US009559852B2

(12) **United States Patent**
Miller et al.

(10) **Patent No.: US 9,559,852 B2**
(45) **Date of Patent: Jan. 31, 2017**

(54) **CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE**

(71) Applicant: **mSignia, Inc.**, Irvine, CA (US)

(72) Inventors: **Paul Timothy Miller**, Irvine, CA (US); **George Allen Tuvell**, Thompson's Station, TN (US)

(73) Assignee: **mSignia, Inc.**, Irvine, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/075,066**

(22) Filed: **Mar. 18, 2016**

(65) **Prior Publication Data**

US 2016/0261416 A1 Sep. 8, 2016

Related U.S. Application Data

(63) Continuation of application No. 14/458,123, filed on Aug. 12, 2014, now Pat. No. 9,294,448, which is a (Continued)

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 9/3271*** (2013.01); ***H04L 9/0861*** (2013.01); ***H04L 9/0866*** (2013.01); ***H04L 9/0872*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC ... H04L 36/0876; H04L 9/0861; H04L 9/0866
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,041,133 A * 3/2000 Califano G06K 9/00067 382/124
6,185,316 B1 * 2/2001 Buffam G06F 21/32 382/100
(Continued)

FOREIGN PATENT DOCUMENTS

JP 2008516472 5/2008
JP 2009111971 5/2009
(Continued)

OTHER PUBLICATIONS

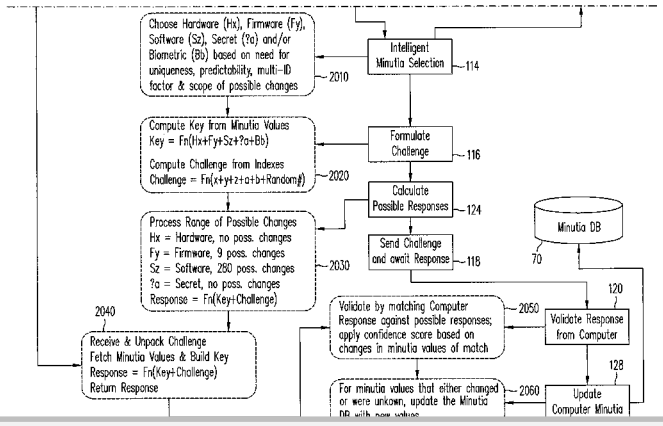
Shibata, Yoichi, "Mechanism-based PKI," Computer Security Symposium, Oct. 29, 2003, vol. 2003, No. 15, pp. 181-186, Information Processing Society of Japan, Japan.
(Continued)

Primary Examiner — Dao Ho
(74) *Attorney, Agent, or Firm* — Haynes and Boone, LLP

(57) **ABSTRACT**

Dynamic key cryptography validates mobile device users to cloud services by uniquely identifying the user's electronic device using a very wide range of hardware, firmware, and software minutiae, user secrets, and user biometric values found in or collected by the device. Processes for uniquely identifying and validating the device include: selecting a subset of minutia from a plurality of minutia types; computing a challenge from which the user device can form a response based on the selected combination of minutia; computing a set of pre-processed responses that covers a range of all actual responses possible to be received from the device if the combination of the particular device with the device's collected actual values of minutia is valid; receiving an actual response to the challenge from the device; determining whether the actual response matches any of the pre-processed responses; and providing validation, enabling authentication, data protection, and digital signatures.

25 Claims, 11 Drawing Sheets



Related U.S. Application Data

continuation of application No. 13/366,197, filed on Feb. 3, 2012, now Pat. No. 8,817,984.

(60) Provisional application No. 61/462,474, filed on Feb. 3, 2011.

