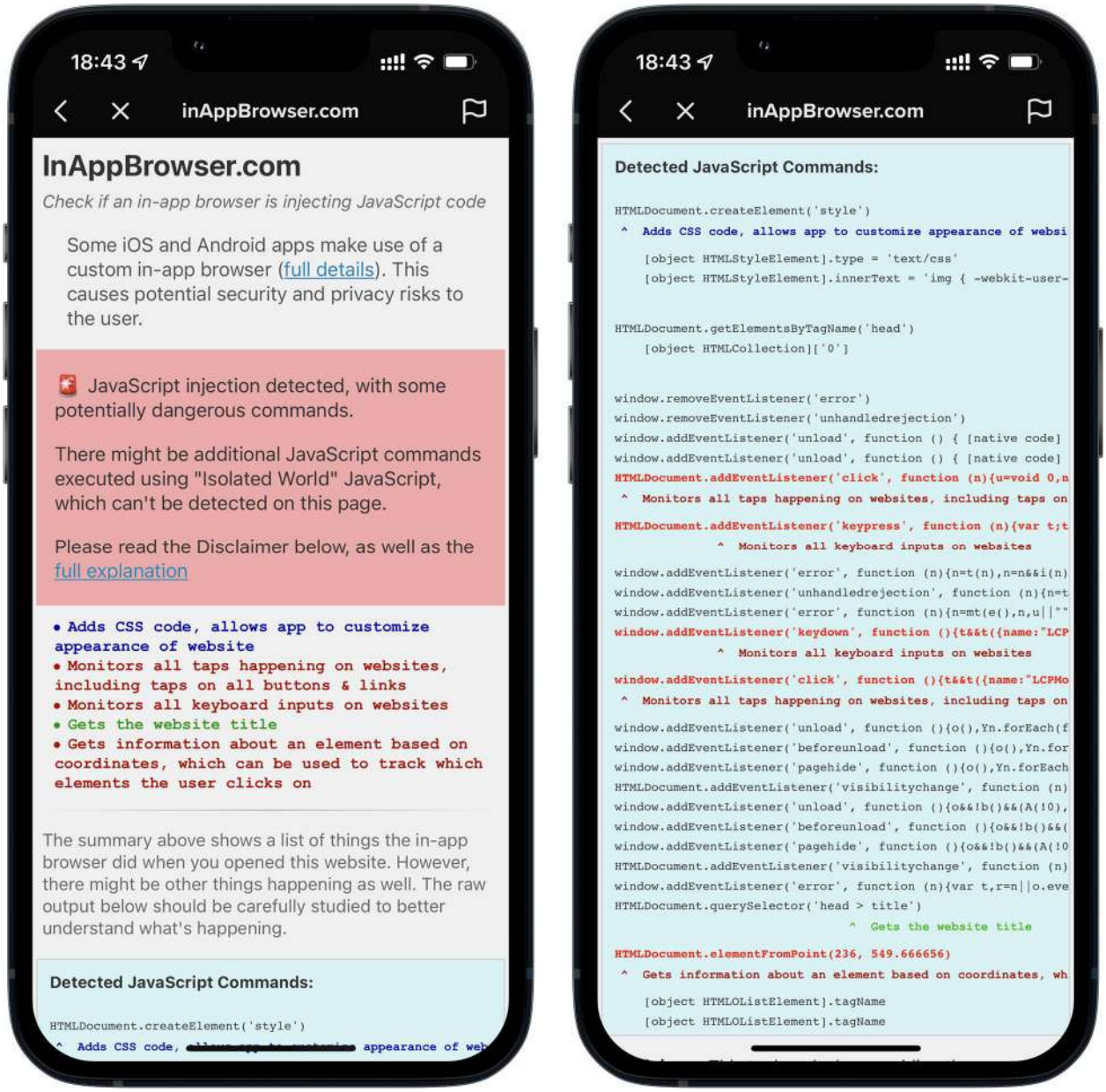
---

[22] *See* Felix Krause, *iOS Privacy: Instagram and Facebook Can Track Anything You Do on Any Website in Their In-App Browser*, krausfx.com (Aug. 10, 2022), https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last visited Jan. 9, 2023).
[23] *Id*.
[24] *Id*.

```
/* --------------------
DISCLAIMER:

The code below was generated through https://inappbrowser.com
which basically overrides many of the standard JavaScript functions to get alerted
whenever the host iOS app runs JavaScript commands. The code below is not complete.
For example, having "[object HTMLStyleElement]" would mean an object, of the type
HTMLStyleElement is being used. However, there are no further insights on those.

Also, there might be more JavaScript code that is being run, through
https://developer.apple.com/documentation/webkit/wkcontentworld, which can't be detected
by this tool.

The code below is for educational purposes only, and does not reflect a 100% accurate
representation of the JavaScript code that is being run.

This file was generated on 2022-08-17
*/



HTMLDocument.createElement('style')

[object HTMLStyleElement].type = 'text/css'
[object HTMLStyleElement].innerText = 'img { -webkit-user-select: none; -webkit-touch-callout: none; }'
HTMLDocument.getElementsByTagName('head')
[object HTMLCollection]['0']
window.removeEventListener('error')
window.removeEventListener('unhandledrejection')
window.addEventListener('unload', function () { [native code] }
window.addEventListener('unload', function () { [native code] }

HTMLDocument.addEventListener('click', function (n){u=void 0,n&&e!==n&&r({event:e=n,name:t})})

HTMLDocument.addEventListener('keypress', function (n){var t;try{t=n.target}catch(n){return}var
r=t&&t.tagName;r&&("INPUT"===r||"TEXTAREA"===r||t.isContentEditable)&&(u||i("input",e)(n),clearTimeout(u),u=window.setTimeout
(function(){u=void 0},o))})

