LIC 117-001119
4-20-26
BW 9:22 am

HECTOR LOMBARD,
Plaintiff,

VS.

[redacted],
an Illinois Corporation,

Defendant.
_____/

IN THE COUNTY COURT IN AND FOR BROWARD COUNTY, FLORIDA

CASE NO. COWE-26-028474
JUDGE: Ellen Feld
DIV: 83

STATE OF FLORIDA – NOTICE TO PLAINTIFF(S) AND DEFENDANT(S)

[redacted]

YOU ARE HEREBY NOTIFIED that you are required to appear in person or by attorney at the Broward County Courthouse in Courtroom_____, located at_____, _____ on_____at_____for a **PRETRIAL CONFERENCE** before a Judge of this court.

IMPORTANT – READ CAREFULLY
THE CASE WILL NOT BE TRIED AT THAT TIME.
DO NOT BRING WITNESSES--APPEAR IN PERSON OR BY ATTORNEY.

The defendant(s) must appear in court on the date specified in order to avoid a default judgment. The plaintiff(s) must appear to avoid having the case dismissed for lack of prosecution. A written MOTION or ANSWER to the court by the plaintiff(s) or the defendant(s) shall not excuse the personal appearance of a party or its attorney in the PRETRIAL CONFERENCE. The date and time of the pretrial conference CANNOT be rescheduled without good cause and prior court approval.

A corporation may be represented at any stage of the trial court proceedings by an officer of the corporation or any employee authorized in writing by an officer of the corporation. Written authorization must be brought to the Pretrial Conference.

The purpose of the pretrial conference is to record your appearance, to determine if you admit all or part of the claim, to enable the court to determine the nature of the case, and to set the case for trial if the case cannot be resolved at the pretrial conference. You or your attorney should be prepared to confer with the court and to explain briefly the nature of your dispute, state what efforts have been made to settle the dispute, exhibit any documents necessary to prove the case, state the names and addresses of your witnesses, stipulate to the facts that will require no proof and will expedite the trial, and estimate how long it will take to try the case.

Mediation may take place at the pretrial conference. Whoever appears for a party must have full authority to settle. Failure to have full authority to settle at this pretrial conference may result in the imposition of costs and attorney fees incurred by the opposing party.

Pretrial Information: Appear at
100 North Pine Island Road,Plantation, FL 33324
on 06/02/2026 at 2:00 PM
in West Courtroom 240.

If you admit the claim, but desire additional time to pay, you must come and state the circumstances to the court. The court may or may not approve a payment plan and withhold judgment or execution or levy.

RIGHT TO VENUE. The law gives the person or company who has sued you the right to file in any one of several places as listed below. However, if you have been sued in any place other than one of these places, you, as the defendant(s), have the right to request that the case be moved to a proper location or venue. A proper location or venue may be one of the following: (1) where the contract was entered into; (2) if the suit is on an unsecured promissory note, where the note is signed or where the maker resides; (3) if the suit is to recover property or to foreclose a lien, where the property is located; (4) where the event giving rise to the suit occurred; (5) where any one or more of the defendants sued reside; (6) any location agreed to in a contract; (7) in an action for money due, if there is no agreement as to where the suit may be filed, where payment is to be made.

If you, as the defendant(s), believe the plaintiff(s) has/have not sued in one of these correct places, you must appear on your court date and orally request a transfer, or you must file a **WRITTEN** request for transfer in affidavit form (sworn to under oath) with the court 7 days prior to your first court date and send a copy to the plaintiff(s) or plaintiff(s) attorney, if any.

A copy of the statement of claim shall be served with this summons.

DATED at_____Florida, on APR 17 2026

Attorneys for Plaintiff
Abdul-Sumi Dalal, Esq.
Veronika Balbuzanova, Esq., CIPP/US

JOHNSON DALAL
111 N. Pine Island Road, Suite 105
Plantation, FL 33324
Telephone: (954) 507-4500
Email: AD@JohnsonDalal.com
Email: VB@JohnsonDalal.com

BRENDA D. FORMAN AS
CLERK OF THE COURT

By_____

CLERK OF CIRCUIT & COUNTY COURT
IN GOD WE TRUST
FLORIDA
BROWARD COUNTY

BRENDA D. FORMAN

If you are a person with a disability who needs any accommodation in order to participate in this proceeding, you are entitled, at no cost to you, to the provision of certain assistance. Please contact the ADA Coordinator, Room 20140, 201 S.E. Sixth Street, Fort Lauderdale, Florida 33301, 954-831-7721 at least 7 days before your scheduled court appearance, or immediately upon receiving this notification if the time before the scheduled appearance is less than 7 days. If you have a hearing or voice disability you can contact the court through the Florida Relay Service by calling 711.

