



US007295516B1

(12) **United States Patent**  
**Ye**

(10) **Patent No.:** **US 7,295,516 B1**  
(45) **Date of Patent:** **Nov. 13, 2007**

(54)	<b>EARLY TRAFFIC REGULATION TECHNIQUES TO PROTECT AGAINST NETWORK FLOODING</b>	6,865,185 B1 *	3/2005	Patel et al. ....	370/412
		7,058,015 B1 *	6/2006	Wetherall et al. ....	370/236
		7,062,782 B1 *	6/2006	Stone et al. ....	726/22
		7,092,357 B1 *	8/2006	Ye .....	370/230
		7,188,366 B2 *	3/2007	Chen et al. ....	726/23
(75)	Inventor: <b>Baoqing Ye</b> , Nashua, NH (US)				
(73)	Assignee: <b>Verizon Services Corp.</b> , Waltham, MA (US)	2002/0101819 A1 *	8/2002	Goldstone .....	370/229
		2003/0172289 A1 *	9/2003	Soppera .....	713/200

( \* ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1068 days.

**OTHER PUBLICATIONS**

(21) Appl. No.: **10/010,774**

H-Y Chang S. F. Wu, C. Sargor, and X. Wu, "Towards Tracing Hidden Attackers on Untrusted IP Networks", pp. 1-19.

(22) Filed: **Nov. 13, 2001**

S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Practical Network Support for IP Traceback", Technical Report UW-CSE-00-02-01, University of Washington, 6 pgs.

(51) **Int. Cl.**  
**H04J 1/16** (2006.01)  
**H04J 3/16** (2006.01)  
**G06F 11/00** (2006.01)

(Continued)

(52) **U.S. Cl.** ..... **370/232; 370/236; 370/468; 726/22**

*Primary Examiner*—Chau Nguyen  
*Assistant Examiner*—Nittaya Juntima

(58) **Field of Classification Search** ..... **370/229–236.1, 370/395.1, 465**  
See application file for complete search history.

(57) **ABSTRACT**

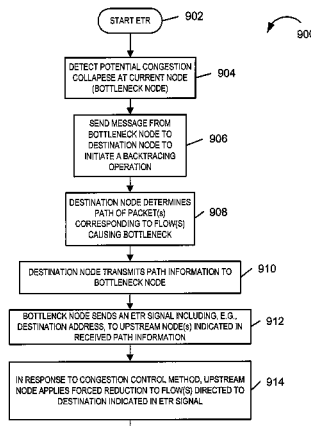
(56) **References Cited**

Methods and apparatus for providing an Anti-Flooding Flow-Control (AFFC) mechanism suitable for use in defending against flooding network Denial-of-Service (N-DoS) attacks is described. Features of the AFFC mechanism include (1) traffic baseline generation, (2) dynamic buffer management, (3) packet scheduling, and (4) optional early traffic regulation. Baseline statistics on the flow rates for flows of data corresponding to different classes of packets are generated. When a router senses congestion, it activates the AFFC mechanism of the present invention. Traffic flows are classified. Elastic traffic is examined to determine if it is responsive to flow control signals. Flows of non-responsive elastic traffic is dropped. The remaining flows are compared to corresponding class baseline flow rates. Flows exceeding the baseline flow rates are subject to forced flow rate reductions, e.g., dropping of packets.

**U.S. PATENT DOCUMENTS**

4,769,811	A *	9/1988	Eckberg et al. ....	370/236
5,090,011	A *	2/1992	Fukuta et al. ....	370/230
5,309,431	A *	5/1994	Tominaga et al. ....	370/235
5,457,687	A *	10/1995	Newman .....	370/232
5,706,279	A *	1/1998	Teraslinna .....	370/232
5,835,484	A *	11/1998	Yamato et al. ....	370/230
5,901,140	A *	5/1999	Van As et al. ....	370/236
5,914,936	A *	6/1999	Hatono et al. ....	370/230
6,028,842	A *	2/2000	Chapman et al. ....	370/235
6,144,714	A *	11/2000	Bleiweiss et al. ....	375/376
6,208,653	B1 *	3/2001	Ogawa et al. ....	370/395.52
6,424,620	B1 *	7/2002	Nishihara .....	370/229
6,463,036	B2 *	10/2002	Nakamura et al. ....	370/236.1
6,657,961	B1 *	12/2003	Lauffenburger et al. ....	370/231
6,724,721	B1 *	4/2004	Cheriton .....	370/229
6,735,702	B1 *	5/2004	Yavatkar et al. ....	726/13

**11 Claims, 10 Drawing Sheets**



## OTHER PUBLICATIONS

"Characterizing and Tracing Packet Floods Using Cisco Routers", downloaded from: [wysiwyg://23/http://www.cisco.com/warp/public/707/22.html](http://www.cisco.com/warp/public/707/22.html), 5 pgs.

