Recommendations to mitigate SS7 vulnerabilities

1 Introduction

The USSD and SMS communication channels with which the end-user communicates with the DFS provider rely on the legacy Signaling System 7 protocol which has for long been "broken" and with many published vulnerabilities, some over 20 years old, which enables attackers to commit fraud, compromise DFS and steal funds through account takeovers, DFS interception, denial of service attacks etc.

The SS7 Vulnerabilities and Mitigation Measures for DFS Transactions contain details on the recommendations for DFS regulators and mobile network operators to mitigate SS7 vulnerabilities. These recommendations are summarized below.

2 Regulatory guidance to address vulnerabilities due to SS7

a) **Regulatory coordination: -** a bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the Central Bank on SS7. A sample MOU is included at Annex B of the Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions. The MOU should include modalities around the creation of a Joint Working Committee on DFS security and risk-related matters that address SS7.

b) **Incentivize the industry** - create incentive programs with industry to promote the development of countermeasures in the Telcom-DFS anti-fraud field.

c) **Incentivize the operators and providers** - create regulation that passes the financial damage from DFS fraud to the DFS providers and to the telcos, creating a financial incentive for action.

d) **Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS** - telecom and financial regulators around the world needs to be aware of the risks and most importantly be aware that there are available solutions to mitigate these risks.

e) **IMSI validation gateway**: An IMSI validation gateway can be used to validate to DFSPs and banks that the real, registered customer is using the system via USSD for DFSPs to detect USSD interception.

f) **Telecom regulators to establish baseline security measures for each category (3G/4G/5G)** - Telecom regulators are encouraged to establish baseline security measures for each category (3G/4G/5G) which should be implemented by telecom operators to ensure a more secure interconnection environment.

g) **Mobile Network operators and DFS operators should consider adopting controls in section 2.1 and 2.2 below.**

2.1 MNO controls to address DFS vulnerabilities due to SS7

i. **Secure GSM ciphers for radio network traffic**: The mobile operator should ensure the use of secure radio encryption between users' devices and base stations.

ii. **Session time out:** use session timeout for USSD and STK to reduce success man in the middle attacks.

iii. **USSD PIN masking:** Deploy USSD PIN masking whenever possible.

iv. **Secure and monitor core network traffic**: Use a TLS v1.2 or higher to secure the connection between the SMSC GW, USSD GW, and the DFS application server.

v. **Limit access to traces and logs**: Ensure there is an auditable process in place to review access to traces and logs on interfaces that use inherently insecure protocols. USSD PINs should not be logged in the event data records.

vi. **SMS filtering**: Remote attackers rely on mobile networks to deliver binary SMS to and from victim phones. Mobile operators should implement blocking the ability to send and receive binary messages like OTA SMS. Such SMS should only be allowed from whitelisted sources.

vii. **SMS home routing:** This is the barring of all outgoing and incoming SMS except those routed through the home network hosts. OTA messages with STK coding from home subscribers should be restricted to only be sent to/by the MNO platform—and not to other subscribers.

2.2 DFS provider controls to address DFS vulnerabilities due to SS7

DFS operators should consider adopting the following controls to mitigate SS7 risks**.**

i. **Session time out:** use session timeout for USSD and STK to reduce success man in the middle attacks, OTP messages for DFS should also have a session time out.

ii. **Transaction limits for insecure channels:** Set transaction limits for customer withdrawals and transfers through insecure channels like USSD.

iii. **User education:** DFS users should be educated on how to engage securely with digital financial services including impacts of using rooted devices, connecting to public Wi-Fi, installing unverified applications etc.

iv. **Bidirectional OTP SMS flow**:- The DFS provider should make the authentication flow bidirectional, that is receive the OTP from the user, not send it.

v. **Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD** by verifying using secureOTP, location validation, IMSI and IMEI validation