Filing # 245956309 E-Filed 04/14/2026 02:53:06 PM

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

Case No:

HECTOR LOMBARD,

Plaintiff,

v.

[redacted],
an Illinois Corporation,

Defendant.
_____/

COMPLAINT

Plaintiff, HECTOR LOMBARD ("Plaintiff"), brings this lawsuit against Defendant, [redacted] ("Defendant"), for violation of Florida's Security of Communications Act, Fla. Stat. § 934.01, *et seq.*, and alleges:

INTRODUCTION

1. This complaint is brought pursuant to Florida's Security of Communications Act ("FSCA"), Fla. Stat. § 934.01, *et seq*. This matter arises out of Defendant's unauthorized installation of third-party scripts (also colloquially referred to as third party "cookies"), on Plaintiff's web browser, without consent, which were used to de-anonymize Plaintiff's presence online, intercept electronic communications from Plaintiff's computer, and surveil Plaintiff's online activity across multiple websites, in violation of Florida law.

2. Because the information unlawfully taken from Plaintiff has commercial—and monetary—value, Plaintiff also seeks damages grounded in tort.

3. Internet users frequently experience the unsettling sensation that their online activity is being monitored. Whether through advertisements that appear ubiquitously after a product is viewed, or through targeted promotions that surface following casual conversation, Floridians—like Americans generally—reasonably believe they are being tracked and surveilled without their consent. They are correct.

4. A multi-billion-dollar industry, commonly referred to as "identity resolution," exists for the purpose of de-anonymizing consumers and effectively cyber-tracking them across the Internet for commercial gain. This occurs despite the fact that most Americans expect to remain anonymous online unless they affirmatively disclose identifying information.

5. Recent data indicates that approximately eighty-six percent (86%) of Americans intend to remain anonymous online and take affirmative steps to avoid being identified or monitored, and ninety percent (90%) believe they should have control over whether their information is shared. *See* Lee Rainie et al., *Part 1: The Quest for Anonymity Online*, PEW RESEARCH CENTER (Sept. 5, 2013), https://www.pewresearch.org/internet/2013/09/05/part-1-the-quest-for-anonymity-online; Jon Gingerich, *Online Privacy Becomes Top Concern in 2019*, O'DWYER'S (Jan. 4, 2019), https://www.odwyerpr.com/story/public/11834/2019-01-04/online-privacy-becomes-top-concern-2019.html.

6. Yet this Defendant—and the identity-resolution companies whose technologies Defendant deploys through scripts embedded on unsuspecting users' browsers—renders true anonymity, and consumer control over their own personally identifiable information ("PII"), virtually impossible.

7. Defendant operates a commercial website located at [redacted] (the "Website").

8. When a visitor lands on the Website, Defendant installs certain pen register and trap and trace ("PR/TT") processes in the form of JavaScript on the visitor's web browser, without first obtaining consent.

9. Defendant then uses these processes to intercept certain electronic data, for example, each visitor's IP address, so that third parties can de- anonymize, intercept, surveil, and/or target that visitor's information, all over the internet, for years.

10. Because the processes deployed by Defendant capture electronic "routing, addressing, or signaling information," they are a "pen register" or "trap and trace" pursuant to Fla. Stat. § 934.02 (20) and (21).

11. Notably, Plaintiff is not referring to session replay issues (whereby a company tracks a user's keystrokes and mouse movements on its own website), but rather, to the installation of spyware (e.g., third party scripts, pixels, and others) used to identify an otherwise anonymous user online via electronic addressing, routing, and/or signaling information, and to then secretly intercept and surveil that user's activity across multiple websites and platforms, without consent.

12. Absent a court order or express consent, using PR/TT violates Florida law. *See* Fla. Stat. § 934.31(1) ("[N]o person may install or use a pen register or a trap and trace device without first obtaining a court order").

13. Plaintiff seeks all civil remedies permitted by the FSCA because of this unlawful misconduct, including actual damages, liquidated damages, punitive damages, attorney's fees and costs, and litigation costs. Fla. Stat. § 934.10(1).

14. Plaintiff also seeks damages grounded in tort based on the commercial value of otherwise-private information, which was taken from Plaintiff, by Defendant, without consent.