window.addEventListener('error', function (n){n=t(n),n=n&&i(n);n&&r&&r(n)}
window.addEventListener('unhandledrejection', function (n){n=t(n),n=n&&i(n);n&&r&&r(n)}
window.addEventListener('error', function (n){n=mt(e(),n,u||"");n&&t&&t(n)}, true
window.addEventListener('keydown', function (){t&&t({name:"LCPMonitor",lcp:e}),i()}, true

window.addEventListener('click', function (){t&&t({name:"LCPMonitor",lcp:e}),i()}, true

window.addEventListener('unload', function (){o(),Yn.forEach(function(n){window.removeEventListener(n,u,!0)})}
window.addEventListener('beforeunload', function (){o(),Yn.forEach(function(n){window.removeEventListener(n,u,!0)})}
window.addEventListener('pagehide', function (){o(),Yn.forEach(function(n){window.removeEventListener(n,u,!0)})}
HTMLDocument.addEventListener('visibilitychange', function (n){w(r)?r(n):"hidden"===document.visibilityState&&t(n)})
window.addEventListener('unload', function (){o&&!b()&&(A(!0),r&&r())}
window.addEventListener('beforeunload', function (){o&&!b()&&(A(!0),r&&r())}
window.addEventListener('pagehide', function (){o&&!b()&&(A(!0),r&&r())}
HTMLDocument.addEventListener('visibilitychange', function (n){w(r)?r(n):"hidden"===document.visibilityState&&t(n)})
window.addEventListener('error', function (n){var
t,r=n||o.event||{};try{t=r.target||r.srcElement||{}}catch(r){return}w((n=t).getAttribute)?n.getAttribute("integrity"):n.inte
grity)&&(n=w((n=t).getAttribute)?n.getAttribute("src"):n.src||n.href||"",t=(null===(t=t.tagName)||void 0===t?void
0:t.toLowerCase())||"",n&&t&&n!==location.href&&e(n))}, true
HTMLDocument.querySelector('head > title')
```

25

[25] *Id.*



26

36. When a purchase is made via TikTop's in-app browser, Defendants automatically intercept all the details of the purchase entered by the user, including the name of the purchaser, their address, telephone number, credit card or bank information, usernames, passwords, dates of birth, and other personal information.

