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

February 4, 2021

*Via Electronic Mail Submission (*2020-ANPR-1033@cfpb.gov*)*

Comment Intake—Section 1033 ANPR
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

RE: Docket No. CFPB-2020-0034– Consumer Access to Financial Records

Dear Acting Director Uejio:

The South Carolina Department of Consumer Affairs ("SCDCA"/"Department") is pleased to offer comments in response to the Bureau of Consumer Financial Protection's ("CFPB"/"Bureau") advance notice of proposed rulemaking to implement section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"). 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.

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. Overall, SCDCA protects consumers while giving due regard to those businesses acting in a fair and honest manner.

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

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 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[4]. 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. Of the seven industry categories recognized by the Department (Education, Financial, Government, Health, Hospitality, Retail, and Other), the financial industry has the third highest number of breaches reported (after Retail and Other) and the second highest number of consumers affected (after Government).

From 2012-2020, at least 3,028,248 South Carolinians have been affected by a breach of companies in the financial industry. Financial data (credit/debit card numbers, income, financial transactions, bank statements, etc.) was compromised in 25% of the breaches reported in 2020 and 32% of the breaches reported from 2012-2020.

SCDCA supports the Bureau's efforts to effectively and efficiently implement the financial record access rights described in Section 1033 while working to establish standards in the rapidly evolving landscape of technology and information security. We offer the following comments for the Bureau's consideration based upon SCDCA's research and experience as a consumer credit regulator, mediating consumer complaints and assisting consumers with mitigating identity theft events.

Topic Discussion

Section E. Consumer Control and Privacy - *Question 26: In what respects do consumers understand the actual movement, use, storage, and persistence of authorized data? To what extent do such movement, use, storage, and persistence of authorized data align with reasonable*

[2] *See* Act. No. 190, *available at* https://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm.
[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.

consumer expectations or preferences, including privacy expectations or preferences? What should the Bureau do, if anything, to improve consumer understanding or to effect closer alignment between practice and consumer expectations or preferences? Should the Bureau consider placing any restrictions on the movement, use, storage and persistence of authorized data, and if so, what restrictions and why?

As discussed above, SCDCA is the state agency in South Carolina designated as the agency to receive security breach information form businesses and to assist security breach and identity theft victims with mitigating breach/ theft events. A recurring theme amongst some financial industry security breach victims is one of confusion when a notice is received. The business providing the notice is often not the one with which the consumer had the primary transaction, but rather a third-party contractor thereof. Due to the lack of name recognition, consumers often think the notice is a scam attempt or otherwise not legitimate.

To improve consumer understanding, SCDCA recommends a required disclosure regarding the company's authorized data maintenance and sharing policies and practices at the beginning of establishing the customer relationship, at least once per year thereafter and upon any change. It should cover the movement, use, storage and persistence of the authorized data. The language/ requirement of a similar disclosure contained in the Gramm-Leach-Bliley Act[5] and accompanying Privacy Rule could serve as a model or starting point. A comprehensive and succinct disclosure would ideally provide consumers with the big picture, enabling them to fully understand the potential journey of their data and options to prevent misuse or unauthorized disclosure.

Regarding restrictions, requirements similar to those of the Fair Credit Reporting Act (FCRA)[6] could be helpful to create standards for restrictions on authorized data, including the purpose for which it is permitted to be used and methods of records disposal. SCDCA also believes a requirement for data to be destroyed once the permissible use is exhausted, could enhance information security. Several breaches reported to the Department, including a large state agency breach, involved "resting" data. That is, data that was stored but not actively in use. Such a measure could help to reduce opportunities for unauthorized access.

Section F. Legal Requirements Other Than Section 1033 – *Question 33: How, if at all, are data holders subject to laws or regulations (whether Federal, State, or foreign) that may be in tension with any proposed obligation to make consumer data accessible per section 1033? How, if at all, should the Bureau address such potential tension?*

[5] 15 U.S.C. 6801 through 6809.
[6] 15 U.S.C. §1681, et seq.

Data holders may be subject to the specific federal laws mentioned previously, Gramm-Leach-Bliley Act[7] and FCRA[8], as well as state privacy and identity theft protection statutes. While we do not interpret the federal laws, SCDCA's perspective is that both would seemingly apply to most if not all of data holders. We would recommend one set of standards for all data holders to comply with to reduce regulatory burden and provide a level playing field for industries. While a nod could be given, or sample language or direction found from, the federal laws, enhancements or additions are likely warranted.

Section G. Data Security – *Question 38. How effectively does existing law that bears on data security mitigate data security risks associated with data access and, in particular, authorized data access? What steps, if any, should the Bureau take to improve the effectiveness of existing laws that bear on data security in the context of data access?*

Several federal laws, including the Gramm-Leach-Bliley Act (GLBA)[9], complement South Carolina's identity theft protection laws. While both set privacy and security standards for safekeeping consumer data, the Safeguards Rule fills in gaps contained in South Carolina's laws and vice versa.

Current South Carolina law does not address or otherwise require a business create and implement an incident response plan. As such, the Department, in addition to having similar security standards as required by the GLBA, is in favor of providing additional clarification for businesses in this area of privacy and security standards for safekeeping consumer data at the federal level. With the pervasiveness of security breaches and timing being of the essence when responding or otherwise attempting to mitigate any of its affects, it is the Department's opinion that explicitly requiring a written incident response plan is vital to an effective information security plan.

We further encourage the Bureau to require that internal processes for responding to a security event include promptly notifying the senior personnel responsible for overseeing information security. Such a requirement would allow a timelier mitigation effort and quicker consumer notification.

SCDCA also recommends a due diligence requirement be placed on the business when choosing a third party with whom it will share data. Parameters should include:

---

[7] 15 U.S.C. 6801 through 6809.
[8] 15 U.S.C. §1681, et seq.
[9] Public Law 106-102, 113 Stat. 1338 (1999); Several of South Carolina's identity theft protection statutes exempting institutions that are both subject to and ***in compliance with*** the privacy and security provisions of the Gramm-Leach Bliley Act. *See* Act. No. 190, *available at* https://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm

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.

Conclusion

SCDCA appreciates the opportunity to comment on this important topic 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,

Carri Grube Lybarker, Esq.