15. Growing market research indicates that the value of consumers' personal data can be quantified into a specific dollar amount that runs as high as hundreds, or even thousands, of

dollars per consumer. *See, e.g.*, Kienzle, Martin G., *How much value are consumers giving away to feed the data economy?*, MEDIUM, Aug. 15, 2021, https://medium.com/@kienzle/how-much-value-are-consumers-giving-away-to-feed-the-data-economy-b44438bf6657 (noting that the "aggregate value [of consumer data] is at a minimum $500 per person per year, and likely higher than $1000 per year"); *What Are Data Brokers – And What Is Your Data Worth?*, WEBFX, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ (explaining that data brokering is a $200 billion industry and that, for example, **"[t]he average email address is worth $89 to a brand over time"**) (emphasis added); Stein, Lukas, *What your data is actually worth*, DATAPODS, Oct. 10, 2023, https://www.datapods.app/en-US/blog/what-your-data-is-actually-worth ("For example, general information about an individual, such as age, gender and location, has a price of around $0.0005 per person. The data of people who are looking for a car, a financial product or a holiday, is more expensive. If you want to buy a car, companies pay around $0.0021 for this information. The information that a woman is expecting a child is worth $0.11.").

PARTIES

16. At all times material hereto, Plaintiff was and is a citizen and resident of Broward County, Florida.

17. Upon information and belief, Defendant is an Illinois Corporation with its principal place of business at [redacted], and is otherwise *sui juris*.

18. At all times material hereto, Defendant was and is an Illinois Corporation, which owns, publishes, and operates the Website for profit; Defendant's Website is usable and viewable by consumers located inside Florida, who can order and pay for products through the Website from within Florida, which products are then delivered by Defendant to consumers in Florida.

19. Upon information and belief, Defendant has made and is making sales through the Website to customers located in Florida and/or has shipped products purchased through its Website to its Florida customers.

20. Furthermore, Defendant used the Website to install pen register and trap and trace processes on Plaintiff's web browser while Plaintiff and its computer were in Florida, which could then be used to unlawfully surveil Plaintiff's online activities, while Plaintiff was in Florida, in a manner that violated Florida law.

21. Plaintiff accessed the subject Website in Broward County, Florida and suffered injury in Broward County, Florida.

JURISDICTION AND VENUE

22. This is an action for damages that exceeds Five Hundred Dollars ($500.00) but does not exceed Two Thousand Five Hundred Dollars ($2,500.00), exclusive of interest, attorney's fees, and costs, and is otherwise within the jurisdiction of this Court.

23. Plaintiff reserves the right to amend this complaint to assert additional damages as provided in Fla. Stat. §§ 934.10, 934.27, as continuing or multiple FSCA violations may be revealed or identified during discovery.

24. Jurisdiction of this Court arises under Chapter 34.01, Florida Statutes, and the FSCA.

25. Upon information and belief, Defendant engaged in substantial and not isolated activity within this state by way of online marketing and sales, including by making online sales to Floridians in Florida, and subsequent shipment of Defendant's products into Florida.

26. Moreover, Defendant violated the privacy rights of Floridians in Florida by installing electronic surveillance processes on the computers of Floridians in Florida, capturing electronic data of Floridians without consent, capturing electronic data of Floridians without

consent, de-anonymizing the otherwise-private digital identity and data of Floridians online, which was then used to surveil and spy on Floridians in Florida, thus committing a tort (invasion of privacy) and an FSCA violation within this state.

FACTUAL ALLEGATIONS

27. The FSCA was promulgated by the Florida Legislature to safeguard privacy – including electronic privacy – of Floridians in Florida.

28. The FSCA mandates that "no person may install or use a pen register or a trap and trace device without first obtaining a court order under Section 934.33." Fla. Stat. § 934.31(1).[1]

29. Violation of this prohibition entitles Plaintiff to the civil remedies and damages set forth *supra*. Moreover, anyone who violates these requirements "is guilty of a misdemeanor of the first degree, punishable as provided" by Florida law. *Id.* § 934.31(5).

30. PR/TT devices were originally used by law enforcement to record incoming and outgoing telephone numbers, which were received and sent by a specific targeted telephone number. As technology advanced, PR/TT was used to record additional forms of electronic and digital information, including IP addresses and other digital identifying information; accordingly, federal law constantly broadened the definition of PR/TT to keep pace with evolving internet and other relevant technologies, and Florida has consistently adopted those expanding federal definitions.

31. In 1986, the Federal Wiretap Act, was amended to clarify that its prohibitions extend to electronic forms of communication; two years later, in 1988, the FSCA was amended to include that same clarification.

