Toll Fraud Security Program

Toll fraud, like other corporate crimes, causes a high loss to companies through both direct and indirect costs. These steps outline some minimum elements a company may use to design a toll fraud security program.

Step 1: Establish responsibility.

Designate a member of management or your Director of Security to develop and maintain a toll fraud prevention and response program.

Step 2: Include toll fraud, abuse of phone privileges, and password/authorization number protection into corporate policy.

This can be combined with Human Resources Rules and Regulations, as part of the Security Policy or as a separate policy.

Step 3: Establish good physical security measures for the facility as well as for telecommunications assets.

Restrict unauthorized access to equipment rooms and wire connection closets (MDF, IDFs). Protect system documentation and reports from compromise.

Step 4: Train users and/or switchboard operators and administrators.

Educate users about the exposures, policies and procedures, indicators of abuse, and how to report suspected problems. Training should include protection of calling cards, cellular phones, and fraud schemes.

Step 5: Establish port security procedures.

Establish security measures to manage and control access to the ports into the communication system. The security measures should also control the calling privileges user will have access to. Use passwords, authorization codes, and barrier codes set to maximum length and changed frequently. Assign calling privilege restrictions levels to users on a need-to-call basis. Block off-hours and weekend calling privileges or use alternate restriction levels when possible.

Step 6: Secure the administration system.

Management of the access into administration and maintenance capabilities is an important part of the plan. Control administrative access passwords and change them frequently. Never store administrative port numbers or passwords as part of a connection 'script'. Use report port security devices or other types of equipment to 'lock-up' administrative and maintenance ports.

Step 7: Monitor system usage and the latest techniques used by hackers and phreakers to break into your systems.

System security monitoring plays a critical role in the overall security program by allowing the company to react quickly to suspected fraud and subsequently minimize loss. Monitor call detail records and '800 service' billing records for unusual activity. Monitor invalid login attempts on remote access and administrative ports. Establish thresholds and monitor port and trunk activity levels.

Toll Fraud Warning Signs

The following warning signs may indicate the presence of toll fraud within your system. Communications employees should be trained to recognize these warning signs and the company should immediately investigate if any one is detected.

- Customers or employees complain that the 800 number is always busy. Could even impact local Direct Inward Dial (DID) lines.
- Switchboard operators complain of frequent hang-ups or touch-tone sounds when they answer.
- Significant increase in 'internal' requests for 'operator assistance' in making outbound calls, particularly international calls.
- Unexplained increase in long distance usage.
- Heavy call volume on nights, weekends, and/or holidays.
- Station Message Detail Recording (SMDR) shows an unusual amount of short duration calls.
- Established thresholds on trunk groups are exceeded.
- Switchboard operators note or complain about frequent calls from individuals with foreign accents.
- Staff or customer complaints of inability to enter voice mail system.
- Any attempts by outsiders to obtain sensitive information regarding the telecommunications system or calls from individuals posing as employees when they clearly are not.
- Sudden or unexplained inability to access specific administrative functions within the system.
- Employees complain of difficulty in obtaining an outside line.
- Simultaneous Direct Inward System Access (DISA) authorization code use coming from two different places at the same time.
- An upsurge in use on DISA or other trunks.

- Unusual increase in customer premises equipment-based memory usage.
- Unexplained changed in system software parameters.
- Unexplained problems related to being ‘locked out’ of the system or Personal Identification Number (PIN) changes in the voice mail system.
- Significant increase in calls from a single geographic area or from the same Automatic Number Identification (ANI).
- Any discrepancies in telephone bills, such as unusual calling patterns, calls to international locations with which the user does not normally interact, and calls that cannot be accounted for.