(51) **Int. Cl.**
H04L 9/16 (2006.01)
H04L 9/08 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/16*** (2013.01); ***H04L 9/3231*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 63/0428*** (2013.01); ***H04L 63/0861*** (2013.01); ***H04L 63/0876*** (2013.01)

(58) **Field of Classification Search**
USPC 380/255
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,269,160	B1 *	9/2007	Friedman	G06Q 30/0601 370/352
7,330,871	B2	2/2008	Barber	
7,333,871	B2	2/2008	Schwarm	
7,373,669	B2	5/2008	Eisen	
7,908,662	B2	3/2011	Richardson	
7,937,467	B2	5/2011	Barber	
8,213,907	B2	7/2012	Etchegoyen	
8,312,157	B2	11/2012	Jakobsson et al.	
8,335,925	B2	12/2012	Taugbol	
8,375,221	B1 *	2/2013	Thom	G06F 21/57 713/189
2006/0031676	A1 *	2/2006	Vantalon	G06Q 10/02 713/176
2006/0104484	A1 *	5/2006	Bolle	G06K 9/00885 382/115
2007/0124801	A1	5/2007	Thomas et al.	
2007/0174206	A1 *	7/2007	Colella	G06Q 20/382 705/64
2007/0214151	A1	9/2007	Thomas et al.	
2007/0240217	A1	10/2007	Tuvell et al.	
2007/0240218	A1	10/2007	Tuvell et al.	
2007/0240219	A1	10/2007	Tuvell et al.	
2007/0240220	A1	10/2007	Tuvell et al.	
2007/0240221	A1	10/2007	Tuvell et al.	
2007/0240222	A1	10/2007	Tuvell et al.	
2008/0086773	A1	4/2008	Tuvell et al.	
2008/0086776	A1	4/2008	Tuvell et al.	
2008/0175449	A1 *	7/2008	Fang	G06F 21/32 382/124
2008/0196104	A1	8/2008	Tuvell et al.	
2008/0235515	A1 *	9/2008	Yedidia	G06K 9/00073 713/186
2008/0244744	A1	10/2008	Thomas et al.	
2008/0267510	A1 *	10/2008	Paul	G06K 9/00577 382/209
2009/0138975	A1	5/2009	Richardson	
2009/0310779	A1 *	12/2009	Lam	G06K 9/00093 380/46
2010/0027834	A1	2/2010	Spitzig et al.	
2010/0229224	A1	9/2010	Etchegoyen	
2010/0332400	A1	12/2010	Etchegoyen	
2011/0007177	A1 *	1/2011	Kang	H04N 5/232 348/222.1
2011/0082768	A1	4/2011	Eisen	
2011/0093503	A1	4/2011	Etchegoyen	
2011/0113388	A1	5/2011	Eisen et al.	
2011/0293094	A1	12/2011	Os et al.	
2011/0296170	A1	12/2011	Chen	
2012/0201381	A1 *	8/2012	Miller	H04L 9/16 380/255
2013/0340052	A1	12/2013	Jakobsson	
2014/0229386	A1	8/2014	Tervo et al.	

FOREIGN PATENT DOCUMENTS

WO	WO 2010/035202	4/2010
WO	WO 2013/138714	9/2013
WO	WO 2013/154936	10/2013

OTHER PUBLICATIONS

Juels et al., "A Fuzzy Vault Scheme," Designs, Codes and Cryptography, Feb. 2006, pp. 237-257, vol. 38, No. 2, Springer Science + Business Media, Inc., New York/USA.

Notice of Reasons for Rejection dated Sep. 6, 2016, Japanese Patent Application No. P2014/555571.

Jakobsson et al., "Implicit Authentication for Mobile Devices," HotSec'09 Proceedings of the 4th USENIX conference on Hot topics in security, 2009, USENIX Association, Berkeley, California/USA. Retrieved from the Internet on Nov. 18, 2016: <URL:https://www.usenix.org/legacy/event/hotsec09/tech/full_papers/jakobsson.pdf>.