32. In its first legislative session following passage of the USA Patriot Act (the "Act"), the Florida Legislature amended the FSCA to adopt, word-for-word, the Act's definition of PR/TT,

1. Certain statutory exceptions exist that are inapplicable in this case because Defendant is not a telephone company, internet provider, or other provider of electronic or wire communication services.

including the addition of the words "a process" for recording "routing, processing, or signaling information" that is transmitted by an instrument through which electronic communications are sent, and "a process" that "captures electronic or other impulses," that can identify the originating "routing, addressing, or signaling information." 2002 Fla. HB 1439.

33. Accordingly, as of 2002, the Act and the FSCA define PR/TT identically. *See* Fla. Stat. § 934.02(20), (21) (defining "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but such information does not include the contents of any communication"; defining "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but such information does not include the contents of any communication").

34. By adopting the Act's definition of PR/TT, the FSCA deleted old language limiting PR/TT to mechanical systems or devices, and expanded PR/TT to include computer and internet related processes; indeed, to copy the Act, the Florida Legislature deleted the words "electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line" and replaced them with the words "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 2002 Fla. HB 1439; *see also, e.g.,* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 S. CAL. L. REV. 949, 982-89 (1996) (describing the evolution of the pen register from mechanical device to computer process).

35. Federal courts have consistently held the PR/TT language of the Act (and thus the FSCA) reaches communications and impulses sent through the Internet. *See, e.g., In re the*

Application of United States, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (the Act amended "the Pen/Trap Statute to include all 'dialing, routing, addressing, or signaling information,' thereby extending its coverage to Internet communications"); *In re Certified Question of Law*, 858 F.3d 591 (FISA Ct. Rev. 2016) ("USA PATRIOT Act made the pen register provisions applicable to a wide array of modern communications technologies, such as the Internet"); *In re the United States*, 2018 U.S. Dist. LEXIS 209036 (S.D. Fla. 18) ("definitions of 'pen register' and 'trap and trace device' were broadened to reach Internet communications in 2001").

36. Software that identifies consumers, gathers data, and correlates that data through unique "fingerprinting" is one collection tool that can be used as a PR/TT. *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023).

37. In addition to the prohibitions against unauthorized use of PR/TT processes, the FSCA prohibits any person or entity from intercepting, endeavoring to intercept, or procuring any third party to intercept or endeavor to intercept any electronic communication. Fla. Stat. § 934.03(1)(a).

38. It is unlawful to intercept any electronic communication under Florida law "unless all of the parties to the communication have given ***prior consent*** to such interception. *Id.* § 934.03(2)(d) (emphasis added).

39. It is also unlawful to intentionally use, or endeavor to use, the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication. *Id.* § 934.03(1)(d).

40. The FSCA defines "intercept" of an electronic communication as "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 934.02(3).

41. The penalties for unauthorized interception of an electronic communication are the same as for the unauthorized use of a PR/TT device.

42. Website operators, like Defendant, ignore legal requirements and monetize each visitor's PII by installing PR/TT processes on visitor web browsers without consent.

43. This is little more than spyware, which intercepts and collects PII, including, for example, each visitor's unique IP address, operating system name and version, browser name and version, language, geolocation information, email address, embedded social media identities, device signatures, and undeclared identifiers including subscriber lists, demographics, purchases/transactions, visits to online news sites, survey results, voter registration, motor vehicle records, and other such data embedded within the visitor's web browser history.

44. To be clear, Defendant is unlawfully intercepting and storing electronic communications sent by each visitor's computer, ***and additionally***, is installing PR/TT processes on each visitor's computer, to spy on otherwise private behavior on a forward-looking basis, on behalf of itself and/or third parties (as set forth in detail below), resulting in a double FSCA violation.

45. Even just by simply collecting electronic addressing and routing information in the form of a visitor's IP address, a website can discern significant personal identifying data and information.

46. An IP address is a unique identifier, expressed as four sets of three numbers (i.e. 123.456.789.012). The first six numbers reveal the network used by the website visitor, and the second six numbers reveal the device used by the visitor.

