ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) PROCEDURE

EB DOCKET 06-36

ACN Communication Services, LLC and ACN Communication Services Virginia, LLC and ACN Digital Phone Service Puerto Rico, LLC and Flash Wireless, LLC

Exhibit A

STATEMENT OF CPNI PROCEDURES AND COMPLIANCE (CY 2017)

ACN Communication Services, LLC, ACN Communication Services Virginia, LLC, its Virginia operating subsidiary, ACN Digital Phone Service Puerto Rico, LLC and Flash Wireless, LLC (collectively known as "the ACN Companies" or "Companies") provide the following as their Statement of CPNI compliance.

ACN Communication Services, LLC and ACN Communication Services Virginia, LLC provide wireline local and long distance telecommunication services to business and residential customers, primarily as bundled services. ACN Communication Services, LLC, along with ACN Digital Phone Service Puerto Rico, LLC, also provides Voice over Internet Protocol ("VoIP") services and customer premises equipment to business and residential customers. Flash Wireless, LLC provides wireless telecommunications services. All of the ACN Companies have the same methods and procedures and operating policies with respect to CPNI, including customer call detail records.

The ACN Companies do not use CPNI to market services to their customers. Therefore, the ACN Companies do not utilize the opt-in or opt-out approval processes. Should the Companies elect to use CPNI in future marketing efforts, they will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

The ACN Companies bill customers directly and have taken steps to secure CPNI and manage its release in accordance with FCC rules. The ACN Companies have instituted processes to safeguard customer CPNI and call detail information from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to CPNI. Customer Service Agents are trained on how to authenticate customers when hired and continually coached on safeguarding customer CPNI.

User account information can only be accessed by authorized representatives of the ACN Companies. Such authorized representatives have access to customer records management systems only via an established password protected account setup in their name by a system administrator. When the ACN Companies' agents take action on a customer's account (e.g. make package changes, billing changes, wrap codes, create cases, etc.) an audit log is created on the account with respect to the actions the agent took on the customer's account. Additionally, access to CPNI used for the purpose of reporting and managing the business is centralized to individuals who have limited password access to customer information through the establishment of a Business Objects database that is populated only with specified customer information.

Call detail information is provided to customers over the telephone pursuant to the procedures identified below.
Customers define an account User Name and Password at the time the customer account is established. In addition, each Customer must select a secret question and answer upon establishment of an account. Should a customer forget or lose the password, such information can be provided to the customer at the email address established when the account was set up.

If the customer cannot provide the password or backup authentication question response, and the customer question does not fall into the exception where the call detail information is provided by the customer to the Customer Service Representative, then call detail can only be provided by mail to the customer's physical or electronic address of record or by calling the customer at the telephone number of record.

The ACN Companies maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI.

The ACN Companies protect against the unauthorized disclosure of CPNI on the Internet through the establishment of a customer username and password. In addition, each Customer must select a secret question and answer upon establishment of an account. Should a customer forget or lose the password, such information can be provided to the customer at the email address established when the account was set up. If the customer cannot provide the password or backup authentication question response then the customer can contact customer service. Upon the customer's contact with the ACN Companies' customer service department regarding a forgotten password or user name, the customer must provide their email address of record prior to the customer service representative emailing the customer their username and password.

The ACN Companies do not have retail locations and therefore do not disclose CPNI in-store.

The ACN Companies notify customers via a previously established email address, telephone call or mail to the customer address of record, all notifications regarding account changes.

The ACN Companies have not taken any actions against data brokers in the last year.

The ACN Companies have procedures in place to notify law enforcement (United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI)) of a breach of a customer's CPNI within seven (7) business days, and to notify customers of the breach. The ACN Companies maintain a record of any breaches discovered and notifications made to the USSS and FBI. The customer's electronic record is updated with information regarding notifications on CPNI breaches.

The ACN Companies have not received any complaints about unauthorized release or disclosure of CPNI for the last calendar year.

The ACN Companies have not developed any information with respect to the processes that pretexters are using to attempt to access CPNI.