Exhibit A

Filing # 127493815 E-Filed 05/25/2021 02:08:09 PM

IN THE CIRCUIT COURT OF THE SEVENTEETH JUDICIAL CIRCUIT IN AND FOR BROWARD COUNTY, FLORIDA

DANIEL LUBIN, on behalf of himself and others similarly situated, Plaintiff, v. BANK OF AMERICA, N.A, a Delaware corporation, Defendant.	No. CACE21-010486 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Daniel Lubin ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant Bank of America, N.A. ("Defendant") for wiretapping the electronic communications of visitors to bankofamerica.com (the "Websites") and the Bank of America App (the "App"). .

2. The wiretaps, which are embedded in the computer code on the Websites and the App, are used by Defendant to secretly observe and record visitors' keystrokes, mouse clicks, swipes, gestures and other electronic communications, including the entry of Personally Identifiable Information ("PII") into the App and Websites' forms, in real time.

3. To accomplish this wiretapping, Defendant uses tracking, recording, and/or "session replay" software to secretly observe and record Plaintiff's and Class Members' electronic

communications with the Websites and the App, including their keystrokes, mouse movements, swipes, gestures and clicks, information inputted into the Websites and the App, and/or pages and content viewed on the Websites and the App.

4. Defendant intercepted or allowed for the interception of the electronic communications at issue without the knowledge or prior consent of Plaintiff and the Class Members, for its own financial gain.

5. By doing so, Defendant has violated Florida's Security of Communications Act ("FSCA"), Fla. Stat. §§ 934.03 and 934.04, and invaded Plaintiff's and Class Members' privacy rights in violation of Florida law.

6. From May 2020 through May 2021, Plaintiff visited the Websites and used the App. During the visits and App usage, Defendant captured, stored, and analyzed Plaintiff's electronic communications in real time through a third party, Glassbox, Inc., including Plaintiff's mouse clicks, keystrokes, swipes, gestures, personal checking and savings accounts, credit score, banking transactions and payment card information, as well as any other information input into the Websites' or the App's forms.

7. Plaintiff brings this action on behalf of himself and a class of all persons whose electronic communications were intercepted through the use of Defendant's wiretap on the Websites and the App.

THE PARTIES

8. Plaintiff Daniel Lubin is a Florida resident who lives in Fort Lauderdale, Florida. From May 2020 through May 2021, prior to the filing of this lawsuit, Mr. Lubin visited the Websites and used the App. Mr. Lubin was in Fort Lauderdale, Florida when he visited the Websites and used the App. During the visits, Mr. Lubin's keystrokes, mouse clicks, swipes, gestures and other electronic communications—including the entry of his personal checking and

savings accounts, credit score, banking transactions and payment card information—were intercepted in real time by Defendant and was disclosed to a third party, Glassbox, Inc. ("Glassbox"), through the wiretap. Mr. Lubin was unaware at the time that his keystrokes, mouse clicks, swipes, gestures and other electronic communications, including the data he input into the Websites' and the App's forms, were being intercepted in real-time and would be disclosed to Glassbox, nor did Mr. Lubin consent to the same.

9. Defendant Bank of America, N.A. is a national banking association chartered under the laws of the United States and incorporated in Delaware with its principal place of business in North Carolina.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

11. This Court has personal jurisdiction over Defendant because the Defendant has purposefully availed themselves of the laws and benefits of doing business in this State, and Plaintiff's claims arise out of the Defendant's forum-related activities. Furthermore, a substantial portion of the events giving rise to Plaintiff's claims occurred in this District. In fact, the information Bank of America gathers through its wiretap includes geolocation information, and therefore Bank of America knows it is wiretapping users in Florida, including the Plaintiff.

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

STATEMENT OF FACTS
Overview Of The Wiretaps

13. While many websites have third-party analytics scripts that record pages visited and searches made, certain websites are now using "session replay" scripts. These scripts record keystrokes, mouse movements, and scrolling behavior, along with the entire contents of the pages users visit, and send them to third-party servers. Unlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions, as if someone is looking over your shoulder as you interact with the website.

14. Glassbox is a company that developed and controls such a feature. Glassbox's software feature is called "Session Replay," and purports to help businesses improve customer experiences with their website and app.

