**Workshop on Caller ID Spoofing**

**2 June, Geneva**

**Welcome**

Reinhard Scholl

Deputy to the Director, Telecommunication Standardization Bureau
International Telecommunication Union

Distinguished guests

Ladies and gentlemen,

Welcome to this workshop on ‘Caller ID Spoofing’. Malcolm Johnson gives his best regards – he is currently attending the ITU Kaleidoscope event in Saint Petersburg.

We sandwiched this workshop in between the meeting of ITU-T SG 3 which met last week and the one of ITU-T SG 2 which has started last week with WP2/2 meeting and with WP1/2 and WP2/2 meeting for this week. We also welcome delegates from other study groups such as ITU-T SG 16 and ITU-T SG 17, and representatives from IETF STIR WG, 3GPP TSG SA3 , M3AAWG (Mobile Messaging Malware Anti Abuse Workgroup) and LAP (London Action Plan), and ECO (European Communications Office).

We have all come to appreciate caller identification, for many reasons, some nobler than others.

It tells me if it is a trusted friend or colleague calling me, or my mother, and that gives me the information I need to decide whether I have enough time to take the call.

But it is not just the tool our children use to avoid us, it is essential in today’s interconnected world. In a world where anyone can reach anyone via telecommunications networks, caller identification is key to establishing trust.

We communicate by sharing a vast range of interconnected networks and establishing trust frameworks has been a core element of expanding the use and applications of the Internet.

I’m sure all in this room will be familiar with the importance of ITU-standardized X.509 digital certificates and the broader public-key infrastructure – it provides a mechanism to establish trust on the Web and, without it, the rise of e-commerce would have been impossible.

If it puts on a good enough act, a webpage masquerading as a financial services platform might succeed in requesting you to provide personal information, such as your home address or credit card details.

And so it is with Caller ID spoofing. If we can be led to believe that we are receiving a call from a trusted caller – with a caller spoofing our trusted phone numbers – we will be much more likely to hand over compromising information.

Caller IDs provide a trust framework, and maintaining the integrity of this trust framework is essential.

This is something ITU takes very seriously. The membership has given us a strong mandate to tackle this issue, which is articulated in:

* WTSA-12 Resolution 65 on “Calling Party Number Delivery, Calling Line Identification and Origin Identification”; as well as in,
* WTSA-12 Resolution 29 on “Alternative Calling Procedure”;
* PP-06 Resolution 21 on “Alternative Calling Procedures on Telecommunication Networks”; and,
* WTDC-10 Resolution 22 on “Alternative Calling Procedures on International Telecommunication Networks, Identification of Origin and Apportionment of Revenues, in Providing International Telecommunication Services”.

CLI is also covered by the new International Telecommunication Regulations (ITRs), which provides that Member States shall endeavor to ensure that international Calling Line Identification (CLI) information is provided, taking into account the relevant ITU-T standards (ITU-T Recommendations).

Particular to the Standardization Sector, WTSA-12 requested that ITU-T SG2 and SG3, and possibly SG17, study the impact of non-origin identification and spoofing, including its economic and security impacts.

This workshop is part of delivering an answer to this call from our membership. I am sure it has brought many new people into the fold, and I look forward to meeting you this afternoon and to learning from what I am sure will be a very interesting discussion.

Thank you. I wish you a very productive workshop.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_