The State of South Carolina
Department of Consumer Affairs

293 GREYSTONE BOULEVARD, STE 400
PO BOX 5757
COLUMBIA, SC 29250-5757

Carri Grube Lybarker
Administrator/
Consumer Advocate

Celebrating Over 40 Years of Public Service

May 5, 2021

Via Electronic Submission
Federal Communications Commission
Office of the Secretary
GN Docket No 21-79
45 L Street NE
Washington, DC 20554

RE: Implementing the Privacy Act of 1974
GN Docket No 21-79

Dear Secretary Dortch:

The South Carolina Department of Consumer Affairs ("SCDCA"/"Department") is pleased to offer comments in response to the Federal Communications Commission's ("FCC"/"Commission") proposed rule implementing the Privacy Act of 1974. 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 state and federal privacy laws such as the South Carolina Financial Identity Fraud and Identity Theft Protection Act[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.

In its regulation of the consumer credit marketplace, SCDCA helps formulate and modify consumer laws, policies, and regulations; resolves complaints arising out of the production, promotion, or sale of consumer goods or services in South Carolina, whether or not credit is involved; and promotes a healthy competitive business climate with mutual confidence between buyers and sellers.

Background: South Carolina Privacy Laws and Related Data

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* 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 10.4 million South Carolina consumers, with over 4 million of those consumers, or almost 40%, having been affected by a breach of government data.[4] The government category is by far the highest with regard to percentage of total consumers affected. The financial industry category has the next highest percentage of consumers affected, with 29%. Nearly 50 percent of breaches reported to the Department involve the improper or unauthorized disclosure of personal data, including names, addresses, driver's license numbers and/or social security numbers.

In October 2013, SCDCA launched its Identity Theft Unit ("the Unit"/"IDTU"), which provides tailored remediation and guidance to identity theft victims. The Unit also takes scam reports, allowing the Department to track trends in the marketplace. From 2013 to 2020, the Department received 2,455 reports from South Carolina residents who were affected by identity theft, and nearly 13,000 reports of residents affected by scams. Of the 2,455 consumers that reported identity theft, 15% involved theft of government benefits.

SCDCA commends the FCC for its work to amend the Privacy Act regulations to promote privacy safeguards and better align its rules with the evolving developments in the law and the directives from governmental bodies. We provide the following comments based on our experience in processing security breach notices and scam reports and assisting South Carolina consumers in mitigating identity theft events in hopes of assisting the Commission with this effort.

Topic Discussion

Amendments to § 0.554: Requests for Notification of and Access to Records

The Commission proposes several changes to its Privacy Act rules pertaining to the process individuals should follow to determine whether the Commission is holding information about them in its systems of records. Of note, the Commission proposes to modify how an individual may verify their identity when requesting access to records and is requesting comment on whether relying on a notarized form rather than the provision of two forms of identification would increase the risk of fraudulent requests.

As stated above, scammers often obtain personal identifying information via security breaches. Such information could in turn be utilized to complete an identity statement and obtain

[3] *See supra*, Note 2.

[4] Not all companies affected by breaches are able to identify exactly how many consumers were affected, even after a thorough, professional investigation. Because of that, the true number of affected consumers is likely much higher. For the government category, totals provided reflect the minimum number of South Carolina residents potentially affected as one report did not include a specific number of consumers affected.

additional information from the FCC. While we appreciate the concern of collecting additional personal information from an individual seeking records, and believe notarization provides an additional safeguard to ensuring the appropriate person is making the request, the Department encourages the FCC to weigh the burdens and benefits of current and proposed methods.

Two forms of identification are readily accessible by many consumers. A notary, however, is not something many consumers are accustomed to having to locate. As such, solely providing a request process where a notarized form must be used may increase the consumer burden of requesting their information. A hybrid approach that combines existing and proposed practices could increase safeguards without increasing consumer burden. Under a such an approach, the Commission could require the consumer either provide two forms of identification, *or* they may sign the identity statement which would require notarization. To further reduce fraudulent requests using the notarized identity statement, the Privacy Analyst could verify the authenticity of the notary signature with the appropriate state agency, and the identity statement could require selection of the method used by the notary to authenticate the requester's identity. This would serve to prevent scammers from either circumventing the Commission's safeguards by submitting a fraudulently notarized identity statement or using personal identifying information they already have to obtain more information from the Commission's databases. Offering options for individuals to either submit the two forms of identification or a notarized form would also likely reduce the amount of additional data collected as some will choose the latter.

Amendment to § 0.556: Request to Correct or Amend Records

The Commission proposes to amend § 0.556 of its rules to clarify the requester's procedural rights when a request to amend a record is denied. The Department believes having a clear, streamlined process that precisely informs the requester of their rights when a request to amend a record is denied is an important part of creating consumer awareness. It would also serve to ensure the FCC maintains accurate data.

Due to the prevalence of security breaches and identity theft, the integrity of data is often compromised. One area the Department often sees this play out is in credit reporting. Since 2013, over 25% of South Carolina consumers reporting identity theft discovered they were a victim based off the information in their credit report. The Department advises these consumers to follow the process laid out in the Fair Credit Reporting Act ("FCRA"), [5] which sets out a clear process to address account-related identity theft and "block" the fraudulent transactions from their credit report. While it was certainly not drafted to apply to the operations of a federal agency, the process delineated in the FCRA may provide a framework or otherwise be helpful as the FCC grapples with implementing appropriate guardrails in its efforts to protect the release and integrity of the data it maintains.

Relaying the steps to take upon a denial may encourage an individual to pursue an appeal should they believe the data held by the FCC is inaccurate. This would serve to give the FCC a second look and potentially correct any prior errors in its review of the record. A convoluted,

[5] See 15 U.S.C. § 1681c-2, *Block of Information Resulting from Identity Theft*

unclear process would seemingly serve to do the opposite and discourage a consumer from moving forward with an appeal and result in incorrect data remaining on the books.

Conclusion

SCDCA appreciates the opportunity to comment on this important proposal. It is our belief that for consumers to have the confidence government, there must be safeguards surrounding the disclosure of their data and corresponding amendments thereto. Unfortunately, we have seen the ramifications of the misuse of customer data, especially when information falls into the wrong hands, and appreciate any efforts to prevent such an occurrence.

We hope the information provided is helpful. Should you have any questions pertaining to our comments, please feel free to contact me at 803-734-4233.

Best Regards,

Carri Grube Lybarker, Esq.