1   PACIFIC TRIAL ATTORNEYS
    A Professional Corporation
2   Scott J. Ferrell, Bar No. 202091
    sferrell@pacifictrialattorneys.com
3   4100 Newport Place Drive, Ste. 800
    Newport Beach, CA 92660
4   Tel: (949) 706-6464
    Fax: (949) 706-6469
5
    Attorneys for Plaintiff
6

7

8   UNITED STATES DISTRICT COURT

9   CENTRAL DISTRICT OF CALIFORNIA

10

11 MIGUEL A. LICEA, individually and on   Case No. 5:22-cv-01562
    behalf of all others similarly situated,
12
                    Plaintiff,
13
                    v.
14   **CLASS ACTION COMPLAINT FOR
    GAMESTOP, INC., a Minnesota   VIOLATION OF PENAL CODE § 631**
15 corporation, and DOES 1 through 25,
    inclusive,
16
                    Defendants.
17

18

19

20

21

22

23

24

25

26

27

28

INTRODUCTION

Defendant (1) covertly wiretaps the communications of all visitors who utilize the chat feature at www.gamestop.com; and (2) shares the secret transcripts of those wiretaps with a third party that boasts of its ability to harvest personal data from the transcripts for marketing and other purposes. Defendant neither informs visitors nor obtains their prior, express consent to these intrusions. As a result, Defendant has violated the California Invasion of Privacy Act ("CIPA"), California Penal Code § 631.

JURISDICTION AND VENUE

1.   This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is at least minimal diversity because at least one Plaintiff and Defendant are citizens of different states.

2.   Pursuant to 28 U.S.C. Section 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: Plaintiff is a citizen of California who resides in this District and Defendant conducted a substantial portion of the unlawful activity in this District.

3.   Defendant is subject to personal jurisdiction in California based upon sufficient minimum contacts which exist between Defendant and California. Defendant also does business with California residents.

PARTIES

4.   Plaintiff is a citizen of California residing within the Central District of California.

5.   Defendant is a Minnesota corporation that owns, operates, and/or controls the above-referenced website.

6.   The above-named Defendant, along with its affiliates and agents, are collectively referred to as "Defendants."   The true names and capacities of the Defendants sued herein as DOE DEFENDANTS 1 through 25, inclusive, are currently unknown to Plaintiff, who therefore sues such Defendants by fictitious names. Each of the Defendants designated herein as a DOE is legally responsible for the unlawful acts alleged herein. Plaintiff will seek leave of Court to amend the Complaint to reflect the true names and capacities of the DOE Defendants when such identities become known.

7.   Plaintiff is informed and believes that at all relevant times, every Defendant was acting as an agent and/or employee of each of the other Defendants and was acting within the course and scope of said agency and/or employment with the full knowledge and consent of each of the other Defendants.

8.   Plaintiff is informed and believe that each of the acts and/or omissions complained of herein was made known to, and ratified by, each of the other Defendants.

FACTUAL ALLEGATIONS

9.   Under the California Invasion of Privacy Act, website operators cannot create transcripts of visitors' conversations (or provide such transcripts to third parties) without obtaining prior, express consent from all parties to the conversation. Compliance with CIPA is easy, and the vast majority of companies comply with the law by simply notifying website visitors if their conversations are being recorded.

10.   Unlike most companies, Defendant has chosen not to comply with CIPA. Rather, without warning visitors or obtaining their consent, Defendant has secretly deployed wiretapping software on its Website. Using that software, Defendant covertly monitors, records, and creates secret transcripts of all communication through the chat feature on its website.

11.   Going from bad to worse, Defendant shares the secret transcripts with Zendesk, a third party that publicly boasts about its ability to harvest highly personal data from chat transcripts for sales and marketing purposes.   Rather than merely

1 providing a software service, Defendant allows Zendesk to intercept and use the secret

2 transcripts.

3   12.   Given the nature of Defendant's business, website visitors typically share

4 highly personal and sensitive data with Defendant when using the website chat feature.

5 Consumers would be shocked and appalled to know that Defendant secretly creates

6 transcripts of those conversations and shares them with a third party.

7   13.   Defendant's conduct is both illegal and offensive: indeed, a recent study

8 conducted by the Electronic Privacy Information Center, a respected thought leader

9 regarding digital privacy, found that: (1) nearly 9 in 10 adults are "very concerned"

10 about data privacy, and (2) 75% of adults are unaware of the extent to which companies

11 gather,   store,   and   exploit   their   personal   data.   *See*

12 https://archive.epic.org/privacy/survey/ (last downloaded September 2022).

13   14.   Within the statute of limitations period, Plaintiff visited Defendant's

14 Website and communicated with an employee of Defendant through the website chat

15 feature.   Unbeknownst to website visitors, Defendant creates exact transcripts of all

16 such communications and shares the transcripts with at least one third party using

17 secretly embedded wiretapping technology.

18   **15.   Simplified to common parlance, Defendant: (1) encourages website**

19 **visitors to share personal information through the website chat feature; (2)**

20 **secretly creates a transcript of all such conversations without warning website**

21 **visitors or obtaining their consent; and (3) shares the secret transcripts with a**

22 **third party that boasts of its ability to harvest personal data from the transcripts**

23 **for sales and marketing purposes.**

24   16.   Defendant did not inform Plaintiff, or any of the Class Members, that

25 Defendant was secretly monitoring, recording, and sharing their communications.

26   17.   Defendant did not obtain Plaintiff's or the Class Members' consent to

27 intercepting, monitoring, recording, and sharing the electronic communications with the

28 Website.

18. Plaintiff and Class Members did not know at the time of the communications that Defendant was secretly intercepting, monitoring, recording, and sharing the electronic communications.

CLASS ALLEGATIONS

19. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class") defined as follows:

All persons within California who: (1) visited Defendant's website, and (2) whose electronic communications were recorded, stored, and/or shared by Defendant without prior express consent within the statute of limitations period.

20. <u>NUMEROSITY</u>: Plaintiff does not know the number of Class Members but believes the number to be in the tens of thousands, if not more. The exact identities of Class Members may be ascertained by the records maintained by Defendant.

21. <u>COMMONALITY</u>: Common questions of fact and law exist as to all Class Members, and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class Member, include but are not limited to the following:

a. Whether Defendant caused Plaintiff's and the Class's electronic communications with the Website to be recorded, intercepted and/or monitored;

b. Whether Defendant violated CIPA based thereon;

c. Whether Plaintiff and Class Members are entitled to statutory damages pursuant to Cal. Penal Code § 631(a);

d. Whether Plaintiff and Class Members are entitled to punitive damages pursuant to Cal. Civil Code § 3294; and

e. Whether Plaintiff and Class Members are entitled to injunctive relief.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.