Robert Tauler (SBN 241964)
rtauler@taulersmith.com
TAULER SMITH LLP
626 Wilshire Boulevard, Suite 1100
Los Angeles, California 90017
Tel: (213) 927-9270

Attorney for Plaintiff
Sara Cammorata

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

SARA CAMMORATA, an individual

Plaintiff,

vs.

P39 TECH LLC, a New York Limited Liability Company,

Defendant.

CASE NO.: 26STCV09460

PLAINTIFF'S CASE SUMMARY AND COMPUTATIONS IN SUPPORT OF APPLICATION FOR DEFAULT JUDGMENT BY COURT

Complaint Filed: March 24, 2026

Default Entered: June 22, 2026

I. CASE SUMMARY.

A. INTRODUCTION.

Plaintiff Sara Cammorata ("Plaintiff") alleges P39 Tech LLC ("P39" or "Defendant") violated the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Penal Code section 502 et seq., and committed common law fraud.

Defendant operates the website at www.peer39.com (the "Website"), where it presents visitors with a consent banner representing that users may opt out of online tracking. Despite those representations, Defendant deploys tracking technologies and data-mining software provided by registered data brokers (the "Data Broker Software" or "DBS"), regardless of whether a visitor affirmatively declines tracking. The DBS is comprised of advanced technology that functions by accessing information from the Website visitors' computers, collecting information about the device and its user, and placing tracking files on visitors' computers. These technologies enable Defendant and third-party data brokers to monitor Website visitors' browsing activity and behavior for commercial surveillance and profiling purposes.

Plaintiff expressly opted out of tracking and did not consent to Defendant accessing Plaintiff's computer, collecting information from it, or installing tracking technologies. Nonetheless, Defendant caused the DBS to be deployed on her device, despite representing that users who declined tracking would not be monitored. Defendant's representations were false, and due to the nature of this misrepresentation, Plaintiff could not consent as a matter of law.

Based on the foregoing and as discussed in further detail below, the Court should grant Plaintiff's request compensation for Defendant's misconduct, to enjoin Defendant's fraudulent practices, disgorgement of data unlawfully obtained, reasonable costs, and such other relief as the Court deems just and proper.

B. PROCEDURAL HISTORY.

This case was originally filed on March 24, 2026.

Defendant was served with the Complaint on March 30, 2026, by personal service on Alyssa Daniels, person authorized to accept for A Registered Agent, Inc. (Defendant's Registered Agent), at 8 The Green, Dover, DE 19901 (the "Dover address"). A true and correct copy of the Proof of Service of Summons was filed on June 3, 2026. (Tauler Dec. ¶ 3; Ex. A.)

Plaintiff filed a Request for Entry of Default on June 22, 2026. The clerk entered default on that same day. (Tauler Dec. ¶ 4; Ex. B.) The Request for Entry of Default was also sent by first class mail to Defendant on June 22, 2026, at the Dover address. (Tauler Dec. ¶ 4; Ex. B.)

C. FACTUAL ALLEGATIONS.

1. <u>Plaintiff's Action</u>.

a. <u>Violation of CDAFA (Cal. Penal Code § 502).</u>

The California Comprehensive Computer Data Access and Fraud Act ("CDAFA") Cal. Penal Code § 502 (a)-(e) makes it unlawful for parties to obtain data from a computer user outside of the scope of their authorization.

Under CDAFA, it is unlawful to knowingly take, copy, or make use of any data from a computer. Cal. Penal Code § 502(c)(2). Similarly, adding "data, computer software, or computer programs" to a device without consent violates CDAFA. Cal. Penal Code § 502(c)(4). Third parties are liable if they "[k]knowingly and without permission provide[] or assist[] in providing a means of accessing a computer, computer system, or computer network in violation of this section." Cal. Penal Code § 502(c)(6). Section 502(e) provides a private right of action for "compensatory damages and injunctive relief or other equitable relief[,]" and a court may award reasonable attorney's fees and punitive damages on a case-by-case basis. *See* Cal. Penal Code § 502(e).

b. <u>Fraud.</u>

California Civil Code § 3294(a) provides "[i]n an action for the breach of an obligation not arising from contract, where it is proven by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice, the plaintiff, in addition to the actual damages, may recover damages for the sake of example and by way of punishing the defendant."

