

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2013 covering the prior calendar year 2012

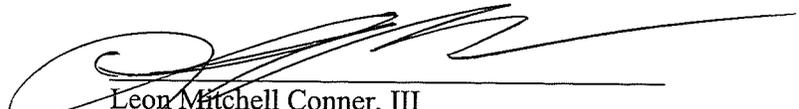
1. Date filed: February 28, 2013
2. Name of entity covered by this certification:
South Georgia Regional Information Technology Authority d/b/a SyncSouth
3. Form 499 Filer ID: 827804
4. Name of signatory: Leon Mitchell Conner, III
5. Title of signatory: Director
6. Certification:

I, Leon Mitchell Conner, III, certify that I am an officer of the South Georgia Regional Information Technology Authority (“SGRITA”) and, acting as an agent of SGRITA, that I have personal knowledge that SGRITA has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Federal Communications Commission’s customer proprietary network information (“CPNI”) rules as set forth in Part 64, Subpart U of the Commission’s rules, 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how SGRITA’s procedures ensure that it is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission’s rules.

SGRITA has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. SGRITA does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission’s CC Docket No. 96-115. SGRITA has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by SGRITA at either the Georgia Public Service Commission, any court, or at the Commission. SGRITA has established procedures to report any breaches to the FBI and United States Secret Service, and it has emphasized in its employee training the need for vigilance in identifying and reporting unusual activity in order to enable SGRITA to continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission’s rules, 47 C.F.R. §-1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject a filer to enforcement actions.


Leon Mitchell Conner, III
Director, South Georgia Regional Information
Technology Authority
Executed February 27, 2013

CPNI Compliance Policies of the South Georgia Regional Information Technology Authority

South Georgia Regional Information Technology Authority d/b/a SyncSouth (“SGRITA”) has implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*

CPNI is “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

SGRITA may use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including to initiate, render, bill and collect for telecommunications services; to protect the rights or property of SGRITA, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

SGRITA does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

SGRITA does not use CPNI to market its services. In the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use would be subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, SGRITA shall modify these policies and conduct additional training as needed to assure compliance with the FCC’s rules.

In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), when SGRITA receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it only uses such information for such purpose, and does not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

SGRITA will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of

possible changes to SGRITA's existing policies that would strengthen protection of CPNI, they should report such information immediately to SGRITA's CPNI Compliance Manager so that SGRITA may evaluate whether existing policies should be supplemented or changed.

At this time, SGRITA only provides interconnected VoIP services to schools. Pursuant to 47 C.F.R. § 64.2010(g), the FCC's authentication requirements for disclosure of CPNI do not apply to such accounts where, as is the case, the customer has a dedicated account representative and a contract with SGRITA that specifically addresses SGRITA's protection of CPNI. Except as permitted by this business customer exemption and SGRITA's contractual relationship with its customers, SGRITA does not disclose CPNI to any inbound telephone caller or any visitor to an SGRITA retail office, and does not provide online access to any account that provides access to CPNI.

When a customer's address of record is created or changed, except when customer initiates service, SGRITA will send a notice immediately to customer's preexisting address of record notifying them of the change. These notifications will not reveal the changed information, and will direct the customer to notify SGRITA if they have any questions.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any SGRITA employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the SGRITA CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is SGRITA's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate SGRITA's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a SGRITA employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to SGRITA's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. SGRITA's CPNI Compliance Manager will determine whether it is appropriate to update SGRITA's CPNI policies or training

materials in light of any new information; the FCC's rules require SGRITA on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the SGRITA CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. SGRITA's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

SGRITA will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided below. (A full business day does not count a business day on which the notice was provided.) If SGRITA receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

SGRITA will delay notification to customers or the public upon request of the FBI or USSS. If the SGRITA Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; SGRITA still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The CPNI Compliance Manager is responsible for assuring that SGRITA maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

SGRITA maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI.

Because SGRITA does not use CPNI for marketing or for any other purpose for which customer approval is required, it does not have any records to keep regarding supervisory review of marketing; or of sales and marketing campaigns that use CPNI; or of records associated with customers' "opt-out" approval or non-approval to use CPNI, or notification to customers prior to any solicitation for customer approval to use or disclose CPNI.

SGRITA will maintain a record of any customer complaints related to their handling of CPNI, and records of SGRITA's handling of such complaints, for at least two years. The CPNI

Compliance Manager will assure that all complaints are reviewed and that SGRITA considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

SGRITA will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that SGRITA has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how SGRITA's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

Employees with access to CPNI receive a summary of SGRITA's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, SGRITA requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.