Resolution 97– Combating mobile telecommunication device theft

Essence of the Resolution

- **Prevention Strategies:** Implement measures to discourage theft, such as improved security features.
- **Tracking and Recovery:** Develop technologies and systems to track and recover stolen devices, reducing financial losses for users and deterring theft.
- **Disabling Stolen Devices:** Create mechanisms to render stolen devices unusable, minimizing their value to thieves.
- **Protection for Device Owners:** Enhance security measures to protect users from financial and personal information losses and potential misuse of stolen devices.
- **Industry Collaboration:** Encourage collaboration among manufacturers, service providers, and government bodies to develop effective solutions against device theft.

Limitations of the resolution

- **Automated Deactivation:** The proposal for automated device deactivation may not consider all user scenarios, potentially affecting genuine device owners facing password or PIN issues. Additionally, it might not cover every unauthorized access possibility.
- **Network Access Prevention:** The plan to block stolen devices from mobile networks overlooks other network types like Wi-Fi. Relying solely on unique identifiers for blocking could have limitations if some networks don't check these identifiers.
- **Tampered Device Identification:** While aiming for accurate identification of tampered devices, the proposal might not encompass all tampering methods, leading to challenges in distinguishing genuine from tampered devices in every situation.
- **International Coordination:** Although recommending global databases for reporting stolen devices, the proposal lacks comprehensive international collaboration. Insufficient data sharing could allow stolen devices to move unchecked across borders.
- **Privacy Protection:** While emphasizing consumer data protection, the proposal might lack clear guidelines or enforcement methods for effective data protection in lost or stolen devices.
- **Market Access Controls:** The proposal suggests controlling market access for stolen devices but may not cover every avenue allowing their sale. Lacking strict controls or legal actions against sellers of stolen devices could limit its effectiveness.
- **Tampering Prevention:** While suggesting policies and education, the proposal might not comprehensively cover preventing tampering or misuse of hardware/software to alter device identifiers, requiring more effective strategies.

Modifications proposed

- **Enhanced Automated Deactivation:** Implement a more nuanced automated deactivation system that considers scenarios where genuine owners might face difficulties accessing their devices. Introduce backup access methods for legitimate users to regain control if they forget passwords or PINs.
- **Comprehensive Network Access Prevention:** Develop a multi-tiered approach to prevent stolen devices from accessing various networks, including Wi-Fi. Explore solutions beyond unique identifiers to cover networks that don't check these identifiers.
- **Refined Tampered Device Identification:** Invest in advanced technology capable of accurately differentiating between tampered and genuine devices across various tampering methods. Continuously update and refine this technology to counter evolving tampering techniques.
- **Global Collaboration Framework:** Establish a robust global collaboration framework among countries to efficiently share stolen device data. This would require international coordination and standardized protocols to prevent cross-border illegal trade of stolen devices.
- **Enforced Privacy Protection:** Develop and enforce strict regulations and measures to safeguard consumer data on lost or stolen devices. Implement foolproof mechanisms to remotely wipe personal data and educate users on their usage.
- **Tightened Market Access Controls:** Strengthen partnerships between regulatory agencies and customs to enhance controls on the sale of stolen devices. Enforce stringent actions against outlets involved in selling stolen devices.
- **Holistic Tampering Prevention:** Develop comprehensive policies addressing hardware and software tampering, including strict penalties for tampering with device identifiers. Educate law enforcement on these measures for effective implementation