As used in this section, the following definition applies: "'Fraud' means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury." CA Civ. Code § 3294(c).

2. Data Broker Software ("DBS").

The DBS is a collection of tracking and data-mining technologies that allows third-party brokers to identify, profile, and monitor visitors to Defendant's Website. Defendant embedded the DBS on its Website and deployed it notwithstanding visitors' election to opt out of tracking through Defendant's consent banner. (Compl. ¶¶ 1, 12, 14-15, 22, 24-26, 31; Ex. C, Weiss Decl. ¶¶ 9-16, 22-28.)

As part of its operation, the DBS accesses information from a Website visitor's computer, including the computer's make and model, browser information, routing information, display settings, installed fonts, and other technical characteristics. (Compl. ¶ 14; Ex. C, Weiss Decl. ¶¶ 15, 22, 26 & Ex. A.) The DBS copies this information and transfers it to data broker servers, where it is matched against existing profiles contained in pre-existing data broker databases. (Compl. ¶¶ 14, 22; Ex. C, Weiss Decl. ¶¶ 12, 14-15, 22, 24, 26.) This matching process allows the data brokers to learn the identity of otherwise anonymous Website visitors, like Plaintiff. (Compl. ¶¶ 14, 22; Ex. C, Weiss Decl. ¶¶ 22-24, 26.)

The DBS monitors Website visitors by installing a small tracking data file on the visitor's device. (Compl. ¶¶ 1, 15, 24; Ex. C, Weiss Decl. ¶¶ 11, 14, 28 & definition of "Cookie.") Through this tracking mechanism, the DBS records and analyzes the user's browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and geolocation data. (Compl. ¶ 15; Ex. C, Weiss Decl. ¶¶ 13-16, 22, 26 & Ex. A.) The tracking data file also allows data brokers to observe a visitor's subsequent behavior and communications and to track the visitor's activity across other websites. (Compl. ¶¶ 15, 24, 31; Ex. C, Weiss Decl. ¶¶ 15, 23, 28 & definitions of "Cookie" and "Identifiers.")

The DBS is a computer contaminant because it self-propagates onto users' devices to record and transmit the data that would not otherwise be transmitted or recorded in the normal operation of a computer system. (Compl. ¶ 16.) These technologies supplant users' choices regarding how their devices and resources are used, effectively transforming those devices into tools for commercial surveillance. (*Id.*)

It bears repeating that Defendant's installation and use of the DBS are performed for the purpose of obtaining information from Website visitors, matching that information to existing data broker records to identify those visitors, and facilitating ongoing surveillance of their internet activity; all without their knowledge, against the user's consent, and enacted through false representations to the user regarding their ability to opt-out of tracking. (Compl., *generally;* Ex. C, Weiss Decl., *generally.*)

3. **Plaintiff's Injury**.

Plaintiff visited Defendant's website, www.peer39.com, on December 30, 2025. (Cammorata Dec. ¶ 2.) During the visit, Defendant operated the DBS on the Website, which it continues to do to this day. Plaintiff rejected the use of tracking technologies on the Website, but Defendant nevertheless caused DBS to access Plaintiff's device, allowing the Data Brokers to install a data mining script on Plaintiff's computer, and allowing Data Brokers to install data files to be placed on Plaintiff's browser for enhanced long-term surveillance of Plaintiff's internet behavior. (*See* Cammorata Dec. ¶¶ 2, 4.) The DBS is a computer contaminant which has infected Plaintiff's computer, usurping the normal operation and effectively turning her computer into a surveillance device. (*See* Cammorata Dec. ¶¶ 2, 4.) Plaintiff would like to visit the Website again in the future, but not if Defendant continues collecting Plaintiff's data through the DBS, especially without her permission. (Cammorata Dec. ¶ 3.)

