



NetNumber Expands Subscriber Data Management Strategy with EIR Application to Prevent Use of Stolen Mobile Devices

LOWELL, Mass. — ~~Oct~~^{Sept.} 4, 2016 — NetNumber today announced availability of the Equipment Identity Register (EIR) application on the industry's most robust centralized signaling and routing (CSRC) platform, TITAN. This application expands upon the company's subscriber data management (SDM) strategy, and is deployed in circuit switched (CS), packet switched (PS) and Long Term Evolution (LTE) networks to prevent the use of stolen mobile devices, thereby protecting users' data. The theft of mobile devices, particularly smartphones, continues to increase around the globe, and the high resale value of handsets and their information make them a prime target for thieves.

“The rise in thefts of mobile devices supports the rise in counterfeit handsets since stolen SIM cards most often end up in these devices. These grey market devices have been a challenge for the mobile phone industry for a long time,” explained Sue Rudd, Director Service Provider Analysis at Strategy Analytics. “The EIR Application can be an effective solution for operators looking to protect their networks and subscribers.”

The NetNumber EIR application is designed for operational efficiency, high performance and scalability. Subscriber and other data is provisioned centrally and distributed in real-time to the EIR nodes. The application supports all three registries known as white, black and grey lists to make a distinction between all number series permitted, barred and tracked, respectively. The NetNumber EIR application can either be deployed in combination with HLR and HSS servers in existing networks or in collocated scenarios with other NetNumber applications like HSS, HLR, DSC, and STP. With the collocated scenarios the data can be accessed also by NetNumber HLR and NetNumber HSS for seamless interworking across multiple network domains.

“Governments are looking to mobile device manufacturers, users, and network operators to help deter thefts of mobile devices and secure customer data,” said Matt Rosenberg, NetNumber vice president of Global Sales. “Given the sensitive and growing nature of security threats globally, it is becoming more critical for operators to know if the devices connecting to their networks are

authorized or have been reported as lost or stolen. With our comprehensive SDM solution, operators can synchronize subscriber data with other key functions of the core network, including with the OSS/BSS layers, and gain significant efficiencies due to the centralized data management approach on TITAN.”

NetNumber TITAN provides a common, virtualized infrastructure for all signaling control, routing policy enforcement and subscriber database services in the network. It uniquely delivers centralized provisioning and management combined with a powerful distributed, in-memory database replication method that enables all signal processing to happen at the optimal location in an operator’s network. TITAN is transforming how operators deliver new services to their customers while significantly simplifying the network core and reducing operating costs.

Today, TITAN is deployed on more than 350 servers on five continents, and supports more than 200 billion transactions per month.

Learn more about TITAN at <http://netnumber.com/products/titan/> or by contacting sales@netnumber.com.

About NetNumber

NetNumber, Inc. brings 16 years of experience delivering innovative signaling control solutions that enable carriers to accelerate implementation of new services across multiple generations of networks, while dramatically simplifying the core network and reducing operating costs. Today, we are the leading provider of Centralized Signaling and Routing Control (CSRC) solutions to the global communications industry. Visit www.netnumber.com for more information. Connect with us on Twitter, LinkedIn, Google+ and Facebook.

#

Contact Information:

Kim Gibbons

+1 408 398 5223

kgibbons@netnumber.com