South Carolina
DEPARTMENT OF CONSUMER AFFAIRS
293 Greystone Boulevard Suite 400
P. O. BOX 5757
COLUMBIA, SC 29250-5757

Carri Grube Lybarker
Administrator/
Consumer Advocate

PROTECTING CONSUMERS SINCE 1975

November 21, 2022

Via Electronic Submission
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B)
Washington, DC 20580

RE: Commercial Surveillance ANPR, R111004

Dear Secretary Christie:

The South Carolina Department of Consumer Affairs ("SCDCA"/"Department") is pleased to offer comments in response to the Federal Trade Commission's ("FTC"/"Commission") request for comments on the prevalence of commercial surveillance and data security practices that harm consumers. 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.

SCDCA commends the FTC 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 implementation of new trade regulation rules or other regulatory alternatives to regulate the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.

[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.

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 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. The law is unique from some of the more general, federal privacy laws the agency deals with on a daily basis as the Act applies universally to persons conducting business with South Carolina residents.

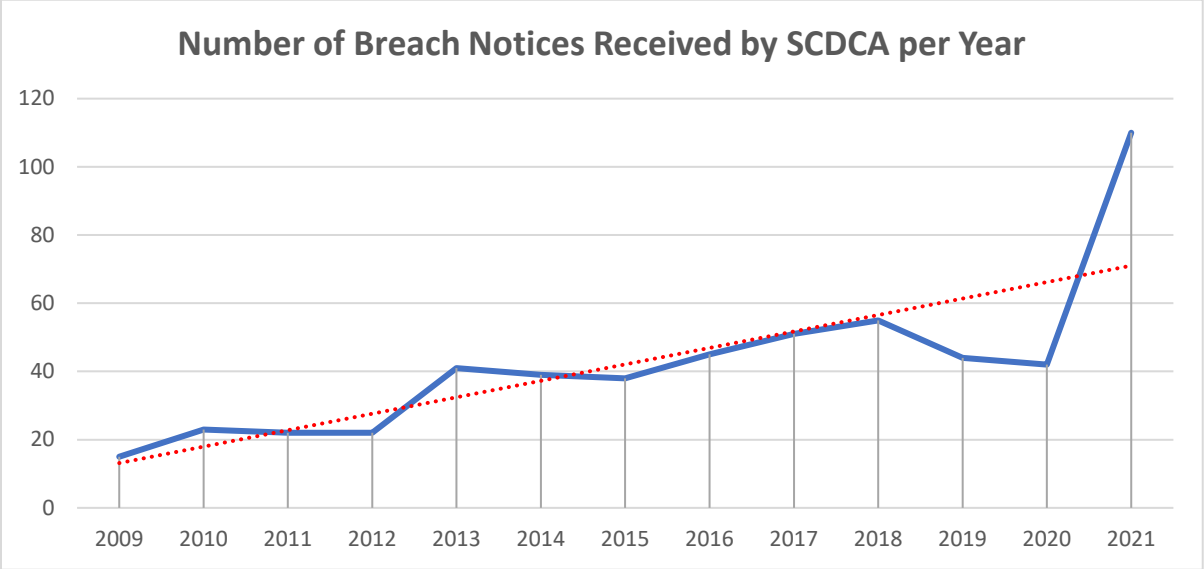
Question 10: What kinds of data should be subject to a potential trade regulation rule?

In the thirteen years since the Act's reporting requirements came into effect, the Department has received over 550 breach notices affecting almost 13 million South Carolina residents, which is almost three times the state's population. Most breaches exposed the type of "consumer data" for which the Commission is considering implementing new trade regulation rules or other regulatory alternatives:

- 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.
- Over 30 percent involve the disclosure of financial data, including credit/debit card numbers, income, financial transactions, bank statements, etc.
- Ten percent of breaches involved the disclosure of credential data, such as personal email addresses, non-banking account numbers, usernames and/or passwords.
- Eight percent involve the disclosure of protected health data, such as diagnoses, treatment info, test results, etc.

The Department has seen a rising trend in the number of security breach notifications in the recent years as shown in the below chart.

