Norstar – Reducing Toll Fraud Issues

The purpose of this document is to provide information on recommended programming and set up guidelines to avoid potential toll fraud issues on Norstar. This document will include all Norstar products that allow a user to access an external line to make outbound calls. Although this document provides guidelines, it will not guarantee that all toll fraud issues will be eliminated, however, following these guidelines will certainly reduce the risk of the Norstar system from being 'hacked' and unauthorized toll charges being incurred.

Toll fraud occurs when hackers are given an opportunity to access the central office facilities that are connected to the system for making outgoing calls. Norstar has several password and programming capabilities, from a system and user level, to aid in the security of the system which are outlined below. This document will focus on the Norstar KSU and the Voice Messaging components as they are the 2 products that offer central office facilities access.

SYSTEM

The Key Service Unit (KSU) is the main control equipment for the Norstar system and provides the connection interfaces for the external lines and stations. Inserted into the KSU is the software cartridge which contains both the operating software and the customer programmed data. The software provides different levels of programming areas depending on what is being programmed and these are identified below. The Configuration and Administration Programming capabilities are only accessible on site using one of the two-line Norstar telephone sets connected to the system.

Configuration Programming:

Configuration Programming is password protected and is usually accessed by a certified technician for programming the system parameters. Parameters included in this area related to potential toll fraud are Restrictions, DISA, and COS (Class of Service Passwords).

Recommendation: *All Norstar systems are shipped from the factory with the same default configuration password. Ensure this default password is changed by the service provider to prevent unauthorized access by someone else who is familiar with Norstar.*

Restrictions provide the flexibility to add dialing restrictions to prevent specific area codes, telephone numbers, and long distance calls to be dialed. These restrictions can be applied on a per set basis, per line basis, and a per line per set basis.

Recommendation: *Toll restrict those telephones that should not be allowed to make long distance calls.*

DISA (Direct Inward System Access) is a capability of the Norstar system to automatically answer a line and provide dial tone so that the caller can then dial an internal extension number or access an outside line to make a call. This feature is often used in situations where off-site employees need to make business long distance calls and have the calls billed directly to the company.

Recommendation: *If DISA is used, program it so that it answers with stutter dial tone. Stutter dial tone requires a password to be entered prior to any calls being made.*

COS Passwords are user definable 6 digit passwords that are assigned to employees that allows them to override any restrictions (see above) that are assigned to their telephone or lines, and, to get access to tandem calling when DISA with stutter dial tone (see above) is implemented. There are a total of 100 passwords that can be assigned.

Recommendation: *Ensure passwords are more complex numbers than 111111, 123456, etc to ensure integrity of the system.*

Administration Programming:
Administration Programming can be accessed through the Configuration Programming but is also separately accessible with its own password. Administration Programming is usually used by a system administrator to set up capabilities such as Set Names, User Preferences, System Speed Dial. However, the Administration Programming also gives access to Restrictions and COS Passwords.
Recommendation: *All Norstar systems are shipped from the factory with the same default administration password. Ensure this default password is changed by the service provider to prevent unauthorized access by someone else who is familiar with Norstar.*

User Programming:
User Programming allows individual users to customize their telephones by changing the features that they use. User Programming does not give the user access to areas that could affect toll fraud incidents.
Recommendation: *None*

In addition to the system programming capabilities, it is possible for a telephone to be Call Forwarded to an external line access code. For example, if the lines are pooled and assigned an access code (for example, 9), a telephone could be call forwarded to "9" and then from off-site the call could be made into that telephone. The caller would hear external dial tone and be able to dial a long distance call.
Recommendation: *Program Restrictions to the telephone lines and provide users COS Passwords that will allow them to make toll calls when in the office. COS Passwords cannot be used off site when calling call forwarded telephones.*
Recommendation: *Program a Line Pool button to the telephone rather than giving out the access code. When the Line Pool button is pressed, the system will automatically grab a free line instead of the access code being manually dialed.*

VOICE MESSAGING
Norstar has different voice messaging products in its portfolio over the years which included Norstar Voice Mail, Flash, and the newest additions to the portfolio CallPilot 100 and CallPilot 150. Norstar Voice Mail and Flash are now manufacture retired but all of these voice messaging products have the same features that will be talked about below as related to toll fraud prevention.
The software of the voice messaging system is provisioned to allow for System Programming and Mailbox User Programming.
System Programming:
System programming of the voice mail system is conducted on site using a two-line Norstar telephone and is accessed using Feature 983. Feature 983 is used to program such things as the Automated Attendant, Custom Call Routing (CCR), and setting up Mailboxes. CCR allows the set up, within the Automated Attendant, of providing callers to be able to dial a single digit (1 to 8) to reach an individual or department. A feature of CCR is External Transfer.

External Transfer from CCR allows the business to set up a CCR point so that when a caller dials a single digit they will be transferred outside the system. The toll fraud possibility with this feature is that a hacker could get into the system and set up a CCR point to access an external line which would then allow them to dial a number.
Recommendation: *Feature 983 is password protected and the passwords can be 4 to 8 digits in length. Choose a password that is not easily broken by hackers eg. don't use 1111. Making the password less intuitive will increase the difficulty of unauthorized persons getting access. After 3 unsuccessful attempts the access will be locked out until corrected by an authorized person using the correct password.*

Mailbox User Programming:
Mailbox owners have specific capabilities to set up their mailboxes based on their preferences on how they want to receive callers when they reach a mailbox. Mailbox owners set their mailboxes up using Feature 981 which is password protected. Users also have the ability to access their mailbox off-site by entering their mailbox number and password. A toll fraud issue could be encountered with a feature known as External Transfer from a Mailbox.

External Transfer form a Mailbox is a feature that allows users to set up an external number so that when a caller is transferred to their mailbox, they can press the digit "7" and be transferred to an external number. If a hacker was able to get access to the mailbox it could be set up to access an external line with no number allowing the hacker to dial any where.
Recommendation: *Mailboxes are password protected and the passwords can be 4 to 8 digits in length. Choose a password that is not easily broken by hackers eg.don't use 1111. Making the password less intuitive will increase the difficulty of unauthorized persons getting access. After 3 unsuccessful attempts the access will be locked out until corrected by an authorized person resetting the password. Resetting the password is done via Feature 983 which is also password protected (see above).*

ADDITIONAL MEASURES
In addition, there are other options available to assist in reducing toll fraud infractions. Within the Norstar system Configuration Programming there is a feature called Restriction Service. Restriction Service can be set up so that toll restrictions to lines and telephone sets will automatically happen after business hours. This will prevent unauthorized personnel that have access to the business after hours and on weekends, from using the telephones to make long distance calls. For example, if business hours are 8:00 a.m until 6:00 p.m Monday to Friday, the Norstar system can be programmed to automatically implement toll restriction on all telephones (or only selected telephones) from 6:00 p.m. to 8:00 a.m Monday to Friday and from 6:00 p.m. Friday until 8:00 a.m Monday. Any employees that work in these off hours can still make long distance calls by entering their COS Password discussed earlier in this document.

If there is suspicion of toll fraud activities, an SMDR (Station Message Detail Recording) unit can be installed on the system. The SMDR can be used to capture all outgoing calls made from the Norstar system.

GENERAL PRACTICES
It is our recommendation that passwords of any kind for the system be changed on a regular basis to keep the integrity of the system secure and that these passwords are kept secure and only made available to the appropriate people. Especially important is ensuring passwords are changed any time someone leaves the company.