47. Knowledge of the visitor's IP address, standing alone, can reveal a range of PII, and is the first step in this unagreed fingerprinting process. Capturing the IP address of a website visitor allows the holder of that information to:

a. Perform a reverse lookup (the resolution of an IP address to its associated domain name) to obtain a computer name, which can lead to physical location information;

b. Conduct a traceroute (a computer diagnostic tool for displaying the route (path) of packets across an IP network) to find the logical path to the computer, which can reveal the physical location of the computer;

c. Determine the geolocation of the computer, with varying degrees of accuracy. Depending on the lookup tool used, this could include country, region/state, city, latitude/longitude, telephone area code and a location-specific map;

d. Search the Internet using the IP address or computer names. The results of these searches might reveal peer-to-peer (P2P) activities (e.g., file sharing), records in web server log files, or glimpses of the individual's web activities (e.g., Wikipedia edits). These bits of individuals' online history may reveal their political inclinations, state of health, sexuality, religious sentiments and a range of other personal characteristics, preoccupations and individual interests;

e. Seek information on any e-mail addresses used from a particular IP address which, in turn, could be the subject of further requests for subscriber information;

f. Reveal organizational affiliations or organization to which the address is assigned, including a name, phone number, and physical address.

48. Intercepted IP addresses and other data are paired with data captured by PR/TT processes to further expand upon a website user's fingerprint, and to share that data with third party marketers, other websites, and data aggregators, who seek to monetize it.

49. Indeed, multiple data points are used to create a profile of each visitor, which gives websites (and anyone willing to pay for PII), a detailed overview of the visitors' search history, browsing activity, and frequently visited pages.

50. For example, a PR/TT process known as a third-party script (often called a third party "cookie" to sound innocuous) is implanted on an unsuspecting website visitor's browser, and will thereafter feed data about that visitor and their browsing patterns to third parties, for a protracted period of time (often years), without any notice to the individual whose PII is being trafficked and shared across platforms and networks.

51. A person may visit a website that sells watches and then move on to a different website or to social media. But now, ads for watches are everywhere. They're on news websites, in the social media feed, and everywhere else the targeted person goes online. This is because the watch website intercepted and stored identifying electronic impulses (such as an IP address) and installed a PR/TT process on the user's web browser (likely in the form of a third-party script/cookie) and as the user visits other websites and platforms, that process surveilles all online activity, thus showing ads for watches across digital platforms.

52. In this way, these PR/TT processes act as spyware, decoding the user's identity through their IP address, implanting surveillance processes on their web browser, and following the visitor around the internet to serve ads or gather additional information – or sometimes, to simply observe and surveil browsing habits.

53. Using PR/TT processes that are installed by websites like Defendant's, to surveil internet search history, browsing patterns, and data inputs, creates a powerful and financially valuable digital fingerprint and has given rise to a multi-billion-dollar digital surveillance industry targeting all Americans, known as the "identity resolution" industry.

54. "Identity resolution" is the process of accurately and consistently identifying individual customers across various touchpoints and channels. *What is identity resolution?*, SALESFORCE, https://www.salesforce.com/marketing/data/customer-identity-resolution/#what-is (accessed July 24, 2025).

55. The data of Floridians (and all internet users) is now intercepted, stolen, and harvested across the internet, centralized, mined, and de-anonymized for commercial purposes, all with the help of PR/TT processes, often without consent. The information used by individual companies and marketers, and by the identity resolution industry, to accomplish these tasks, is the very electronic addressing, routing, and signaling data, which Florida law requires a court order or consent to collect. This includes third party scripts (i.e. third-party cookies) that are installed on web browsers to surveil activity across the internet, and device IDs and other identifying information gleaned from an IP address.

56. Of course, none of this is illegal with a court order or with consent. Websites that intend to intercept electronic communications and/or to use PR/TT processes to capture electronic routing, addressing, and signaling information from visitors, including installation of third-party scripts on visitors' web browsers, need only disclose their intent to do so and obtain user agreement. Hence the ubiquity of cookie consent banners on websites across the internet.

57. Whether a website operator chooses a simple or detailed consent form, some type of consent must be obtained before installing and running PR/TT processes in the form of third-party scripts (cookies) on visitors' web browsers.

58. There are dozens (if not hundreds) of companies offering consent banners for use by website operators, some of which are paid, and some completely free. And yet, Defendant has failed and refused to deploy even a free consent banner, which would advise its visitors that it is capturing their electronic data and installing scripts on the web browsers. But why?

59. This is because – while it is easy and free to follow these common-sense electronic privacy requirements (which are not unique to Florida) – it is more profitable to ignore privacy laws.

60. When consent is sought, some number of website visitors will withhold that consent, thus depriving Defendant, its marketing partners, and the ever-expanding identity resolution industry, of key data points needed to create an exploitable fingerprint for every internet user, thus cutting into profits. For some, the information gleaned from these PR/TT processes is simply too valuable to get consent before gathering it – even if consent is required by law.