Plaintiff has been damaged because the fraudulent consent banner on Defendant's website "revoked Plaintiff's control over [their personal] information and diminished its value." *Pemberton v. Restaurant Brands International, Inc.,* 3:25-cv-03647, (N.D. Cal.) Further, the above process also violates CDAFA, as it serves to unjustly enrich data brokers and their partners, who have obtained something for nothing, allowing them to "unjustly profit from Plaintiff's personal information and online activity." *Smith v. Rack Room Shoes, Inc.,* No. 24-cv-06709-RFL, 2025 U.S. Dist. LEXIS 149750, at *6-8 (N.D. Cal. Aug. 4, 2025).

II. <u>RELIEF SOUGHT.</u>

A. CIVIL REMEDIES UNDER CDAFA.

The California Comprehensive Computer Data Access and Fraud Act ("CDAFA") provides a private right of action to "[a]ny owner or lessee of the computer, computer system, computer network, computer program, or data" who suffers damage or loss by reason of a violation of Penal Code § 502. Cal. Pen. Code § 502(e)(1). The "owner or lessee" of the computer who suffers damage or loss may be the action to recover "compensatory damages and injunctive relief or other equitable relief." *Id.*

The statute authorizes compensatory damages, injunctive relief, and other equitable relief. *Id.* Additionally, CDAFA authorizes an award of attorney's fees and punitive damages on a case-by-case basis. Cal. Pen. Code §§ 502(e)(2), (4).

Here, Plaintiff alleges Defendant violated multiple provisions of CDAFA by causing DBS to access Plaintiff's computer without authorization, copy information from Plaintiff's device, make use of that information by matching it against pre-existing data broker profiles, and install tracking files on Plaintiff's device for ongoing surveillance. (Compl. ¶¶ 12, 14-16, 21-28, 31.) So, Plaintiff may seek compensatory damages, injunctive relief, disgorgement, reasonable attorney's fees, punitive damages, and other equitable relief authorized by Penal Code § 502(e).

1. <u>Compensatory Damages Under CDAFA.</u>

Penal Code § 502(e)(1) expressly authorizes an award of compensatory damages[1] to persons injured by conduct prohibited by § 502. Cal. Pen. Code § 502(e)(1).

Here, Plaintiff alleges the Defendant caused DBS to access Plaintiff's device, despite Plaintiff's express election to opt out of tracking. (Compl., ¶ 12.) Plaintiff further alleges that Defendant copied and made use of information from Plaintiff's computer, including browser information, routing information, device characteristics, and other technical information, and caused tracking files to be installed on Plaintiff's device for ongoing surveillance. (*Id.* at ¶¶ 14-16, 21-24, 31.) Plaintiff therefore seeks compensatory damages pursuant to Penal Code § 502(e)(1) to account for some of the unjust enrichment obtained as a result of Defendant's conduct.

2. <u>Injunctive Relief Under CDAFA.</u>

Penal Code § 502(e)(1) authorizes injunctive relief and other equitable remedies. Cal. Pen. Code § 502(e)(1).

Here, Plaintiff alleges Defendant continues to operate, to this day, a website that represents users may opt out of tracking while it nevertheless permits Data Broker Software to access users' devices, obtain information from those devices, and install tracking files for long-term surveillance, even if the user opts

---

[1] Compensatory damages shall include "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access[,]" and "the court may award reasonable attorney's fees." Cal. Penal Code § 502 (e)(1), (2).

out. (Compl. ¶¶ 1-2, 12-16, 25-26, 30-33.) Plaintiff therefore seeks a permanent injunction prohibiting Defendant from continuing the deceptive practice of representing that users may opt out of tracking when in reality, Defendant continues to deploy tracking technologies despite those users' explicit election to reject tracking.

3. Disgorgement and Equitable Relief Under CDAFA.

CDAFA authorizes courts to grant equitable relief to remedy violations of the statute. Cal. Pen. Code § 502(e)(1).

Here, Plaintiff alleges Defendant obtained and made use of information copied from Plaintiff's computer and facilitated the transmission of that information to third-party data brokers for identification, profiling, and surveillance purposes. (Compl., ¶¶ 14-15, 22, 31.) Plaintiff therefore seeks disgorgement of Plaintiff's data which Defendant derived from Defendants' unlawful use of the DBS and damages.

