Star Telephone Implements FCC Ruling Regarding Customer Proprietary Network Information (CPNI)

If you have had to handle any banking, insurance, or virtually any other personal business by phone or computer, most likely you were asked to provide a "password" or maybe answer a "Verification Question" before you could access your account. Even if you use an ATM machine, you have to provide a Personal Identification Number (PIN) in order to access your account information. Sometimes, we feel we are bombarded by passwords we have to remember.

The Federal Communications Commission has recently passed a ruling to protect you, the customer, and Star Telephone, the service provider. This ruling provides our customers with a sense of security that your personal information that is shared with Star Telephone will not be disclosed to any outside party other than you.

So, the next time you come into or call our business offices you will be asked to provide a password (any word that will be easy for you to remember) and the answer to two predetermined security questions; for example, the name of the school you graduated from, the year you were born, the town you reside in, etc. Once we have your password and security questions documented in our computer system, we are required by the FCC ruling to verify your identity before we can discuss your account with you or make any changes to your account. If you forget your password, you will be asked to provide the answers to your two security questions.

This ruling is to protect you. It would be advisable to not share your password and the answers to the security questions except with those you allow to make changes to your account.

Also, each time a change is made to your account, a courtesy letter will be generated and mailed to your billing address to advise you of recent activity on your account. For more information on Customer Proprietary Network Information (CPNI), please contact our business office at 1-800-706-6538.

Star Communications' Statement of Customer Proprietary Customer Information (CPNI)

♦ Star Communications is prohibited from releasing call detail information during customer-initiated telephone contact except when the customer provides a password.
♦ If the customer does not provide a password, the carrier may release the call detail information by sending it to an address of record or by the carrier calling the customer at the telephone number of record.
♦ Star Communications is also required to provide mandatory password protection for online account access.
♦ Star Communications is permitted to provide CPNI to customers based on in-store contact with a valid photo ID.

♦ Address of record means, whether postal or electronic, the address that the carrier has associated with the customer's account for at least 30 days.
♦ Star Communications can call the customer at the number of record but cannot rely on Caller ID as an authentication method, because pretexters can easily replicate Caller ID numbers.
♦ If a customer is able to provide to the carrier, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and, if applicable, the amount charged for the call), then the carrier is permitted to proceed with its routine customer care procedures.
♦ Under this circumstance, a carrier may not disclose any call detail information about the account other than the call detail information that the customer provides unless the customer first provides a password.
♦ New Customers – Star Communications may request the customer establish a password at the time of service initiation. The carrier must still authenticate the customer at that time.
♦ Existing Customers – Star Communications must first authenticate the customer by calling the customer at the telephone number of record, or a carrier could use a Personal Identification Number (PIN) method of authentication.
♦ Establishment of PIN – a PIN can be used to authenticate the customer. The PIN can be sent to the customer's address of record that the carrier has on file for at least 30 days. The customer can use the PIN to authenticate himself if he cannot remember his password.
♦ For accounts that are password protected, a carrier cannot obtain the customer's password by asking for available biographical information, or account information, to prompt the customer for his password.
♦ Star Communications is required to notify customers immediately when a password, customer response back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.
♦ This may be through carrier-originated voicemail or text message to the telephone number of record or sent to the address of record.
♦ Such notification must not reveal the changed account information.
♦ Notification may not be sent to the new account information.
♦ Star Communications is required to password protect online access to CPNI.
♦ Star Communications is prohibited from relying on readily available biographical information, or account information to authenticate a customer's identity before a customer accesses CPNI online.
♦ A carrier must appropriately authenticate both new and existing customers seeking access to CPNI online.
♦ If a carrier's contract with a business customer is serviced by a dedicated account representative as the primary contact, and specifically addresses the carrier's protection of CPNI, then the authentication rules do not apply to these specific business customers.
♦ A telecommunications carrier shall notify law enforcement of a breach of its customer's CPNI no later than seven business days after a reasonable determination of a breach.
♦ The report will be sent via electronic notification through a central reporting facility to the United States Secret Service and the Federal Bureau of Investigation.

♦ The FCC will maintain a link to the reporting facility at www. fcc.gov/eb/cpni.
♦ A carrier may notify the customer and/or disclose the breach publicly after seven business days following notification to the USSS and the FBI, if the USSS and FBI have not requested that the carrier continue to postpone disclosure.
♦ Star Communications must maintain a record of any discovered breaches, as well as the USSS and FBI responses to the notifications for a period of two years.
♦ The record must include the date the carrier discovered the breach, the date the carrier notified law enforcement, a detailed description of the CPNI that was breached, and the circumstances of the breach.