[26] *Id.*

37. Moreover, in the case of many other types of websites, the Session Replay Code in TikTok's in-app browser enables Defendants to obtain valuable, but undeniably private, information, such as about a user's mental health, physical health, or sexual preferences. For example, the online talk therapy company BetterHelp has a verified account on the TikTok app with a link to its website, which immediately asks the website visitor questions about their mental health needs. Knowing which pages a user chooses to click on and spends time reading (a click without time spent scrolling on the text would be distinguishable as a mere mistake by the user) can reveal deeply personal and private information, which TikTok intercepts to monetize by sending more accurate targeted content and advertisements to the user. Other third-party websites that users can link to via the TikTok app connect users with doctors or mental health professionals, and the information entered by the user to be placed with the appropriate professional is also tracked via the TikTok app unbeknownst to the website user.

38. In an endlessly reinforcing feedback loop staring with the TikTok app, moving to third-party websites that reveal a plethora of data about the user, and then returning back to the TikTok app now better informed to feed the user targeted content (*i.e.*, to connect the user with advertisers), Defendants have a data-driven business model unprecedented in scope that directly violates the privacy rights of U.S. citizens transacting in interstate commerce, and of Illinois citizens, Massachusetts citizens, Maryland citizens, and Missouri citizens.

39. Defendants have specifically targeted consumers in the United States, Illinois, Massachusetts, Maryland, and Missouri with advertising campaigns that appeared on television, online, and through other media promoting the TikTok app.[27]

---

[27] *See* Sam Bradley, *TikTok on TV: What Does the Social Media Platform's Ad Spend Tell Us?*, thedrum.com (Apr. 27, 2021), https://www.thedrum.com/news/2021/04/27/tiktok-tv-what-does-the-social-video-platform-s-ad-spend-tell-us; Todd Spangler, *TikTok Launches Biggest-Ever Ad Campaign as Its Fate*

40. Defendants embed computer code on the TikTop app that acts to intercept the Website Communications of a user of the TikTop app who links to a third-party website via TikTok's in-app browser.

41. After intercepting and capturing the Website Communications, Defendants use those Website Communications to recreate the user's entire visit to the websites. Defendants create and save video replay of the user's behavior on the website for analysis. This is the electronic equivalent of "looking over the shoulder" of each visitor to the websites for the entire duration of their website interaction.

42. The wiretaps engage as soon as the user clicks on a link in the TikTok app to a third-party website launching TikTok's in-app browser. Therefore, users are not provided with an opportunity to review any privacy policies or disclosures regarding deployment of the wiretaps on the third-party websites.

43. The Session Replay Code used by Defendants is not a cookie, tag, web beacon, or analytics tool. Unlike website analytics services that provide aggregate statistics, Session Replay Code is intended to record and play back the entirety of an individual's browsing session.

44. Defendants' actions through TikTok's in-app browser are not part of routine Internet functionality. As standard web browsers on mobile phones (*e.g.*, Google Chrome, Apple's Safari) do not record users with Session Replay Code, even the companies that created and host the third-party websites to which TikTok users link are unaware that these visitors to their websites are recorded by Defendants using Session Replay Code. Surreptitious interception and recording of a user's keystrokes, clicks, swipes, and text communications are contrary to the legitimate

---

Remains Cloudy, VARIETY (Aug. 18, 2020), https://variety.com/2020/digital/news/tiktok-advertising-brand-campaign-sale-bytedance-1234738607/ (both last visited Jan. 9, 2023).

expectation of TikTok users in the United States browsing the web via the TikTok app, and contrary to established industry norms.

45. Defendants maintain the records of users they have wiretapped, either through their own computer systems or through a third-party contractor.

