South Carolina
DEPARTMENT OF CONSUMER AFFAIRS
293 GREYSTONE BOULEVARD, STE. 400
P. O. BOX 5757
COLUMBIA, SC 29250-5757

Carri Grube Lybarker
Administrator/
Consumer Advocate

PROTECTING CONSUMERS SINCE 1975

August 3, 2020

Commissioner Comer H. Randall
Public Service Commission
101 Executive Center Drive, Suite 100
Columbia, SC 29210

RE: Proposed Regulation 103-823.2: Protection of Customer Data
Docket No. 2019-387-A

Dear Commissioner Randall:

The South Carolina Department of Consumer Affairs ("SCDCA"/"Department") is pleased to offer comments in response to the Public Service Commission's ("PSC"/"Commission") promulgation of a regulation to protect public utility customer data. SCDCA is the state's consumer protection agency. Established in 1974, SCDCA is responsible for the administration and enforcement of over 120 state and federal laws. The agency's jurisdiction includes several South Carolina Identity Theft Protection statutes[1] and the federal Gramm-Leach-Bliley Act which, among other things, provides a framework for regulating the privacy practices of a broad range of financial institutions. SCDCA helps formulate and modify consumer laws, policies, and regulations; regulates the consumer credit marketplace; resolves complaints arising out of the production, promotion, or sale of consumer goods or services, whether or not credit is involved; and promotes a healthy competitive business climate with mutual confidence between buyers and sellers.

Background: Existing South Carolina Privacy Laws

To aid in combating identity theft, the South Carolina General Assembly passed the Financial Identity Fraud and Identity Theft Protection Act (the "Act"), which largely became effective in 2008[2]. In addition to making identity theft a crime, the Act also provides for security freezes, sets parameters for the collection, disclosure and use of social security numbers by

[1] *See* S.C. Code Ann. § 37-1-101 et seq.; Act. No. 190, *available at* https://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm.
[2] *See* Act. No. 190, *available at* https://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm.

businesses and state agencies, puts forth requirements for disposing of items containing personal identifying information and provides a framework for security breach notifications.[3] All portions of the law, except the provisions regarding security breaches, became effective on December 31, 2008. The security breach provisions became effective on July 1, 2009.

In the eleven years since the reporting requirements came into effect, the Department has received over 400 breach notices affecting over 10.1 million South Carolina consumers. Most breaches exposed the type of data included in the proposed regulation's definition of "customer data." Nearly 50 percent of the breaches involve the improper or unauthorized disclosure of personal data, including names, addresses, driver's license numbers and/or social security numbers. Twelve percent of breaches involved the disclosure of credential data, such as personal email addresses, non-banking account numbers, usernames and/or passwords.

SCDCA commends the PSC for its work to establish standards and transparency in the rapidly evolving landscape of technology and information security. We provide the following comments based on our experience in hopes of assisting the Commission's goals of providing covered utilities with guidance on protecting customer data and improving accountability.

Section (A)(3): Definition of "Customer Data"

A. Reference to "personal identifying information"

Section (A)(3) of the proposed regulation provides a definition of "customer data" which references "personal identifying information." "Personal identifying information" is a phrase currently defined in two South Carolina laws specifically pertaining to privacy and are cross-referenced in additional statutes.

Section 39-1-90 delineates parameters a business must comply with when a security breach affecting South Carolina residents occurs. The law applies to "person[s] conducting business in [South Carolina], and owning or licensing computerized data or other data that includes [PII]. . . ."[4] "Personal identifying information" is defined in Section 39-1-90(D)(3) as:

> The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted:
>
> (a) social security number;
>
> (b) driver's license number or state identification card number issued instead of a driver's license;

[3] *See supra*, Note 2.
[4] S.C. Code Ann. § 39-1-90(A).

(c) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or

(d) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

An alternate definition of "personal identifying information" is found in Section 16-13-510(D). This definition is broader than that of Section 39-1-90(A)(3) listing items such as social security numbers, driver's license numbers, and checking account numbers without the requirement that they be revealed in conjunction with part of a person's name to trigger the statute. The Title 16 definition also adds additional categories, including digital signatures and dates of birth, and clarifies that the itemized listing is not exhaustive. This definition is cross-referenced by several statutes, including Chapter 20 of Title 37 entitled "Consumer Identity Theft Protection."