B. PLAINTIFF IS ENTITLED TO A PERMANENT INJUNCTION.

1. Legal Standard for Permanent Injunctions.

> Code Civ. Proc. § 526(a) provides for a permanent injunction in the following instances:
> (1) When it appears by the complaint that the plaintiff is entitled to the relief demanded, and the relief, or any part thereof, consists in restraining the commission or continuance of the act complained of, either for a limited period or perpetually.
> (2) When it appears by the complaint or affidavits that the commission or continuance of some act during the litigation would produce great or irreparable injury, to a party to the action.
> (3) When it appears, during the litigation, that a party to the action is doing, or threatens, or is about to do, or is procuring or suffering to be done, some act in violation of the rights of another party to the action respecting the subject of the action, and tending to render the judgment ineffectual.
> (4) When pecuniary compensation would not afford adequate relief.
> (5) Where it would be extremely difficult to ascertain the amount of compensation which would afford adequate relief.
> (6) Where the restraint is necessary to prevent a multiplicity of judicial proceedings.
> (7) Where the obligation arises from a trust.

See Cal. Code Civ. Proc. § 526(a).

A permanent injunction is an equitable remedy for certain torts or wrongful acts of a defendant where a damage remedy is inadequate. *Art Movers, Inc. v. Ni West, Inc.* (1992) 3 Cal.App.4th 640, 646. A permanent injunction is a determination on the merits that a plaintiff has prevailed on a cause of action and that equitable relief is appropriate. *Horsford v. Board of Trustees of California State University* (2005) 132 Cal.App.4th 359, 389. A party seeking permanent injunction must "present evidence proving the elements" of its claim. *Applied Med. Distribution Corp. v. Jarrells* (2024) 100 Cal.App.5th 556. 581.

Here, Plaintiff seeks a final permanent injunction as it is clear by the Complaint that Plaintiff is entitled to the relief demanded, and pecuniary compensation would not afford adequate relief. Cal. Code Civ. Proc. §§ 526(a)(1), (a)(4).

2. **Plaintiff Prevails on the Merits of Her Claim Against Defendant for Violation of CDAFA.**

a. The Defendant's Use of the DBS Violates CDAFA.

The allegations here are similar and warrant a determination on the merits. The DBS, as it appears on the Website, violates CDAFA under Penal Code § 502(e)[2] after analyzing the data collection process in four steps. The Complaint alleges Defendant violated CDAFA by causing Data Broker Software ("DBS") to access Plaintiff's computer after Plaintiff expressly rejected tracking through Defendant's consent banner. (Compl., ¶¶ 12, 25-26, 28.)

First, the DBS "copies" information contained on Plaintiff's computer, including browser information, computer make and model routing information, and other technical characteristics in violation of Cal. Penal Code § 502(c)(2). (Compl., ¶¶ 21; *See* Cal. Pen. Code § 502(c)(2).)

Second, in further violation of § 502(c)(2), the DBS also "makes use of" information contained on Plaintiff's computer by matching the above information with existing profiles in pre-existing data broker databases. The Data Brokers do this to learn the identity of the website visitor. (Compl., ¶22; *See* Cal. Pen. Code § 502(c)(2).)

Third, in violation of § 502(c)(4), the DBS adds data in the form of a small data file to Plaintiff's computer, so that it can track Plaintiff's movements on the website, and on other websites Plaintiff might visit. (Compl. at ¶ 24; *See* Cal. Pen. Code § 502(c)(4).)

Fourth, in violation of § 502(c)(6), the Defendant's collaboration with the Data Brokers to subvert the purposes and functionality of their consent banner, the unauthorized copying and use of Plaintiff's

[2] The California Comprehensive Computer Data Access and Fraud Act ("CDAFA") provides a private right of action to "[a]ny owner or lessee of the computer, computer system, computer network, computer program, or data" who suffers damage or loss by reason of a violation of Penal Code § 502. Cal. Pen. Code § 502(e)(1). The statute authorizes compensatory damages, injunctive relief, and other equitable relief. *Id.* Additionally, CDAFA authorizes an award of attorney's fees and punitive damages on a case-by-case basis. Cal. Pen. Code §§ 502(e)(2), (4).

information, has also overcome a technical barrier (the consent banner itself) to obtain unauthorized access to Plaintiff's computer. (Compl. at ¶¶ 25- 26; *See* Cal. Pen. Code § 502(c)(6).)