15. Session Replay provides a real-time recording of a user's interactions on a website. Glassbox says that Session Replay "is the black box of your website and app, capturing every click, tap, scroll and swipe. Glassbox automatically records all activity alongside events on IT systems, enabling you to use session replay to identify technical issue without having to recreate the experience." As a result, Glassbox can see the mouse clicks and other interactions with Glassbox's clients' websites and apps, including the information input into websites' forms, as well as metadata associated with the website's visitor, including their geolocation.[1]

16. As described by Glassbox:

> Wouldn't it be easier if you could just see a "video" of what happened? From the moment the customer entered their password, where did their fingers move on the phone screen? What did they actually see on the screen? At what point did they give up and leave the app? What was their journey to check out?
> . . .

[1] GLASSBOX, *Capture every moment from every user with session replay*, https://glassbox.com/session-replays/ (last visited May 20, 2021).

> At Glassbox, we explain website and app session recording simply as the recording of every session on an organization's website or native app, exactly as seen by the customer, regardless of the device (laptop, tablet, mobile) or browser used to access the channel. You see exactly what the customer is seeing or doing on your site.[2]

17. This is consistent with the description of GlassBox's technology in its patent, which identifies it as "A web session recording system" that ensures "that each web session is recorded and can be later on replayed in various manners (e.g. a playback an entire web session)."[3]

18. Session Replay operates on both desktop and mobile devices.

19. Session Replay is accomplished by JavaScript, consumer-side recording. It captures the consumer-rendered HTML and active states of the page, and all interactions, including data input, on the page. It then stitches all of these interactions together into a combined recording of the customer's experience on a website.

20. Through Session Replay, Glassbox records a website user's interactions and transmits that information to Glassbox's recording servers. Glassbox then makes the information available to its clients.

21. However, technology like Glassbox's is not only highly intrusive, but dangerous. A 2017 study by Princeton University found that "the extent of data collected by these services far exceeds user expectations; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can't reasonably be expected to be kept anonymous. In fact, some companies allow publishers to explicitly link recordings to a user's real identity." Session recording technologies like Session

---

[2] Yaron Gueta, *The definitive guide to session replay tools*, GLASSBOX BLOG (May 8, 2020), https://www.glassbox.com/blog/the-definitive-guide-to-session-replay-recording.

[3] U.S. Patent No. 10341205 (filed July 2, 2019), https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=6&f=G&l=50&d=PTXT&p=1&S1=glassbox&OS=glassbox&RS=glassbox.

Replay were found to be collecting sensitive information inputted by users such as passwords and credit card numbers.[4]

22. The Princeton study continued:

> "Collection of page content by third-party replay scripts may cause sensitive information such as medical conditions, credit card details and other personal information displayed on a page to leak to the third-party as part of the recording. This may expose users to identity theft, online scams, and other unwanted behavior. The same is true for the collection of user inputs during checkout and registration processes.
>
> The replay services offer a combination of manual and automatic redaction tools that allow publishers to exclude sensitive information from recordings. However, in order for leaks to be avoided, publishers would need to diligently check and scrub all pages which display or accept user information. For dynamically generated sites, this process would involve inspecting the underlying web application's server-side code. Further, this process would need to be repeated every time a site is updated or the web application that powers the site is changed."[5]

23. The Princeton study concluded that the difficulty of redaction necessitating user customization is directly in conflict with the marketing of this technology as "plug and play."[6]

24. In an article published in *The Atlantic* magazine, Glassbox was identified specifically as problematic because, despite their purported usefulness, "the replays also risk capturing sensitive information such as credit-card or passport numbers" without proper disclosures to users. The article notes that Glassbox's marketing vice president, Audelia Boker,

---

[4] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, FREEDOM TO TINKER (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[5] *Id.*

[6] *Id.*

claims in a promotional video "[b]ecause banks are so large, a single banking customer can generate as many as 3 billion recorded sessions a month."[7]

25. Glassbox's business model involves entering into voluntary partnerships with various companies and providing their software to their partners.

26. One of Glassbox's partners is the Defendant, Bank of America.

27. The Defendant utilizes Glassbox's software on the Websites and the App.

28. The Defendant knows that Glassbox's software captures the keystrokes, mouse clicks, swipes, gestures and other communications of visitors to its Websites and App, including data input into the Websites' and Apps' forms, and pays Glassbox to intercept that information.

29. Pursuant to an agreement with Glassbox, the Defendant enabled Glassbox's software by voluntarily embedding Session Replay on the Websites and the App.

30. As currently deployed by the Defendant, Session Replay functions as a wiretap that delivers recordings of users interactions with the Websites and the App in real time to Glassbox.

Defendant Wiretapped Plaintiff's Electronic Communications

31. From May 2020 through May 2021, Plainitff visited the Website and used the App to conduct personal banking transactions.