We would caution the use of the phrase "personal identifying information" within the definition of "customer data" unless it is the intent of the Commission to include the items delineated within both or either of the definitions discussed above. Further, we would recommend referencing the section(s) specifically to alleviate any confusion. If neither of the definitions were meant to be incorporated, we would recommend changing the phrase "personal identifying information" therein.

B. Reference to "customer data"

As currently written, the proposed regulation seemingly does not protect consumers who are not current customers of a public utility. Subsection (A)(3) partially defines *customer data* as "data about a customer's electric, natural gas, water, or wastewater usage; information that is obtained as part of an advanced metering infrastructure; and [PII] in the possession of the electric, natural gas, water or wastewater public utilities, including the name, account number, billing history, address of the customer, email address, telephone number, and fax number." "Customer" is not defined therein. Regulation 103-302(3), however, provides the most generally applicable definition of *customer* as "[a]ny person, firm, association, establishment, partnership, or corporation, or any agency of the Federal, State or local government, *being supplied* with electric service by an electrical utility under the jurisdiction of [the PSC]." S.C. Code Ann. Regs. 103-302(3) (2008) (emphasis added). The language used seems to indicate an ongoing and continuous relationship.

Reading both regulations together could render an interpretation that only a person currently receiving service is a customer, leaving vulnerable the data of former customers. We encourage a clarification that a former customer's data remaining in possession of the utility is customer data and cannot be disclosed without consent of the former customer.

Sections (C)–(F): Sharing of Customer Data with Third Parties

Sections (C)–(F) provide various details regarding the sharing of customer data with third parties. In recognition of the ability for a utility to share information with third parties in certain specific circumstances, whether with or without customer consent, we recommend a due diligence requirement be placed on the utility when choosing the third party with whom it will share data. Parameters should include:

1. Conducting thorough due diligence to verify that the third party understands and is capable of complying with privacy laws prior to contracting with the party and establishing ongoing monitoring to determine compliance during the contract term;
2. Requesting and reviewing the third party's policies, procedures, internal controls, and training materials to ensure that the third party conducts appropriate training and oversight of employees;
3. Including in the contract with the third party clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities, including failing to properly protect customer data; and
4. Taking prompt action to address any problems identified through the monitoring process or that is otherwise brought to the utility's attention, including terminating the relationship when appropriate.

Section (H)(2)(a): Notice to Customers

The proposed regulation appears to be modeled after the Gramm-Leach-Bliley Act's (GLBA) Privacy Rule. Title V, Subtitle A of the GLBA[5] and Regulation P, which implements the GLBA, mandate that financial institutions provide customers disclosures regarding the financial institution's data sharing policies and practices at the beginning of establishing the customer relationship and then at least once per year thereafter. The GLBA provides an exception under which financial institutions that meet certain conditions are not required to provide annual privacy notices to customers. Section 503(f)(1) requires that to qualify for this exception, a financial institution must not share nonpublic personal information about customers except as described in certain statutory exceptions. In addition, Section 503(f)(2) requires that the financial institution must not have changed its policies and practices regarding disclosure of nonpublic personal information from that contained in the most recent privacy notice it sent to customers.

The PSC proposed regulation calls for utilities to file guidelines with the Commission which must include the procedures for notifying consumers of the utility's privacy policies. To further consumer knowledge, the Department encourages the PSC to require both an initial and an annual notice requirement to customers. Exceptions—similar to those for financial institutions under the GLBA—could be considered to alleviate unnecessary disclosures.

[5] 15 U.S.C. §§ 6801 through 6809.

Conclusion

SCDCA appreciates the opportunity to comment on this important regulation as it is our belief that for consumers to have the confidence they need to participate fully in the marketplace, consumers must have choices about how the information collected from them is used. We unfortunately have seen the ramifications of the misuse of customer data, including in misleading or deceptive advertising targeting certain customers for products not needed or leveraging the business relationship the consumer has with one party. Further, when information falls in the wrong hands, it can be used for scam attempts, separating consumers from their money or personal information.

SCDCA appreciates the needed balance between industry burden and consumer protection in the ever-evolving data privacy environment. We hope the information provided assists with this exercise. Should you have any questions pertaining to our comments, please feel free to contact us at 803-734-4233.

Best Regards,

Kelly Rainsford, CIPP/US
Deputy Administrator/ General Counsel

Carri Grube Lybarker, Esq.
Administrator/ Consumer Advocate

cc: All parties of record