46. Plaintiffs and other similarly situated TikTok users had no knowledge of, and did not give prior consent for, Session Replay Code recording her Website Communications on third-party websites she linked to from the TikTok App. Defendants never asked Plaintiffs or similarly situated TikTok users for permission to intercept and record her visits to third-party websites while using TikTok's in-app browser. Nevertheless, upon information and belief, the Session Replay Code that Defendants embedded into the TikTop app intercepted Plaintiffs and similarly situated TikTok users' Website Communications. These intercepted Website Communications were then stored by Defendants or its third-party contractor to be replayed later and used for Defendants' financial benefit.

47. At no point did Defendants inform Plaintiffs or similarly situated TikTok users in the United States of their surreptitious recording of her Website Communications as they browsed third-party websites while using the TikTok app.

CLASS ALLEGATIONS

48. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

> **Nationwide Class:** All natural persons in the United States within the applicable statute of limitations period who had their Website Communications captured through Session Replay Code activated by TikTok's in-app browser.
>
> **Massachusetts Subclass:** All natural persons who, while citizens of the state of Massachusetts and within the applicable statute of limitations period, had their Website Communications captured in Massachusetts through Session Replay Code activated by TikTok's in-app browser.

Maryland Subclass: All natural persons who, while citizens of the state of Maryland and within the applicable statute of limitations period, had their Website Communications captured in Maryland through Session Replay Code activated by TikTok's in-app browser.

Missouri Subclass: All natural persons who, while citizens of the state of Missouri and within the applicable statute of limitations period, had their Website Communications captured in Missouri through Session Replay Code activated by TikTok's in-app browser.

49. Excluded from the Classes are Defendants, their parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Classes, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

50. **Numerosity:** The class members are so numerous that individual joinder of all class members is impracticable. Upon information and belief, the Class exceeds 100,000 persons. The precise number of class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the records of Defendants.

51. **Commonality:** There are numerous questions of law and fact common to the Class, including but not limited to:

a. Whether Defendants violated the FWA;

b. Whether Defendants violated the Massachusetts Act;

c. Whether Defendants violated the Maryland Act;

d. Whether Defendants violated the Missouri Act;

e. Whether Defendants intercepted Plaintiffs' and the class members' electronic Website Communications;

f. Whether Defendants secured prior consent before intercepting Plaintiffs' and the class members' Website Communications; and

g. Whether Defendants are liable for damages provided under each statute alleged to be violated, and the amount of such damages.

52. **Typicality:** Plaintiffs' claims are typical of the claims of the class members, as they are all based on the same factual and legal theories.

53. **Adequacy of Representation:** Plaintiffs are representatives who will fully and adequately assert and protect the interests of the class and has retained competent counsel.

54. ***Declaratory and Injunctive Relief.*** Rule 23(b)(2) of the Federal Rules of Civil Procedure: Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and Class members, thereby making appropriate declaratory relief, with respect to the Classes as a whole.

55. Plaintiffs seek preliminary and permanent injunctive and equitable relief on behalf of the entire Class, on grounds generally applicable to the entire Class, to enjoin and prevent Defendant from engaging in the acts described above, such as continuing to record website communications through TikTok's in-app browser.

56. Unless a class is certified, Defendant will retain monies received as a result of their conduct that were taken from Plaintiffs and the Class members. Unless a Class-wide injunction is issued, Defendant will continue to commit the violations alleged and the members of the Class will continue to be unlawfully eavesdropped upon.

57. **Superiority:** In this lawsuit, a class action is superior to all other available methods for its fair and efficient adjudication because individual litigation of the claims of all class members is economically infeasible and procedurally 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.

58. **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. If Defendants intercepted Plaintiffs' and class members' communications, then Plaintiffs and each class member suffered damages by that conduct.

CAUSES OF ACTION

COUNT I
Violation of the Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*
(On Behalf of the Nationwide Class)

59. Plaintiffs re-allege and incorporates paragraphs 1 through 58 as if fully set forth herein.

60. Plaintiffs bring this claim individually and on behalf of the Nationwide Class.

61. The Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, prohibits he interception of any wire, oral, or electronic communications without the consent of at least one authority party to the communication. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

62. "Person" is defined as including "any individual, partnership, association, joint stock company, trust, or corporation. *Id.* § 2510(6).