"Cert® Advisory CA-1996-26 Denial-of-Service Attack via ping", downloaded from: <http://www.cert.org/advisories/CA-1996-26.html>, 4 pgs., last revised Dec. 5, 1997.

"Cert® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks", downloaded from: <http://www.cert.org/advisories/CA-1996-21.html> on Mar. 14, 2002, pp. 1-8, last revised Nov. 29, 2000.

S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services", Network Working Group Request For Comments: 2475, downloaded from: <ftp://ftp.isi.edu/in-notes/rfc2475.txt> on Mar. 14, 2002, Dec. 1998, pp. 1-32.

L. Houvinen and J. Hursti, "Denial of Service Attacks: Teardrop and Land", Department of Computer Science Helsinki University of Technology, downloaded from: <http://www.hut.fi/~ilhuovine/hacker/dos.html> on Mar. 14, 2002, pp. 1-12.

SecurityFocus home mailing list: BugTraq "The "mstream" distributed denial of service attack tool", downloaded from: <http://online.securityfocus.com/archive/1/57854> on Mar. 14, 2002, May 1, 2000, pp. 1-22.

Bellovin and Leech AT&T Labs Research, "ICMP Traceback Messages", Network Working Group Internet Draft, downloaded from: <http://www.ietf.org/internet-drafts/draft-ietf-itrace-00.txt> on Jul. 9, 2001, Mar. 2001, pp. 1-9.

S. Floyd and V. Paxson, "Why We Don't Know How To Simulate The Internet", AT&T Center for Internet Research, Oct. 11, 1999, pp. 1-13.

S. Floyd and K. Fall, "Promoting the Use of End-to-End Congestion Control in the Internet", May 3, 1999, pp. 1-16.

K. Thompson, G. J. Miller, and R. Wilder, "Wide-Area Internet Traffic Patterns and Characteristics", IEEE Network, Nov./Dec. 1997, pp. 10-23.

S. Floyd and V. Jacobson, "Link-sharing and Resource Management Models for Packet Networks", IEEE/ACM Transactions on Networking, vol. 3, No. 4, Aug. 1995, 22 pgs.

S. Floyd and V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance", Lawrence Berkeley Laboratory University of California, 1993, pp. 1-22.