61. Indeed, the ability to use PR/TT processes to link a digital profile to a specific person by the process of fingerprinting is of significant monetary value to commercial website operators, to online marketers, and to the identity resolution industry.

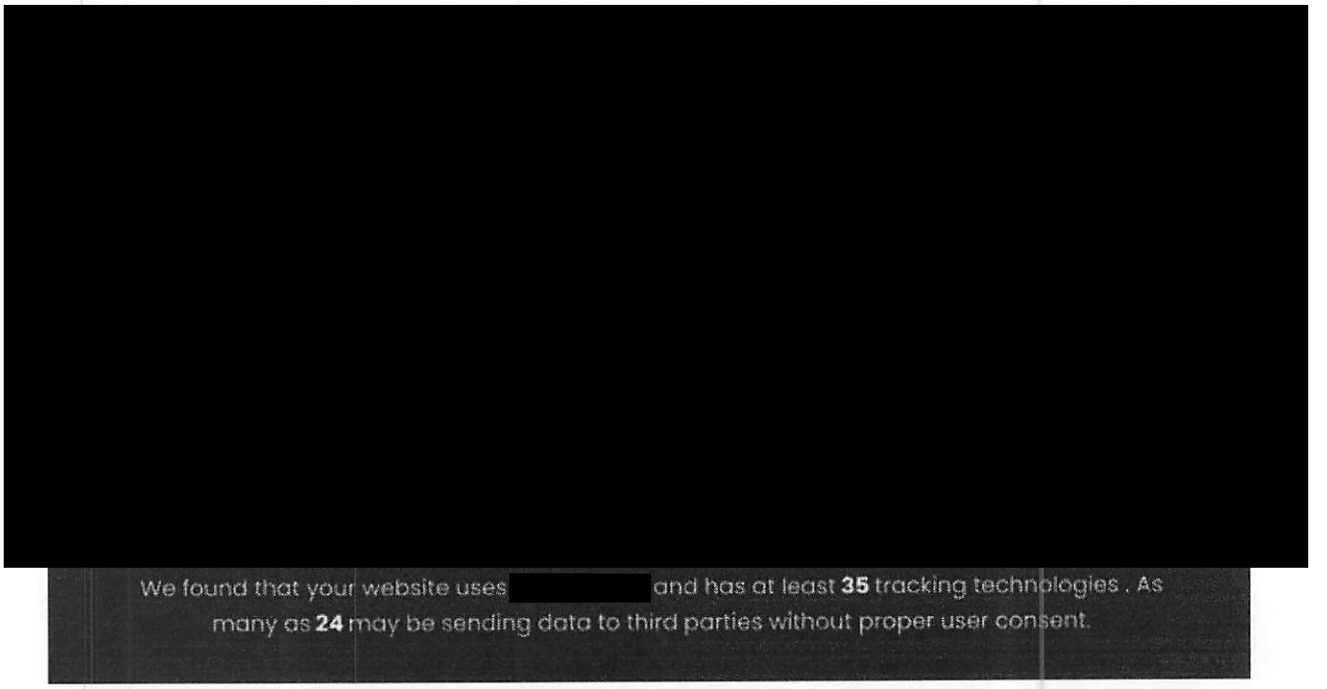
62. In addition to profit generated by the identity resolution industry, individual ecommerce sites like Defendant profit by capturing visitor data and installing PR/TT processes from third party marketers on their visitor's web browsers. These mechanisms allow websites to optimize the way visitors interact with their website, trace and target their visitors across other websites and platforms, build a profile of visitor interests and preferences, and undertake enumerable other for-profit activities related to surveilling visitors' web browsers. The full nature and extent of Defendant's profit from its deployment of PR/TT processes on its website will be determined during discovery in this case.

63. Violating consumer privacy expectations, data collection ethics, and Florida law, Defendant deploys PR/TT processes, including third party scripts/cookies, which install themselves on each visitor's web browser, and act as spyware for Defendant and third-party companies – and Defendant does this without any court order and without obtaining any consent. This spyware then intercepts, surveils, and gathers information about each website user as they use the internet, sometimes for years.

64. Plaintiff – and every Website user – has a reasonable expectation that their own web browsers are private, and that Defendant has not invaded that privacy by secretly installing software

on the browser, to ascertain, intercept, and gather otherwise private and personal information, and to transmit that information to others.