* cited by examiner

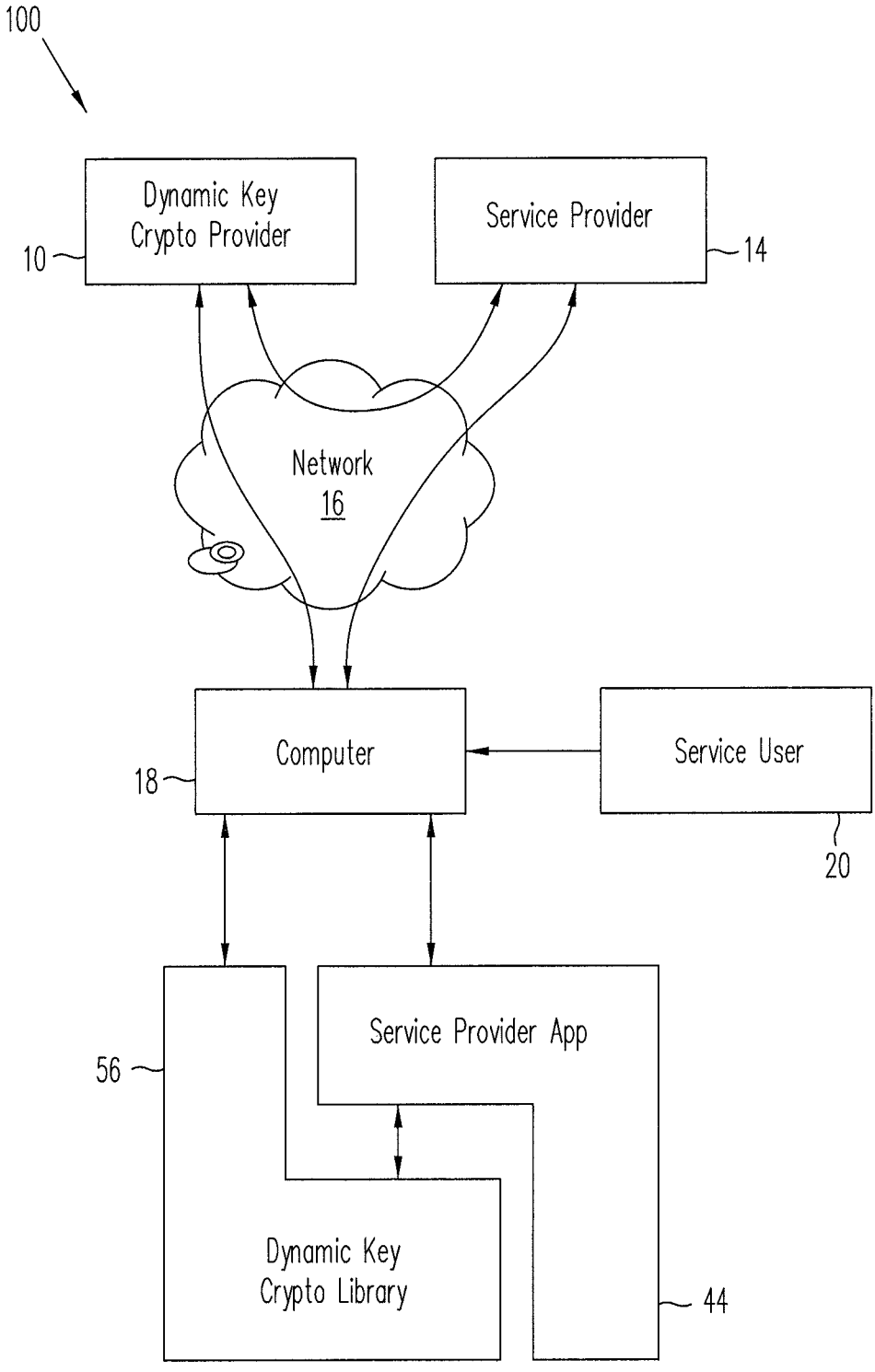


FIG. 1

