HAYNES AND BOONE, LLP
Kenneth G. Parker / Bar No. 182911
kenneth.parker@haynesboone.com
Thomas B. King / Bar No. 241661
thomas.king@haynesboone.com
600 Anton Boulevard, Suite 700
Costa Mesa, California 92626
Telephone: (949) 202-3000
Facsimile (949) 202-3001

Attorneys for Plaintiff
mSIGNIA, Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MSIGNIA, INC., a California corporation,

Plaintiff,

v.

INAUTH, INC., a Delaware corporation,

Defendant.

Case No. 8:17-cv-1289

COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

Plaintiff mSIGNIA, Inc. ("mSIGNIA", or "Plaintiff") hereby brings this action against Defendant InAuth, Inc. ("InAuth", or "Defendant") and alleges as follows upon actual knowledge with respect to itself and its own acts, and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This is a civil action for patent infringement.

2. mSIGNIA is the legal owner by assignment of U.S. Patent No. 9,559,852 ("the '852 Patent"), which was duly and legally issued by the United States Patent and Trademark Office ("USPTO").

3. mSIGNIA provides computer security products to businesses who need to authenticate users and devices. mSIGNIA's products are based on technology that is described and claimed in the '852 patent. mSIGNIA's patented offerings include its iDNA and 3D Secure products.

4. Defendant InAuth also sells products for authenticating users and devices, including products based on the so-called "InAuth Security Platform." However, as set forth below, the InAuth Security Platform infringes one or more claims of the '852 patent, as do any products, systems, and services related to the InAuth Security Platform and other related InAuth products that use or relate to components of the InAuth Security Platform ("Infringing Products"). InAuth's Infringing Products include but are not limited to InMobile, InBrowser, InRisk, InAuthenticate, InExchange, InReach, InPermID, and other products that use the InAuth Security Platform.

5. mSIGNIA brings this action to remedy InAuth's infringement. mSIGNIA seeks injunctive relief and monetary damages as set forth below.

THE PARTIES

6. mSIGNIA is a corporation organized and existing under the laws of California, with its principal office located at 109 Holiday Court, Suite D7, Franklin, TN 37067. Paul Miller, mSIGNIA's co-founder, Chief Executive Officer

and Secretary, resides and works out of this District, at 10 Wandering Rill, Irvine, CA 92603.

7. Upon information and belief, InAuth is a corporation organized and existing under the laws of the State of Delaware. InAuth claims to have a West Coast Office located at 227 Broadway, Suite 200, Santa Monica, CA 90401. (*See e.g.*, https://www.inauth.com/contact/.) Upon information and belief, InAuth's West Coast Office is focused at least in part on engineering and product development.

JURISDICTION AND VENUE

8. This is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*.

9. This Court has subject matter jurisdiction over the matters asserted pursuant to 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over InAuth. InAuth has infringed the '852 patent in the Central District of California by, among other things, engaging in infringing conduct within and directed at or from this District, including, based on information and belief, by developing its Infringing Products out of an office in this District and by the advertisement, solicitation of customers, marketing, and distribution of services that practice the claims of the '852 Patent. For example, InAuth has purposefully and voluntarily sold one or more of its infringing products or services, as described below, into the stream of commerce with the expectation that these infringing products or services will be used in this District. These infringing products or services have been and continue to be used in this District.

11. Venue is proper in this district and division under 28 U.S.C. § 1400(b) at least because InAuth has a regular and established place of business in the Central District of California. Specifically, InAuth's West Coast Office is located at 227 Broadway, Suite 200, Santa Monica, CA 90401. (*See e.g.*,

https://www.inauth.com/contact/.) Moreover, InAuth has committed acts of infringement in this judicial district because, based on information and belief, InAuth's West Coast Office focuses on engineering and technical development, including the development of the Infringing Products, and as such, upon information and belief, InAuth has used the Infringing Products in this district. In addition, InAuth has developed its websites and services from its offices in this judicial district, and additionally, it has purposefully and voluntarily engaged in the making, using, selling, offering for sale, or importing in to the United States without authority, products, methods, equipment, or services that practice one or more claims of the '852 patent.

MSIGNIA'S PATENTED TECHNOLOGY

12. mSIGNIA was founded by Paul Miller and George Tuvell in October 2010. Mr. Miller is the Chief Executive Officer of mSIGNIA, and Mr. Tuvell is the current Chief Product Officer and former Chief Technology Officer. Both Mr. Miller and Mr. Tuvell are longtime experts in the field of authentication and computer security.

13. Online identity fraud has been a major problem for many years. Such fraud costs online retailers and banks billions of dollars per year in the United States and abroad. In 2010, a variety of technologies existed for combatting such identity fraud. These technologies are called "authentication" mechanisms. The most basic type of authentication involves the use of a user name and password. Another type of authentication requires the possession of digital "certificates." Another type of authentication recognizes the device of a user. Yet another type of authentication involves the use of "biometrics" (e.g., a fingerprint scanner).

14. Each of these prior art technologies suffers from some well-known drawbacks. Simple passwords can be easily stolen or guessed by computer programs. Alternatively, passwords may become too complicated in which case they are easily forgotten. Other technologies, such as digital certificates and

device recognition, only confirm the identity of a device; they do not confirm the identity of the person using the device. And biometric authentication suffers from the problem that although a fingerprint may be unique, a digital representation of a fingerprint can be intercepted, copied or not available on a new device.

15. Because of these drawbacks, modern systems often use two or more forms of authentication. But many of these secondary authentication techniques are said to create customer "friction." In other words, they are hard for consumers to use. For example, many authentication technologies require the input of a randomly-generated code that is delivered by text message, by email address, or through a separate application. These authentication technologies create user frustration and, at least in the e-commerce setting, may actually prevent bona fide willing customers from completing a purchase.

16. By 2010, these problems were well-known and getting worse due to the rise of mobile handheld devices. Mobile devices generally do not have anti-virus technology installed, and their applications are designed for simplicity, not security. In fact, many mobile devices are not even protected by a password. At the same time, mobile device users expect their phones to "just work," and get frustrated by authentication technologies that unnecessarily block access to resources.

17. Thus, mobile devices presented a new challenge for combatting identity fraud, because they present an inherently unprotected environment in which users refused to accept the "friction" that was traditionally used to provide authentication.

18. The founders of mSIGNIA invented a new system that addressed these problems. Although mobile devices are insecure, they are also rich sources of information. In particular, mobile devices are highly customizable, such that shortly after purchase, each device is essentially unique to a user. Thus, a mobile device can be used to uniquely authenticate a user because the combination of data

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.