65. Nevertheless, this is exactly what Defendant does. In addition to Plaintiff's own experience visiting the Website and not receiving notice and providing no consent regarding installation of PR/TT processes on Plaintiff's web browser, an independent third-party analysis of



66. A pre-suit expert analysis of the Website confirmed that despite the absence of any consent request, multiple PR/TT devices running on the Website, installing on visitor web browsers, and transmitting private user data and information to third parties, including but not limited to the following:

- **Bazaarvoice**
  Analytics (Tools used to collect, process, and analyze user behavior and traffic on the site)
- **Elevar**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Facebook Connect**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Facebook Custom Audience**

Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)

- **Google Ads**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Google AdWords**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Google Analytics 4**
  Analytics (Tools used to collect, process, and analyze user behavior and traffic on the site)
- **Google DoubleClick**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Google DoubleClick Digital Marketing (DDM)**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Google Dynamic Remarketing**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Google Floodlight**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Google Global Site Destination Tag**
  Analytics (Tools used to collect, process, and analyze user behavior and traffic on the site)
- **Google Global Site Tag**
  Analytics (Tools used to collect, process, and analyze user behavior and traffic on the site)
- **Gorgias**
  Customer Experience Management
- **Impact**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Instafeed**
  Advertising (Platforms or scripts used to serve ads, track conversions, retarget users, or build advertising audiences)
- **Klaviyo**
  Email & SMS Marketing
- **Reddit**
  Analytics (Tools used to collect, process, and analyze user behavior and traffic on the site)
- **Shopify Analytics**
  Analytics (Tools used to collect, process, and analyze user behavior and traffic on the site)

67. Defendant's actions in this case violate the FCSA, entitling Plaintiff to all remedies permitted by law, including compensatory and punitive damages, attorney's fees and costs, and litigation costs.

68. Plaintiff has retained counsel to represent them in this matter and is entitled to recover all reasonable attorney's fees and costs.

COUNT I
VIOLATION OF THE FSCA BY UNAUTHORIZED USE OF PR/TT PROCESSES
Fla. Stat. § 934.31

68. Plaintiff re-avers Paragraphs 1-68 above, as though fully set forth herein.

69. Prior to filing this lawsuit, Plaintiff visited the Website from within Florida.

70. At that time, Plaintiff was not given any notice that Defendant's Website was installing anything on Plaintiff's web browser, was never asked for consent to have the Website install anything on Plaintiff's web browser, and certainly never consented to installation by Defendant of anything onto Plaintiff's computer.

71. Nevertheless, without a court order and without consent, Defendant used the Website to install PR/TT processes, as set forth in detail above, onto Plaintiff's web browser, to gather, intercept, and surveil Plaintiff's internet browsing activities.

72. The scripts installed on Plaintiff's web browser captured electronic addressing, routing, and signaling information from Plaintiff's computer, including the IP address, and monitored Plaintiff's movement around the Internet; the processes installed by Defendant also transmitted Plaintiff's data to multiple third parties, to whom Plaintiff did not agree to provide such information.

73. To comply with Florida law (and other similar privacy laws), all Defendant had to do, was to place a consent banner on the Website, and obtain consent – prior to installing such software on its visitor's web browsers.

74. Defendant thus installed a PR/TT process on Plaintiff's web browser without a court order or consent in violation of Fla. Stat. § 934.31(1) ("[N]o person may install or use a pen register or a trap and trace device without first obtaining a court order").

75. Defendant's actions violate the FCSA and violate the electronic privacy rights guaranteed to Florida's citizens and residents, including Plaintiff, by law.

76. Plaintiff is entitled to recover, and here seeks, all rights and remedies to which Plaintiff is entitled under the facts and circumstances presented in this case.

COUNT II
VIOLATION OF THE FSCA BY UNAUTHORIZED INTERCEPTION OF ELECTRONIC COMMUNICATIONS
Fla. Stat. § 934.03, et. seq.

77. Plaintiff re-avers Paragraphs 1-68 above, as though fully set forth herein.

78. The FSCA prohibits any person or entity from intercepting, endeavoring to intercept, or procuring any third party to intercept or endeavor to intercept any electronic communication. Fla. Stat. § 934.03(1)(a).

79. It is unlawful to intercept any electronic communication under Florida law "unless all of the parties to the communication have given ***prior consent*** to such interception." Fla. Stat. § 934.03(2)(d) (emphasis added).

80. The FSCA defines "intercept" of an electronic communication as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 934.02(3).

81. The FSCA defines electronic communication 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.* § 934.02(12).

82. The real time interception of electronic data in this case starts as soon as the visitor loads the Website into the web browser. The third-party PR/TT scripts that Defendant loads without consent (as set forth above), maintain massive databases including data and profiles on American consumers, including PII of consumers.