63. Defendants, as corporations, are each "persons" under the FWA.

64. "Intercept" is defined as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

65. "Contents" is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

66. "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 that affects interstate or foreign commerce. . . ." *Id.* § 2510(12).

67. Plaintiffs' and the putative Nationwide Class members' keystrokes, clicks, scrolling and swiping finger movements, text typed, and other interactions with websites via TikTok's in-app browser are "contents" of "electronic communications" under 18 U.S.C. § 2510(12).

68. Session Replay Code like that used by Defendants is an "electronic, mechanical or other device" "used to intercept a wire, oral, or electronic communication" under the FWA.

69. Defendants intentionally employ Session Replay Code to automatically and indiscriminately spy on and intercept website visitors' electronic communications as they take place in real time, in violation of 18 U.S.C. § 2520(a).

70. Plaintiffs and the Nationwide Class members did not give prior consent to having their communications intercepted by Defendants. In fact, Plaintiffs and the Nationwide Class members reasonably expected under the circumstances that their electronic communications would not be intercepted.

71. Nor did the third-party websites, as the other parties to the communications, give prior consent to having those communications intercepted by Defendants, and Defendants never sought to or did obtain the third-party websites' consent.

72. At all relevant times, Defendants' conduct was knowing and intentional. Experts who uncovered the JavaScript injections included in Defendants' in-app browser explained that the inclusion of the JavaScript injections were intentional, non-trivial engineering tasks—the kind that do not happen by mistake or randomly.[28]

73. Plaintiffs and the Nationwide Class members are each entitled to "such preliminary and other equitable or declaratory relief as may be appropriate"; "(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000"; and punitive damages. 18 U.S.C. § 2520(b), (c).

74. Plaintiffs and the Nationwide Class are also entitled to a "reasonable attorney's fee and other litigation costs reasonably incurred." *Id*. § 2520(b)(3).

COUNT II
Violation of the Massachusetts Wiretap Act, Mass. Gen. Laws Ann. 272 § 99
(On Behalf of the Massachusetts Subclass)

75. Plaintiff Paige re-alleges and incorporates paragraphs 1 through 58 as if fully set forth herein.

76. Paige brings this claim individually and on behalf of the Massachusetts Subclass.

[28] Richard Nieva, *TikTok's In-App Browser Includes Code that Can Monitor Your Keystrokes, Researcher Says*, FORBES (Aug. 18, 2022), https://www.forbes.com/sites/richardnieva/2022/08/18/tiktok-in-app-browser-research/?sh=5b801c317c55 (last visited Jan. 9, 2023).

77. Massachusetts, along with at least nine other U.S. states, is a "two-party consent" state, *i.e.*, a jurisdiction in which all parties to a conversation must consent to the recording of the conversation.

78. Consistent with this, the Massachusetts Act bars the surreptitious interception and recording of private communications. Mass Gen. Laws Ann. 272 § 99.

79. It is a violation of the Massachusetts Act for any person to willfully commit an interception, attempt to commit an interception, or procure any other person to commit an interception or attempt to commit an interception of any wire communication. *Id.* § 99(C)(1).

80. Further, it is a violation for any person to willfully use, or attempt to use, "the contents of any wire . . . communication, knowing that the information was obtained through interception." *Id.* § 99(C)(3)(b).

81. "Person" includes "any individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 99(B)(13).

82. Defendants, as corporations, are each "persons" under the Massachusetts Act.

83. "Interception" is defined as "to secretly record . . . the contents of any wire . . . communications through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication." *Id.* § 99(B)(4).

84. "Wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." *Id.* § 99(B)(1).

85. "Contents" is defined as either "any information concerning the identity of the parties to such communication," or any information concerning the "existence, contents, substance, purport, or meaning of that communication." *Id.* § 99(B)(5).

86. Paige's and the putative Massachusetts Subclass members' keystrokes, clicks, scrolling and swiping finger movements, text typed, and other interactions with websites via TikTok's in-app browser are "contents" of communications under the Massachusetts Act.