32. During these visits, and upon information and belief, the Session Replay feature in Glassbox's software captures each of Plaintiff's keystrokes, gestures, swipes and mouse clicks on the Websites and the App. The Glassbox wiretap also captured the date and time of the visits, the duration of the visits, Plaintiff's IP address, his location at the time of the visits, his browser type,

[7] Sidney Fussell, *The Analysts Recording Your Screen Say It's for Your Own Good*, THE ATLANTIC (Feb. 12, 2019), https://www.theatlantic.com/technology/archive/2019/02/apple-glassbox-screen-record-banks/582433/.

and the operating system on his device, and any information provided in response to Plaintiff's inputs on the Websites' forms, including but not limited to name, address, account numbers, and personal bank account information.

33. Glassbox's recording of keystrokes, mouse clicks, swipes, gestures, data entry, and other electronic communications begins the moment a user accesses or interacts with the Websites or the App.

34. When users access the Websites and the App, they enter their and PII and conduct personal banking transactions that involve sensitive information including account numbers, social security numbers and credit score.

35. Glassbox's software captures these electronic communications throughout each step of the process.

36. Glassbox's software captures, among other things:

(a) The user's mouse clicks;
(b) The user's keystrokes;
(c) The user's email address;
(d) The user's shipping address;
(e) The user's credit and debit card information, including card number, expiration date, and CVV code;
(f) The user's IP address;
(g) The user's their location at the time of the visit; and
(h) The user's browser type and the operating system on their devices.

37. Crucially, Defendant Bank of America does not ask users, including Plaintiff—who entered all of this information—whether they consent to being wiretapped by Glassbox. Users are never actively told that their electronic communications are being wiretapped by Glassbox.

38. Further, Bank of America's Privacy Policy is located at the very bottom of the Website's home page with no notice directing users to the Privacy Policy, i.e. the hyperlink to the

Privacy Policy functions as browserwrap. Additionally, the Defendant began recording users before any purported disclosure was made *after* the wiretap had already begun.

39. Therefore, users like Plaintiff never agree or are never given the option to agree to the Privacy Policy when using the Websites or the App, nor are they on notice of the Privacy Policy.

40. Even if users do agree to the Privacy Policy by using the Websites or otherwise—and they do not for the reasons stated above—Bank of America does not mention any aspect of Glassbox or its Session Replay (such as that users will have their mouse clicks and keystrokes recorded in real time) in the Websites' Privacy Policy. As such, users do not agree to be wiretapped even if they agree to the Privacy Policy.

41. Neither Plaintiff nor any Class member consented to being wiretapped on the Websites or the App, or to have their communications recorded and shared with Glassbox. Any purported consent that was obtained was ineffective because (i) the wiretapping began from the moment Plaintiff and Class members accessed the Websites or the App; (ii) the Privacy Policy did not disclose the wiretapping or Glassbox; and (iii) the hyperlink to the Privacy Policy is inconspicuous and therefore insufficient to provide notice.

42. In fact, unlike the Websites or the App, other websites and apps actively disclose the use of session recording technology by implementing a pop-up screen that a user must acknowledge before advancing further on a website.

CLASS ACTION ALLEGATIONS

43. Plaintiff seeks to represent a class of all Florida residents who visited the Websites or the App, and whose electronic communications were intercepted or recorded by Glassbox.

Plaintiff reserves the right to modify the class definition as appropriate based on further investigation and discovery obtained in the case.

44. Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the thousands. The precise number of Class members and their identities are unknown to Plaintiff 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 distribution records of Defendant.

45. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendant has violated the Florida Security of Communications Act ("FSCA"), Fla. Stat. §§ 934.03 and 934.04 and invaded Plaintiff's privacy rights in violation of Florida law; and whether class members are entitled to actual and/or statutory damages for the aforementioned violations.

46. The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other class members, visited the Websites and the App and had his electronic communications intercepted and disclosed to Glassbox through the use of Glassbox's wiretaps.

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

48. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

49. Plaintiff brings all claims in this action individually and on behalf of members of the Class against Defendant.

COUNT I
Violation of The Florida Security of Communications Act
Fla. Sta. § 934.03

50. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

52. To establish liability under section 934.03, a plaintiff need only establish that a defendant:

(a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;

(b) Intentionally uses, endeavors to use, or procures any other person to use or

endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

1. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

2. Such device transmits communications by radio or interferes with the transmission of such communication;

(c) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication intercepted by means authorized by subparagraph (2)(a)2., paragraph (2)(b), paragraph (2)(c), s. 934.07, or s. 934.09 when that person knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, has obtained or received the information in connection with a criminal investigation, and intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

53. Pursuant to Fla. Stat. 934.02, "'Electronic communication' means 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 intrastate, interstate, or foreign commerce …," such as through the internet.

