International Telecommunication Union

FINANCIAL INCLUSION GLOBAL INITIATIVE (FIGI)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Security, Infrastructure and Trust Working Group

Security recommendations to protect against Digital Financial Services SIM risks and SIM swap fraud.

1 Best practices for regulators to protect DFS against SIM risks

The Security testing for USSD and STK based DFS applications contain details on the recommendations on mitigating SIM vulnerabilities.

1.1 SIM vulnerabilities

Financial institutions have adopted digital means and are continuing to avail financial products on mobile based application like Unstructured Supplementary Services (USSD) and STK banking, which makes financial services available anywhere, anytime through strings of interactions via Unstructured Supplementary Service Data (USSD), Short Messaging Service (SMS), internet. The interactions between the mobile user and the network are authenticated with the SIM card. However, there has been increased fraud risks on SIMs due to threats arising from notably SIM swaps, SIM jacker attacks and SIM recycling and number porting.

SIM swap fraud

SIM swap fraud has become a common tactic used to takeover accounts. In a SIM swap fraud, a telecom provider is tricked into issuing a replacement of a victim's SIM to a fraudster allowing them to take over a DFS accounts that relies on the SMS one time password (OTP) or USSD for authentication.

SIM recycling risks

SIM recycling risks is related to reliance on the phone numbers, Mobile Station Integrated Services Digital Network (MSISDN) as the primary DFS account numbers. Telco providers reassign phone numbers that are dormant or deemed to have churned (not used within specific period). The reassignment of the phone number may effectively lead to an account takeover of the DFS wallet associated with the number if the DFS provider is not aware of the change of ownership.

Binary Over the Air attack (SIM jacker)

The SIM jacker attack exploits a vulnerability in a SIM Card library called the S@T browser. A specially formatted binary text message is sent to the victim handset, which contains a set of commands to be executed by the S@T Browser environment in the SIM card. The commands can instruct the handset to exfiltrate this information, force the mobile device to initiate a USSD request, make a phone call, or send a message.

2 Regulatory guidance to mitigate SIM risks (SIM swap, SIM cloning, SIM recycling and binary over the air attacks).

a. **Regulatory coordination: -** a bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the Central Bank on SIM swaps. A sample MOU is included at Annex B of the Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions

b. **Mobile network operators should consider adopting the following controls to mitigate SIM risks and fraud in section 2.1 below.**

2.1 Mobile network operator controls to mitigate SIM risks and fraud

i. Standardization by regulators of SIM swap rules amongst MNOs/MVNOs by the regulator, including SIM swaps leading to porting of numbers to other MNOs/MVNOs.

ii. Where SIM replacement is carried out by proxy, the MNO/MVNO or its agents must capture a biometric, facial image of the proxy which must be kept for a specified period.

iii. MNOs should notify DFS providers on swapped SIMs, ported and recycled numbers.

iv. **Biometric SIM swap verification**: Mobile providers should adopt biometric verification before a SIM swap/SIM replacement is performed.

v. **Multifactor user validation before SIM swap:** Mobile providers should use using a combination of something they are, something they have, or something they know authenticate users before a sim swap. User authentication challenges should include verification of personal details (address, email address, DOB), Account information (activation date, last payment, service type), device information (IMEI, ICCID), usage information (recent numbers), knowledge (PIN or password, security question), possession (email OTP, SMS OTP).

vi. **Information sharing with DFS provider on SIM swaps and SIM recycling**: MNO should design a mobile number recycling process that involves communicating with DFS providers on Mobile Subscriber Identification Numbers (MSIDN) churned or recycled. (In this context: number recycling is when the MNO reallocates a dormant/inactive Mobile Subscriber Identification Number (MSISDN) to a new customer). When a SIM is recycled, the mobile operator reports the new IMSI related to the account phone number. The DFS provider should block the account until the identity of the new person holding the SIM card is verified as the account holder.

vii. **SIM swap notifications to users:** On request for a SIM swap, sending of notifications via SMS, IVR or Push USSD of the SIM swap request to the (current) SIM/phone number owner, in case the SIM is still live, and then waiting for a positive response from the owner for a certain time before undertaking the SIM swap

viii. **Secure SIM data protection**: The mobile operator should safeguard personal information that can be used during SIM swaps and securely store SIM data like IMSI and SIM secret key values (KI values).

ix. **Holding time before activation of a swapped SIM**: A general holding time from the time of a SIM card request to providing the new SIM card to the requestor

x. **Customer support representatives training**: Provide better training to customer support representatives. Representatives should thoroughly understand how to authenticate customers and that deviations from authentication methods or disclosure of customer information prior to authentication is impermissible.

2.2 DFS operators controls to mitigate SIM risks and fraud

xi. **Real time IMSI/ICCID detection**: DFS and Payment Service Providers should be able to detect real-time whenever a SIM card associated with DFS services is swapped or replaced. Further verification before authorizing any transaction or account changes with new SIM should be required.

xii. **Real time device change detection:** Device authentication to improve endpoint security by tracking the IMEI's of the devices used to access financial services. In this way, an account that changes devices can be flagged by the DFS operator

xiii. **Encourage use of secure DFS access:** Avail the customers the option to opt-out of the USSD or STK channels for financial transactions, especially those that can access the DFS using an app.

The measures recommended above could also be adopted as regulations by DFS regulators.