87. Session Replay software like that used by Defendants is an "intercepting device" "used to secretly record the contents of wire communications" under the Massachusetts Act.

88. Defendants willfully employ Session Replay Code to automatically and indiscriminately spy on and intercept website visitors' electronic communications as they take place in real time, in violation of Section 99(C)(1).

89. Paige and the Massachusetts Subclass members did not give prior consent to having their communications with third-party website operators intercepted by Defendants. In fact, Paige and the Massachusetts Subclass members reasonably expected under the circumstances that their electronic communications would not be intercepted.

90. Nor did the third-party websites, as the other parties to the communications, give prior consent to having those communications intercepted by Defendants, and Defendants never sought to or did obtain the third-party websites' consent.

91. Defendants violated Section 99(C)(3)(b) by using the unlawfully intercepted electronic communications to inform their marketing tactics, including as to individual users.

92. At all relevant times, Defendants' conduct was willful.

93. Pursuant to Section 99(Q), Paige and the Massachusetts Subclass members are each entitled to "actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, which is higher;" and punitive damages.

94. Paige and the Massachusetts Subclass is also entitled to a "reasonable attorney's fee and other litigation disbursements reasonably incurred." *Id*.

COUNT III
Violation of the Maryland Wiretap Act, Md. Cts. & Jud. Pro. §§ 10-401 *et seq.*
(On Behalf of the Maryland Subclass)

95. Plaintiff Tanzymore re-alleges and incorporates paragraphs 1 through 58 as if fully set forth herein.

96. Tanzymore brings this claim individually and on behalf of the Maryland Subclass.

97. Maryland, along with at least nine other U.S. states, is a "two-party consent" state, *i.e.*, a jurisdiction in which all parties to a conversation must consent to the recording of the conversation.

98. Consistent with this, the Maryland Act bars the surreptitious interception and recording of private communications. Md. Cts. & Jud. Pro. § 10-402.

99. It is a violation of the Maryland Act for any person to "[w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." *Id.* § 10-402(a)(1).

100. Further, it is a violation for any person to willfully use, or endeavor 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." *Id.* § 10-402(a)(3).

101. "Person" includes "any individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 10-401(14).

102. Defendants, as corporations, are each "persons" under the Maryland Act.

103. "Intercept" is defined as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id*. § 10-401(10).

104. "Contents" is defined as either "any information concerning the identity of the parties to such communication," or any information concerning the "existence, contents, substance, purport, or meaning of that communication." *Id.* § 10-401(4).

105. "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." *Id.* § 10-401(5)(i).

106. Tanzymore and the putative Maryland Subclass members' keystrokes, clicks, scrolling and swiping finger movements, text typed, and other interactions with websites via TikTok's in-app browser are contents of electronic communications under the Maryland Act.

107. Defendants willfully employ Session Replay Code to automatically and indiscriminately spy on and intercept website visitors' electronic communications as they take place in real time, in violation of Section 10-402.

108. Tanzymore and the Maryland Subclass members did not give prior consent to having their communications with third-party website operators intercepted by Defendants. In fact, Tanzymore and the Maryland Subclass members reasonably expected under the circumstances that their electronic communications would not be intercepted.

109. Nor did the third-party websites, as the other parties to the communications, give prior consent to having those communications intercepted by Defendants, and Defendants never sought to or did obtain the third-party websites' consent.

110. Defendants violated Section 10-402 by using the unlawfully intercepted electronic communications to inform their marketing tactics, including as to individual users.

111. At all relevant times, Defendants' conduct was willful.

112. Pursuant to Section 10-403, Tanzymore and the Maryland Subclass members are each entitled to "[a]ctual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, which is higher;" and punitive damages.

