

MARKET BRIEF

Are Home Location Register (HLR) Lookups Putting Your Business at Risk?

A Constantly Moving Target

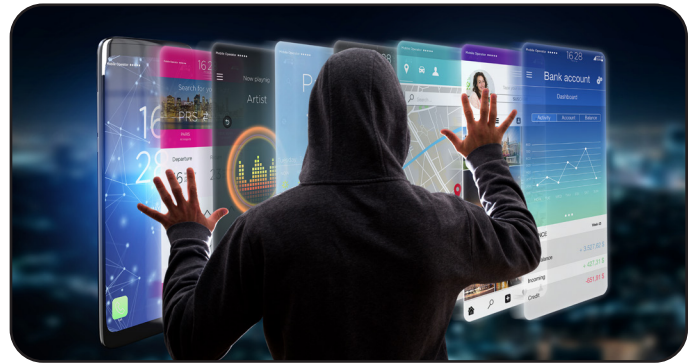
There was a time when numbering and call routing were simple. Not anymore. With tens of millions of phone numbers porting to a different network every week, Communications Service Providers (CSPs) must be able to identify what network a phone is on in order to route a call or message to it in fractions of a second. Getting that detail wrong is a costly mistake.

To run networks efficiently, CSPs need to route calls and text messages via the most cost-effective path possible. Least cost routing (LCR) looks to ensure a CSP does not send a call or message to the wrong network and that it connects the call using a route that best suits the interconnection agreements it has in place.

Keeping Track of the Numbers

To place a voice call or send a SMS requires that the sending party know the network on which the handset is currently registered; the exact location can be left to the actual terminating CSP. Traditionally, within the infrastructure of the CSP, there is a component called the Home Location Register (HLR). Effectively, CSPs 'ping' the HLR over the signaling path of the global mobile network to get the information required to forward a call or text message. The HLR system dates back to the earliest days of mobile communications.

While it might seem perfectly legitimate for CSPs to use the HLR in this way, the number of people with access to the mobile signaling



system has changed dramatically and the way CSPs use handsets now is very different to those breakthrough days and the HLR approach now carries a potential risk for CSPs and consumers.

The Weaknesses Exposed

Today many enterprises, from banks to delivery services, use applications to send SMS messages and voice calls to their customers as part of a two-factor authentication process. The SMS is used to provide information about bank account usage or to keep them up-to-date on the progress of an order. These applications are often run by specialist aggregators that have a direct connection to the signaling system and can access the HLR just like a CSP does. This means they can access portability information, location and other data about that mobile subscriber. It also means that they can find a way to direct traffic over grey routes to avoid paying legitimate charges, which can lead to unreliable and sometimes delayed SMS delivery.

The problem does not end there though. Fraudsters have recognized this weakness and have been able to masquerade as aggregators or legitimate users and use the network's signaling system to hack and track mobile numbers.

Aside from fraudsters and those looking to use grey routes, legitimate enterprise users and aggregators can also be exposed if they access HLR data. This is because the HLR request potentially gives companies access to personal data about a user that could violate privacy regulations such as the General Data Protection Regulation (GDPR). Companies may fall foul of those regulations and be held responsible even if they were not aware the action fell under the scope of those regulations.



Are Home Location Register (HLR) Lookups Putting Your Business at Risk?

It Doesn't Have to be This Way

There is an alternative. TruNumber® Routing provides CSPs, enterprises and aggregators with legitimate number portability information that comes straight from authoritative numbering sources, including number portability clearinghouses and gateways. The data is drawn from the porting service already used by CSPs when customers switch networks, so it is always accurate.

TruNumber Routing is updated with new porting information in near real-time, directly in line with how frequently the home country CSPs update their register and can be accessed via an industry-standard ENUM query service or FTP database download for selected countries.

This critical data is needed to ensure that SMS and voice calls go to the right network and the sender does not get access to any other personal data about the intended handset and its exact location.

The Most Sense, Least Cost Route

While HLR data was once considered the best way to access number portability information, it is now an unsecure and unreliable service accessed by too many questionable parties, reveals too much information and is wide open to misuse and abuse. CSPs should no longer count on HLR data to ensure proper network routing. Instead, they need data that comes directly from authoritative sources, such as number portability clearinghouses, which are updated frequently and easily accessible.

While numbering and call routing may not seem as simple as it once was, there are safe, efficient and cost-effective ways for CSPs to obtain the correct network routing information they need to accurately send calls and text messages to their customers.



Find out how TNS can help you with a wide range of telecom solutions:

solutions@tnsi.com
tnsi.com

©2025 Transaction Network Services. All Rights Reserved.

USA
Europe
Asia Pacific

+1 703 453 8300
+44 (0)114 292 0200
+61 2 9959 0800