In sum, the Defendant's use of the DBS with the explicit intent of accessing, copying, and making use of data from Plaintiff's computer for tracking without consent violates CDAFA. (Compl., at ¶ 28.)

b. The Defendant Has Committed Fraud.

The allegations here warrant a determination on the merits. Defendant's conduct, as alleged in the Complaint, constitutes fraud after analyzing the fraudulent scheme in four steps.[3]

First, Defendant made a material representation by informing Plaintiff that Website visitors could opt out of tracking through the Website's consent banner, which Plaintiff did choose to not be tracked. (Compl. ¶¶ 1-2, 12-13, 30.) Defendant represented that users could browse the Website without being tracked, followed, or targeted by third-party data brokers. (*Id*. ¶ 2.)

Second, despite those representations, Defendant nevertheless caused the DBS to access Plaintiff's device, obtain information from Plaintiff's computer, match that information against existing data broker records, and install tracking files for enhanced long-term surveillance of Plaintiff's internet activity. (*Id.* at ¶¶ 12, 14-15, 31.) Defendant's representations were therefore false regarding the user's ability to opt out. (*Id.* at ¶¶ 2, 30-31.)

Third, Defendant knew, or should have known, that its representations were false because Defendant knew that the Website's programming allowed data files to be placed on users devices and information to be transmitted to data brokers, even after users attempted to opt out of tracking. Defendant has complete control over its website. (*Id.* at ¶¶ 32-33.)

Fourth, Defendant intended Plaintiff to rely on these representations and omissions, and plaintiff in fact relied upon them. (*Id.* at ¶¶ 34-35, 39-40.) Plaintiff would not have used the Website had Defendant disclosed that DBS would continue to access Plaintiff's device and transmit information to data brokers, despite Plaintiff's rejection of tracking. (*Id.* at ¶ 38.) So, Plaintiff suffered damages, including the loss of control over personal information and communications and the diminution in value of that information. (*Id.* at ¶¶ 36-41.)

[3] California Civil Code § 3294(c)(3) defines fraud as "an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury." Cal. Civ. Code § 3294(c)(3).

So, by representing that users could opt out of tracking while simultaneously permitting DBS to continue accessing users' devices and collecting information regardless of those users' choices, Defendant engaged in intentional misrepresentation and deceit within the meaning of Civil Code § 3294(c)(3); Thus, the Court should find that Plaintiff likewise prevails on the merits of her fraud claim.

3. Pecuniary Compensation Will Not Afford Plaintiff Adequate Relief as Defendant's Wrongful Acts Threaten Irreparable Injury.

In seeking a permanent injunction, a plaintiff must show that defendant's wrongful acts threaten to cause irreparable injury, meaning the injury cannot be adequately compensated in damages. *DVD Copy Control Assn., Inc. v. Kaleidescape, Inc.* (2009) 176 Cal.App.4th 697, 722; *Syngenta Crop Protection, Inc. v. Helliker* (2006) 138 Cal.App.4th 1135, 1166.

Where a court determines a plaintiff will succeed at "proving a statutory violation," like Penal Code § 502(e), the Court is "justified in presuming that public harm will result if an injunction is not issued." *IT Corp. v. County of Imperial* (1983) 35 Cal.3d 63, 70. The California Supreme Court clarifies that "[w]here a legislative body has enacted a statutory provision proscribing a certain activity, it has already determined that such activity is contrary to the public interest." *Id*. The California Supreme Court further adds that "where the legislative body has specifically authorized injunctive relief against the violation of such a law," like Penal Code § 502(e) for a violation of CDAFA, "[the legislative] has already determined (1) that significant public harm will result from the proscribed activity, and (2) that injunctive relief may be the most appropriate way to protect against that harm." *Id*. Plaintiff is a part of this public interest and is just one individual of the public who is subsequently aware of Defendant's wrongdoings and inflictions of harm.

