2018 Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Attachment 1: Statement Concerning Company Procedures

Super Prepaid, Inc. ("Super Prepaid") does not use CPNI for marketing purposes. Super Prepaid sells prepaid telecommunications products over the Internet.

During 2018, Super Prepaid had in place the following mechanisms to ensure that CPNI, including customer call detail information, was safeguarded.

For its products for which it maintained call detail records, all employee access was password protected, and was restricted to specific hours set by company management. Every login session is also recorded to track the activities of each representative. All customer access to those call detail records was password protected. A customer could only gain access to his or her call detail records and other CPNI by providing his or her password, either online or by telephone in a customer-initiated call with a Super Prepaid customer service representative. The customer was required to set the password at the time that the customer established his or her account online with Super Prepaid, and purchased his or her prepaid products, which required use of a credit card. At the time the account was established, the customer must also provide an email address of record, in addition to providing the necessary credit card information (name, card number, billing address). Thus, the customer was necessarily authenticated at the time the password is established. The password was chosen by the customer, and was not prompted by any questions or prompts relating to readily-available biographical information or account information.

In addition, it was Super Prepaid's regular practice to call and speak to the customer on a landline telephone after the customer established an account for the first time. The customer service representative making the call would ask to verify the cross street near the credit card billing address. Super Prepaid also checks the phone number to see if it is located at the billing address, including consulting white pages listings.

In the event that the customer had lost or forgotten his or her password, the customer was permitted to reset the password by requesting a verification code, which is emailed to their current email address by verifying the email address and the billing ZIP code on file. After the customer receives the verification code, they are able to reset the password online. The verification code is null after the password has been reset.

A customer was only permitted to change his or her password, email address, or other account information on-line. When a customer made any change to his or her account information, including creating a new password, changing the email address, or changing billing information, Super Prepaid automatically sent an email notification of the change to the customer's email address of record. In the event of a change of email address, this notification was sent both to the customer's prior email address and the new email address.

Super Prepaid also encrypts all of its call detail records and account information, to protect against access by hackers.

All of Super Prepaid staff was instructed that they are not to give out call detail information or passwords, except in accordance with the procedures described above. Employees are subject to discipline, including termination, for violations of these policies.

Super Prepaid's operating procedures require notification of relevant law enforcement agencies and customers in accordance with Federal Communications Commission rules in the event of a breach of CPNI. Super Prepaid maintains records of any breaches discovered, notifications made to law enforcement, and notifications made to customers. These records include, where 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. Super Prepaid maintains these records for 2 years.