113. Tanzymore and the Maryland Sublcass also entitled to a "reasonable attorney's fee and other litigation disbursements reasonably incurred." *Id.*

COUNT IV
Violation of the Missouri Wiretap Act, Mo. Stat. §§ 542.400 *et seq.*
(On Behalf of the Missouri Subclass)

114. Plaintiff Carolyn Smith re-alleges and incorporates paragraphs 1 through 58 as if fully set forth herein.

115. Carolyn Smith brings this claim individually and on behalf of the Missouri Subclass.

116. Missouri, along with at least nine other U.S. states, is a "two-party consent" state, *i.e.*, a jurisdiction in which all parties to a conversation must consent to the recording of the conversation.

117. Consistent with this, the Missouri Act bars the surreptitious interception and recording of private communications. Mo. Stat. § 542.402.

118. It is a violation of the Missouri Act for any person to knowingly intercept, endeavor to intercept, or procure any other person to intercept any wire communication. *Id.* § 542.402(1).

119. Further, it is a violation for any person knowingly use, or endeavor to use, "the contents of any wire communication, when he knows or has reason to know that the information was obtained through the interception of a wire communication." *Id.* § 542.402(4).

120. "Person" includes "any individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 542.400(9).

121. Defendants, as corporations, are each "persons" under the Maryland Act.

122. "Intercept" is defined as the "acquisition of the contents of any wire communication through the use of any electronic or mechanical device." *Id*. § 542.400(6).

123. "Contents" is defined as either "any information concerning the identity of the parties, the substance, purport, or meaning of that communication." *Id.* § 542.400(3).

124. "Wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications." *Id.* § 542.400(12).

125. Carolyn Smith and the putative Missouri Subclass members' keystrokes, clicks, scrolling and swiping finger movements, text typed, and other interactions with websites via TikTok's in-app browser are contents of electronic communications under the Missouri Act.

126. Defendants knowingly employ Session Replay Code to automatically and indiscriminately spy on and intercept website visitors' communications as they take place in real time, in violation of Section 542.402, Missouri Statutes.

127. Carolyn Smith and the Missouri Subclass members did not give prior consent to having their communications with third-party website operators intercepted by Defendants. In fact, Carolyn Smith and the Missouri Subclass members reasonably expected under the circumstances that their communications would not be intercepted.

128. Nor did the third-party websites, as the other parties to the communications, give prior consent to having those communications intercepted by Defendants, and Defendants never sought to or did obtain the third-party websites' consent.

129. Defendants violated Section 542.402 by using the unlawfully intercepted communications to inform their marketing tactics, including as to individual users.

130. At all relevant times, Defendants' conduct was knowing and intentional.

131. Pursuant to Section 542.418, Carolyn Smith and the Missouri Subclass members are each entitled to "[a]ctual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, which is higher;" and punitive damages.

132. Carolyn Smith and the Missouri Subclass is also entitled to a "reasonable attorney's fee and other litigation disbursements reasonably incurred." *Id*.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class alleged herein, respectfully request that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the Class under Federal Rule of Civil Procedure 23 and naming Plaintiffs as the representatives for the Class and Plaintiffs' attorneys as Class Counsel;

B. Declaring that Defendants' conduct violates the FWA, the Massachusetts Act, the Maryland Act, and the Missouri Act;

C. Finding in favor of Plaintiffs and the Class members on the claim asserted herein;

D. Enjoining Defendants to desist from further recording of private communications via TikTok's in-app browser, and awarding such other injunctive relief as the Court deems appropriate;

E. Awarding Plaintiffs and the Class members actual damages, statutory and liquidated damages, punitive damages, and disgorgement, in amounts to be determined by the Court or by the jury at trial;

F. Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest; and

G. Awarding Plaintiffs and the Class members their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR JURY TRIAL

Plaintiffs and the putative class members hereby demand a trial by jury, pursuant to Fed. R. Civ. P. 38(b), on all issues so triable.

Dated: January 10, 2023.

Respectfully submitted,

/s/ Jeff Ostrow
Jeff Ostrow
Steven P. Sukert
Jonathan M. Streisfeld
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
sukert@kolawyes.com
ostrow@kolawyers.com
streisfeld@kolawyers.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiffs and the Putative Class