Here, the Legislature has enacted CDAFA to prohibit unauthorized access to computers, computer systems, and computer data and to 'expend the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. Cal. Pen. Code § 502(a). The Legislature further declared that CDAFA applies to various forms of unauthorized access to computers, computer systems, and computer data and serves to protect "the integrity of all types and forms of lawfully created computers, computer systems, and computer data," recognizing that such protections are vital to safeguarding individual privacy. *Id.*

Thus, given the Legislature's intent and pre-determination of harm to individuals affected by such violations, it is appropriate for the Court to determine that (1) Defendant's activity is contrary to the public interest; (2) significant harm will be sustained by Plaintiff (a member of the public) from the prohibited activity; and (3) injunctive relief against Defendant is the "most appropriate way to protect against that harm" to Plaintiff. *IT Corp. v. County of Imperial* (1983) 35 Cal.3d 63, 70.

Several courts have recognized that the invasion of an individual's privacy is significant harm warranting an injunction. *See Meyer v. Portfolio Recovery Assocs., LLC* (9th Cir. 2012) 707 F.3d 1036, 1044-45 (holding violation of "right to privacy" demonstrates "irreparable harm is likely in the absence of injunctive relief."); *see*, *e.g.*, *Clear Lake Riviera Cmty. Assn. v. Cramer* (2010) 182 Cal.App.4th 459, 473 (finding irreparable harm when neighbors suffered "loss of privacy" caused by construction of a nearby new home); *Maxcrest Limited v. U.S.* (N.D. Cal. Nov. 7, 2016) No. 15-MC-80270, 2016 WL 6599463, at *5 (explaining "harm to . . . privacy interests would be irreparable because 'there is nothing a court can do to withdraw all knowledge or information . . . once that information has already been divulged.'").

Indeed, Plaintiff will suffer harm, specifically the continued loss of control over her personal information and communications, if the Court does not order Defendant to cease permitting the Data Broker Software used on Defendant's website to access its website visitors' devices and transmit information to data brokers. This harm is not only ongoing, it is irreparable—once Plaintiff's information is transmitted, assimilated into existing data broker records, and used for ongoing surveillance and profiling, the resulting loss of privacy and control cannot be undone. (Compl. At ¶¶ 14-15, 22, 31, 36-37.)

Plaintiff will continue to suffer irreparable injury if Defendant is permitted to maintain the deceptive consent mechanism that represents users may opt out of tracking while nevertheless allowing DBS to access their devices and collect information from them. (Compl., ¶¶ 1-2, 12-13, 30-33.) Thus, it is crucial for the Court to take action to prevent further harm and order a permanent injunction against Defendant's unlawful conduct and damages.

III. COMPUTATION.

Total Damages Owed	**$1,026.68**
Value of the Data Improperly Collected	$400.00
Initiating Filing fee	$469.91
Filing Fee for Proof of Service and Request for Default	$20.77
Service of Process Costs	$136.00

A. PLAINTIFF'S DAMAGES CALCULATION IS REASONABLE.

1. CDAFA Does Not Require a Definitive Damages Figure.

Plaintiff seeks damages related to the value of data improperly collected, just some of the unjust enrichment obtained as a result of Defendant's conduct. Given the nature of the proceedings, and the absence of discovery, Plaintiff is unable to demonstrate this number definitively. However, this does not preclude a default judgment, as "damage" or "loss" need meet a "specific monetary threshold for loss related to violations of the statute." *Facebook, Inc. v. Power Ventures, Inc.,* 2010 U.S. Dist. LEXIS 93517, at *14 (N.D. Cal. July 20, 2010); *see Rodriguez v. Google, LLC,* 772 F. Supp. 3d 1093, 1110 (N.D. Cal. 2025) (noting that "the statute sets no minimum threshold for damage or loss, even small harms due to depletion of battery and bandwidth satisfy CDAFA's requirements); *see Lineberry v. Addshopper, Inc.,* 2025 U.S. Dist. LEXIS 29903, at *5 (N.D. Cal. Feb. 19, 2025) (holding that nothing in CDAFA's text limits cognizable damage or loss to only "a computer system, network, program, or data contained on that computer.")