\* cited by examiner

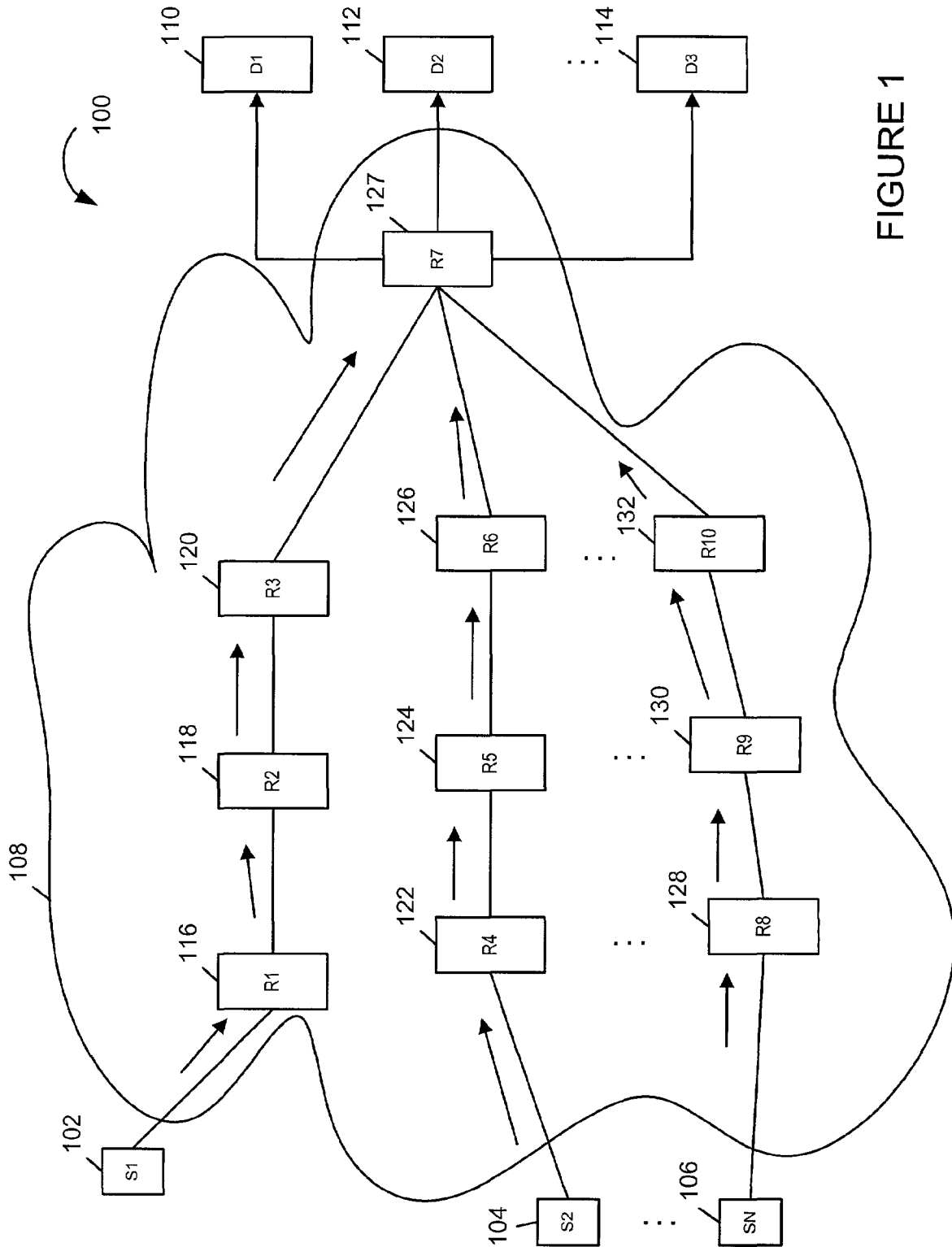


FIGURE 1

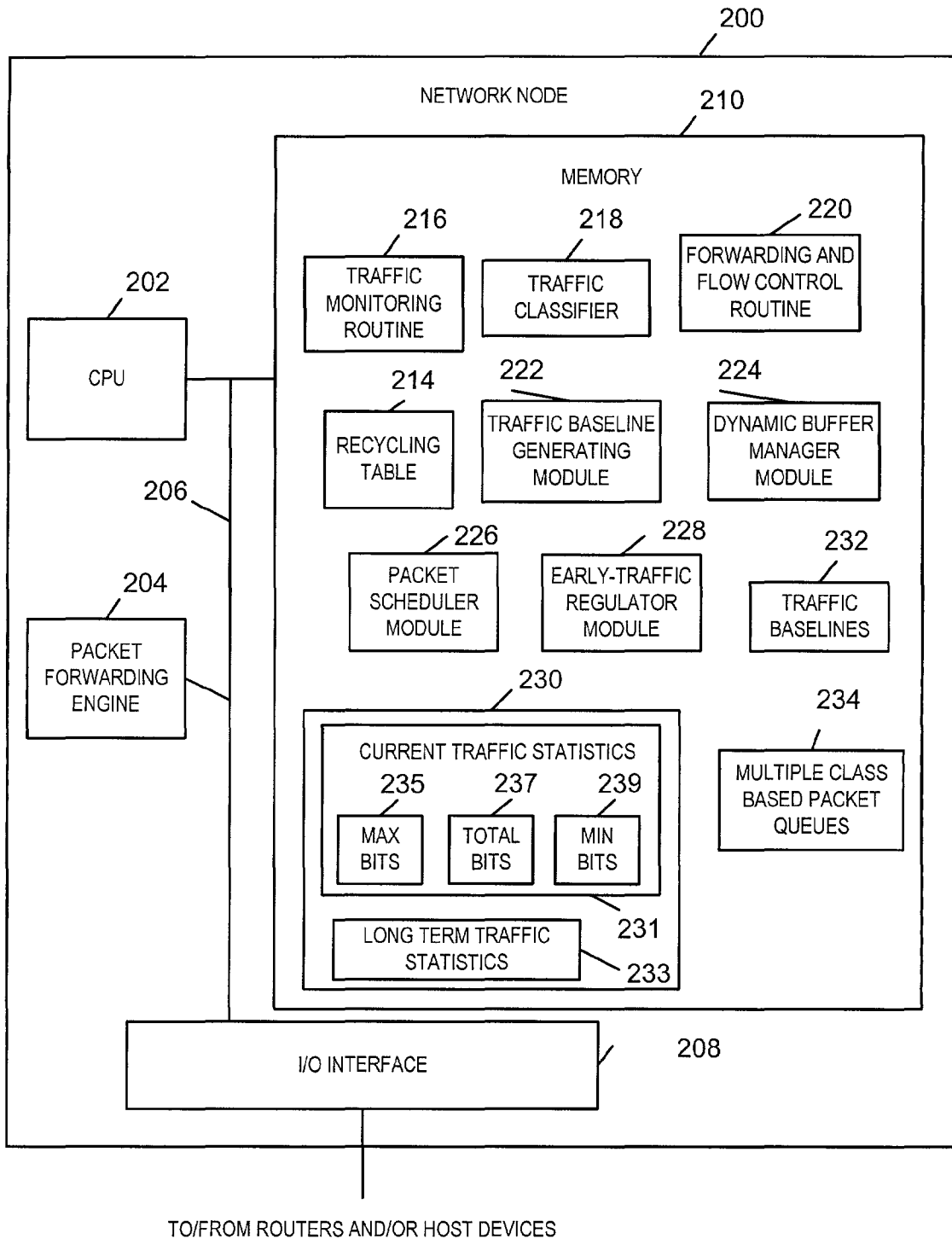