54. At all relevant times, Glasssbox's software, including the Session Replay feature, was intentionally used by Defendant to intercept, endeavor to intercept, use, endeavor to use, disclose, and/or endeavor to disclose Plaintiff's and Class Members' electronic communications.

55. At all relevant times, by using Glassbox's technology, Defendant willfully and without the consent of all parties to the communication, in an unauthorized manner, read or

attempted to read or learn the contents or meaning of electronic communications of Plaintiff and putative Class Members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within Florida.

56. Defendant aided, agreed with, and conspired with each other to implement Glassbox's technology and to accomplish the wrongful conduct at issue here.

57. Plaintiff and Class Members did not consent to any of Defendant's actions in implementing Glassbox's wiretaps on the Websites and the App. Nor have Plaintiff or Class Members consented to Defendant's intentional access, interception, reading, learning, recording, and collection of Plaintiff and Class Members' electronic communications.

58. The violation of section 934.03 constitutes an invasion of privacy sufficient to confer Article III standing.

59. Unless enjoined, Defendant will continue to commit the illegal acts alleged here. Plaintiff continues to be at risk because he uses the internet for online banking, and continues to desire to use the internet for that purpose.

60. Plaintiff and Class Members seek all relief available under Fla. Stat. § 934.10, including declaratory and injunctive relief, statutory damages at the rate of $100 a day for each day of violation or $1,000, whichever is higher, punitive damages, attorneys' fees, and costs.

COUNT II
Violation of The Florida Security of Communications Act
Fla. Sta. § 934.04

61. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

63. Section 934.04 provides a private right of action against "Any person who intentionally:

> (a) Sends through the mail or otherwise sends or carries any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the illegal interception of wire, oral, or electronic communications as specifically defined by this chapter; or
> (b) Manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the illegal interception of wire, oral, or electronic communications as specifically defined by this chapter …."

64. At all relevant times, by implementing Glassbox's wiretaps, Defendant intentionally manufactured, assembled, possessed, and/or sold a wiretap device that is primarily or exclusively designed or intended for eavesdropping upon the communications of another.

65. Glassbox's code is a "device" that is "primarily useful" for eavesdropping. That is, the Glassbox's code is designed to gather PII, including keystrokes, mouse clicks, swipes, gestures and other electronic communications.

66. Plaintiff and Class Members did not consent to any of Defendant's actions in implementing Glassbox's wiretaps.

67. Plaintiff and Class Members seek all relief available under Fla. Stat. § 934.10, including declaratory and injunctive relief, statutory damages at the rate of $100 a day for each day of violation or $1,000, whichever is higher, punitive damages, attorneys' fees, and costs.

COUNT III
Invasion Of Privacy Under Florida Law

68. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

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

71. At all relevant times, by implementing Glassbox's wiretaps on Bank of America\s Websites and App, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under Florida law.

72. Plaintiff and Class Members had a reasonable expectation that their PII and other data, including personal banking transactions would remain confidential and that Defendant would not install wiretaps on the Websites or the App.

73. Plaintiff and Class Members did not consent to any of Defendant's actions in implementing Glassbox's wiretaps on the Websites or the App.

74. This invasion of privacy is serious in nature, scope and impact.

75. This invasion of privacy alleged here constitutes an egregious breach of the social norms underlying the privacy right.

76. Plaintiff and Class Members seek all relief available for invasion of privacy claims under Florida law.

PRAYER FOR RELIEF

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

(a) For an order certifying the Class under Rule 23 and naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

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

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

(d) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

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

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

DEMAND FOR TRIAL BY JURY

Plaintiff demands a jury trial on all claims so triable.

Respectfully Submitted,

Daniel Lubin, individually and on behalf of those similarly situated individuals

Dated: May 25, 2021

/s/ Avi Kaufman
Avi R. Kaufman (FL Bar no. 84382)
kaufman@kaufmanpa.com
Rachel E. Kaufman (FL Bar no. 87406)
rachel@kaufmanpa.com
KAUFMAN P.A.
400 NW 26th Street
Miami, FL 33127
Telephone: (305) 469-5881

Robert R. Ahdoot (*pro hac vice* to be filed)
rahdoot@ahdootwolfson.com
Christopher E. Stiner (*pro hac vice* to be filed)
cstiner@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 West Olive Ave., Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111

Counsel for Plaintiff and the Putative Class