2. Plaintiff's Damages Figure is Based in Expert Analysis.

Plaintiff has engaged expert witness Adam Weiss to assess the Website's data-collection practices and the value of the data collected. Mr. Weiss reviewed the Complaint, HAR network captures of www.peer39.com collected during the visit[4] and market-value data. (Ex. C, Weiss Decl. at ¶¶ 17-21.) His testing found that tracking code executed before a consent choice and continued after rejection; during the roughly 25 seconds after rejection, the visitor's identifier was broadcast to 19 additional third-party hosts, and, in a separate session, every page view was transmitted to Facebook, TikTok, LinkedIn, Google,

[4] He clarified the captures document the Website's behavior toward a visitor who declines tracking and are not a record of Plaintiff's December 30, 2025, visit. (Ex. C, Weiss Decl., ¶ 20.)

and The Trade Desk. (*Id.* at ¶¶ 10-16.) Post-rejection transmissions included device- and browser-identifying characteristics, the visitor's IP address, and persistent identifiers sent to advertising, tracking, and identity-resolution services. (*Id.* at ¶¶ 14-16, 26-28.)

To estimate the value of the data collected, Mr. Weiss compared the categories of data shown in the HAR captures to publicly available market-value data, including markets for browsing-derived audience segments, device and browser characteristics, persistent cross-site identifiers, and IP-derived geolocation. (*Id.* at ¶¶ 21-22.) Mr. Weiss explained that while individual data elements may have modest per-person prices, the more valuable asset is the assembled, identity-resolved, persistently trackable consumer profile. (*Id.* at ¶ 23.) Based on that analysis, Mr. Weiss estimated that the personal-data component of a tracked U.S. user's annual value is approximately $100 to $250 or more per year and concluded that the data collected from Website visitors is a commercially valuable asset obtained without payment. (*Id.* at ¶¶ 24-25, 29.)

3. <u>Plaintiff's Damages Calculation is Deliberately Conservative.</u>

Here, Plaintiff's calculation is deliberately conservative, as it relies on the lowest valuation within the expert's stated range: Plaintiff's expert has valued the data as approximately $100-250. (*Id.*) Taking these presumptions as true, and applying the most conservative valuation identified by Plaintiff's expert ($100 per entity) to each of the four entities that improperly collected or received Plaintiff's data (*See* Ex. C, Weiss Rep., P. 12, Weiss's Exhibit A), Plaintiff seeks **$400.00** in damages ($100 x the four entities). This amount represents the aggregate damage resulting from the collection and use of Plaintiff's data by four separate entities.

This calculation is reasonable because it is based on the data transmissions observed in the HAR capture that Plaintiff's expert observed, verified, and categorized. The expert then compared the collected data categories to publicly available market-value data, valuing the tracked U.S. user's data at approximately $100 to $250 or more per year. It is worth reiterating that, given the nature of the proceedings and the absence of discovery, Plaintiff is unable to demonstrate a more precise number definitively. However, Plaintiff uses only the lowest figure in that range ($100) and applies it to only the four identities identified as having received Plaintiff's data, per the HAR file reviewed by the expert. Thus, the $400 calculation is grounded in expert analysis and avoids higher-end speculative valuation.

D. OTHER COSTS AND TOTAL JUDGMENT REQUESTED.

Plaintiff also seeks costs incurred associated with this lawsuit totaling **$626.68,** including: $469.91 for the Initial Filing Fee; $20.77 for the Filing Fee for Proof of Service and Request for Default; and $136.00 for Service of Process costs.

Thus, totaling the damages and costs incurred, Plaintiff asks for judgment in the amount of **$1,026.68.**

DATED: July 23, 2026

TAULER SMITH

By: ______________________________

Robert Tauler, Esq.
Attorney for Plaintiff
Sara Cammorata