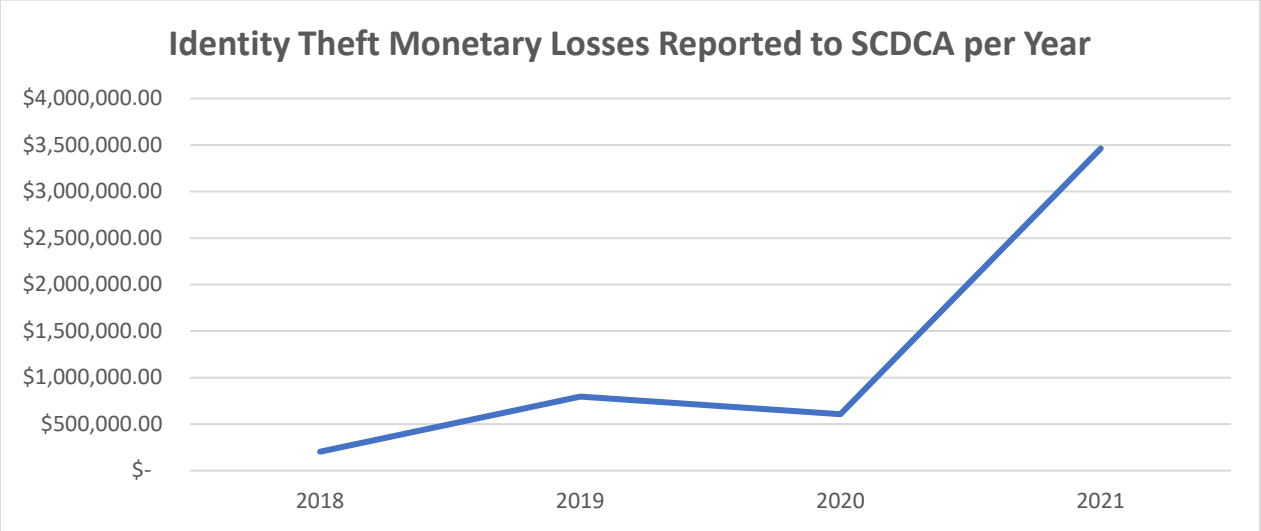
[2] Act. No. 190, *available at* https://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm.
[3] *See supra,* Note 2.



SCDCA also collects Identity Theft Data from South Carolina identity theft victims. Since 2018, the Department has received 1,842 reports of identity theft. Of those:

- 1,317 are categorized as financial identity theft, which includes the misuse of existing ATM/debit/credit cards or checks/checking accounts, or opening new credit cards, loans, or utility accounts using someone else's identifying information.
- Fifty percent of security breaches include personal information needed to open a financial account, and thirty percent of security breaches include financial data needed to use an existing account.

The identity theft incidents reported from 2018-2021 resulted in over $5 million in monetary losses as shown in the chart below.



When read in conjunction with the security breach data on file, 80% of the data breached was the same type of information used by identity thieves in 70% of identity theft reports received by SCDCA. As such, the Department recommends the FTC trade regulation rule include measures to at least adequately protect these types of data.

Question 76: To what extend should new trade regulation rules prohibit certain specific commercial surveillance practices, irrespective of whether consumers consent to them?

In recognition of the value of the information a company may share with third parties, whether with or without customer consent, SCDCA recommends a due diligence requirement be placed on the company when choosing the third party with whom it will share data. Parameters could 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 company's attention, including terminating the relationship when appropriate.

Question 90: Should new rules, if promulgated, require plain-spoken explanations? To what extent, if at all, should new rules detail such requirements?

The Department is in favor of disclosures regarding a company's commercial surveillance practices and the ability for a consumer to opt out of certain practices. To improve readability and prevent overlooking these important terms and conditions, the Department recommends the following:

- Require all fonts be a minimum of 12 point.
- Make headings distinct by increasing font size and/or the use of bold font. Limit the use of bold font below the headings to only items of high importance.

- Provide a simple summary of the proposed use of the consumers' data so the disclosure can be more easily understood by consumers. Recognizing that some business may have numerous uses of the data, we suggest including a link directly to the listing of all possible uses rather than including all of them in the Notice.

- Ensure that language in the terms are shortened, combined, or worded in order to avoid repetitive information and lower the Flesch-Kincaid Grade Level to a maximum 8.0. The consent and permission terms should be shortened to a maximum one page (front and back) printed to preserve consumers' ability to retain this important information and to keep costs down.

Conclusion

We commend the Commission for the work and effort put into this process and appreciate the opportunity to comment. Should you have any questions pertaining to our comments, please feel free to contact me at 803-734-4240.

Regards,

Roger Hall, Esq.
Deputy Consumer Advocate