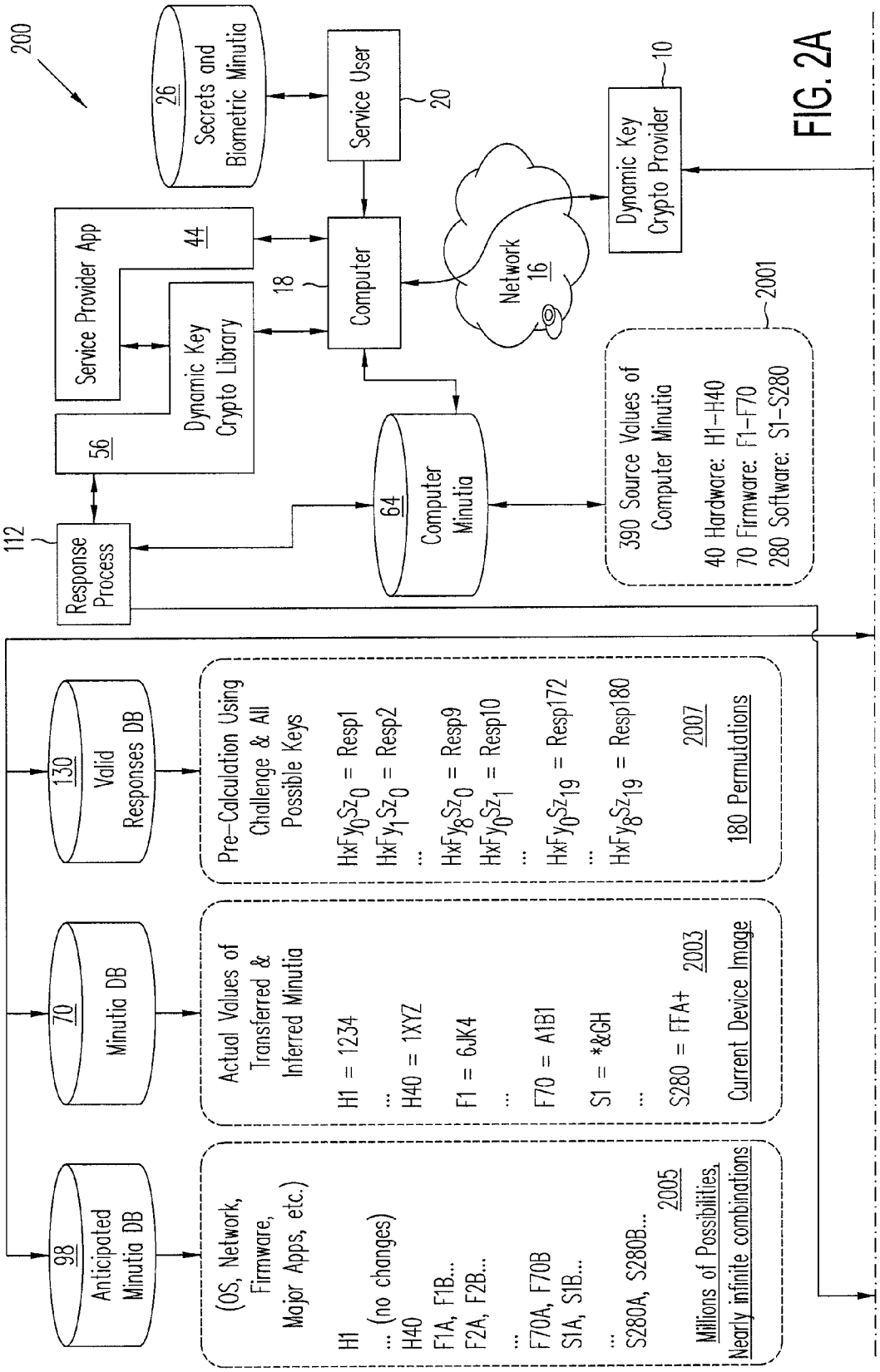


FIG. 2A

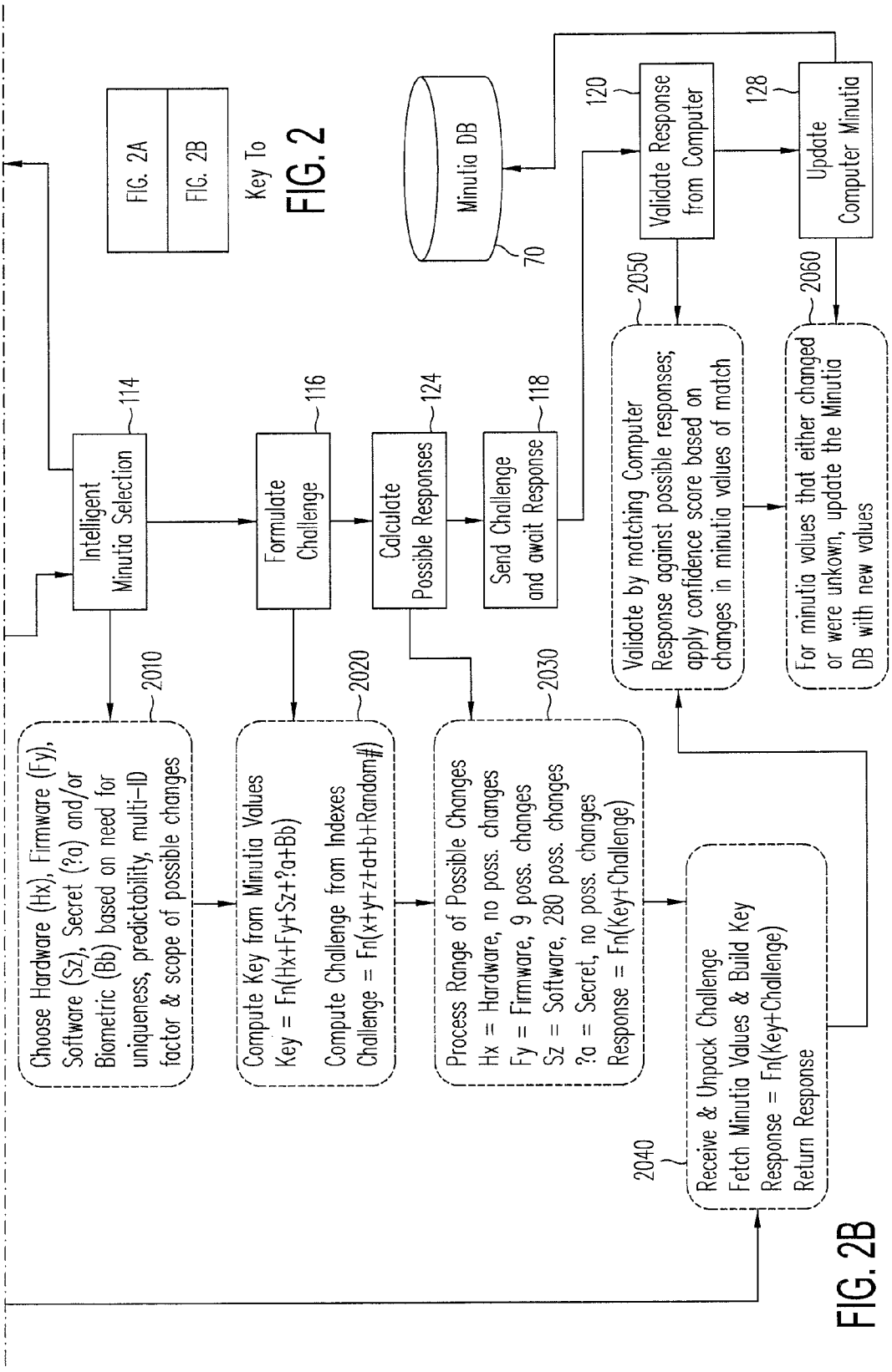


FIG. 2B

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.