83. Defendant begins to intercept and then transmit its visitor's PII as soon as the Website loads. The PR/TT wiretaps used by the Website to intercept this information is only visible by examining the Website's code, unless a website discloses their presence (which Defendant does not).

84. Immediately upon visiting the Website, data transmitted and communicated electronically from a visitor's web browser, such as its IP address and other related PII, is intercepted by the PR/TT devices, which are then illegally installed on the Website by Defendant, and then begin to transmit intercepted data to a third party, with whom Plaintiff has no relationship (as set forth above, the unlawful PR/TT processes installed by the Website continue intercepting and transmitting personal and private data long after a visitor leaves the Website, sometime for many years afterwards).

85. The PR/TT processes that the Website installs on unsuspecting visitors are also deployed over hundreds or thousands of other websites and are therefore able to correlate intercepted PII data. For example, after visiting the Website and having its PII unlawfully intercepted and transmitted, a Website user can never again visit any website on the internet without its identity de-anonymized. Worse, if that user entered any personal information *into any other website* on which the same PR/TT processes are deployed, then its full identity and very personal data is known to the Website (and/or to the PR/TT process owner) the moment the Website intercepts and transmits its IP address (which is done instantly).

86. Defendant is thus committing a serious offense against online privacy, and a "double violation" of the FSCA by using unlawful PR/TT processes to intercept and transmit personal information, without consent.

COUNT III
INVASION OF PRIVACY

87. Plaintiff re-avers Paragraphs 1-68 above, as though fully set forth herein.

88. Defendant intentionally intruded upon Plaintiff's private electronic system (computer) by surreptitiously and secretly installing third party scripts and other PR/TT processes on Plaintiff's web browser, in order to gather and then disseminate Plaintiff's personally identifying information stored on Plaintiff's personal computer's web browser.

89. Plaintiff had a reasonable expectation that information stored on Plaintiff's personal computer was private, and that third parties were not installing software on their computer without notice, to gather and transmit PII.

90. Defendant did not request or obtain Plaintiff's consent before intruding upon the subject electronic systems and provided Plaintiff with no notice that it had installed processes upon Plaintiff's web browser to gather and disseminate personally identifying information.

91. A reasonable person would be offended upon learning that Defendant had installed a software process on their computer without consent or notice, to gather (for themselves) and disseminate (to third parties) personally identifying information.

92. As a result of Defendant's unlawful actions, Plaintiff has been irreparably harmed including, without limitation, by being deprived of the right to exercise meaningful control over the use and dissemination of Plaintiff's personally identifying information, e.g., IP address, name, email address, address, zip code, consumer preferences, etc.

93. This harm also equates to actual, concrete, and quantifiable damages in the form of the monetary value Defendant derives from Plaintiff's personal information without properly compensating Plaintiff for the same.

94. Depending on the specific industry, the nature/extent of the personal information disclosed, and the manner in which it is used and shared, Plaintiff's actual damages may be as high as hundreds or even thousands of dollars.

95. Plaintiff requests disgorgement of all profits generated by Defendant's invasion of privacy i.e. its installation of PR/TT on visitor websites.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter Judgment as follows:

a) Awarding Plaintiff the sum of $100.00 per day for every day from the date on which Defendant installed PR/TT processes, in the form of third-party scripts/cookies or otherwise, through the date of the final judgment in this case, or $1000.00, whichever is greater;

b) Awarding Plaintiff such other compensatory or punitive damages as may be deemed appropriate pursuant to the FSCA;

c) Award Plaintiff such additional compensatory damages as may be deemed appropriate to compensate Plaintiff for invasion of privacy;

d) Awarding Plaintiff all reasonable attorney's fees and costs and litigation costs incurred in this case; and

e) Awarding all such other relief as may be deemed just and equitable under the circumstances presented herein.

JURY DEMAND AND RESERVATION OF PUNITIVE DAMAGES

Plaintiff respectfully requests a trial by jury on all issues so triable. Further, Plaintiff reserves the right to amend the Complaint and add a claim for punitive damages upon serving discovery and subsequent proffer.

Dated: April 14, 2026

Respectfully submitted,

By: */s/ Abdul-Sumi Dalal*
Abdul-Sumi Dalal, Esq.
Veronika Balbuzanova, Esq., CIPP/US
AD@JohnsonDalal.com
VB@JohnsonDalal.com
JOHNSON | DALAL
111 N. Pine Island Road
Suite 105
Plantation, FL 33324
Attorneys for Plaintiff