FIGURE 2

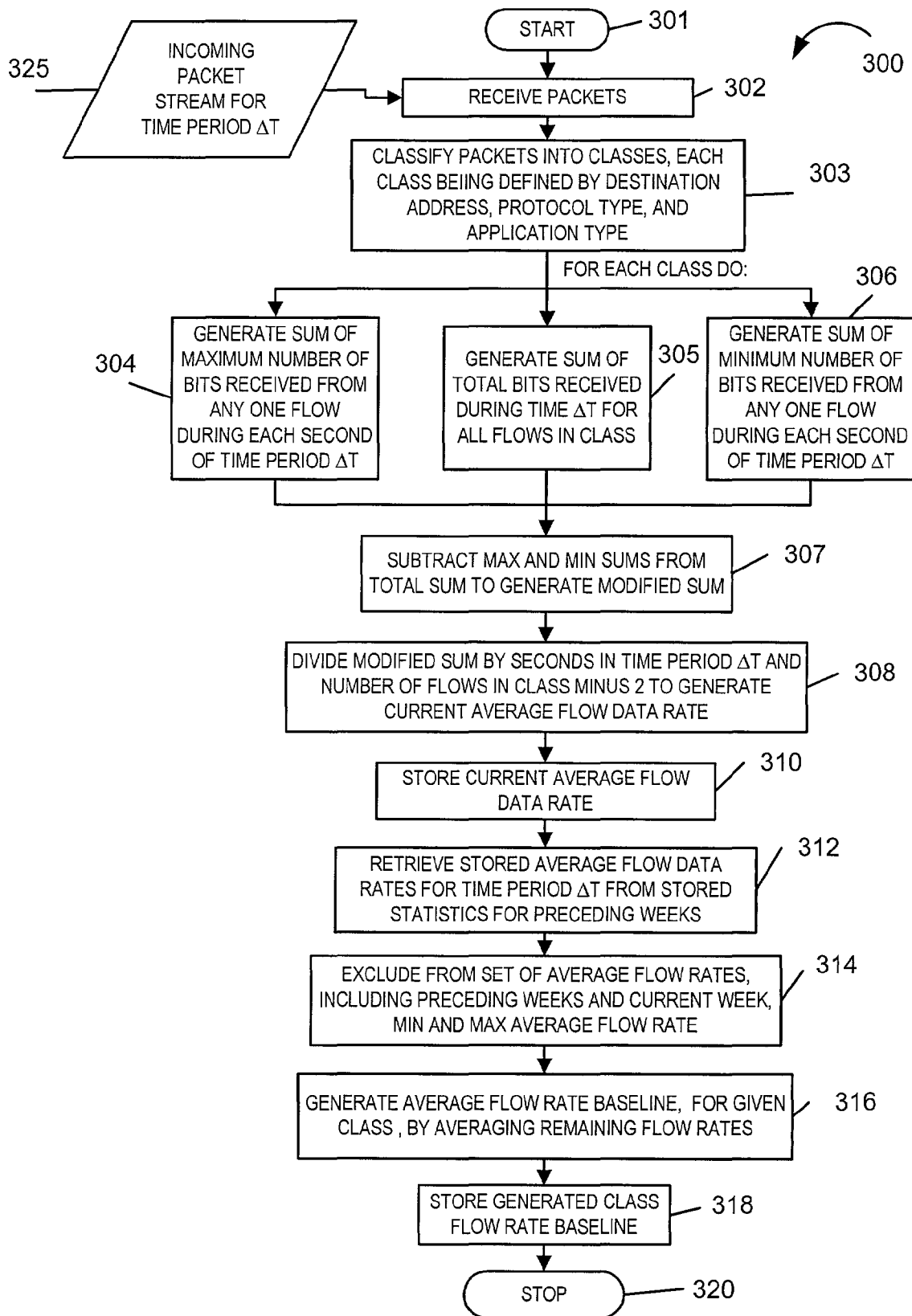


FIGURE 3

# 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.