BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

THIRUVENDRAN VIGNARAJAH
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

July 7, 2015

The Honorable Barbara Mikulski
United States Senate
503 Hart Senate Office Building
Washington, D.C. 20510-2003

Dear Senator Milkulski:

I write to express my concern regarding recent efforts in Congress to pass a national law on data breach notification and data security that would preempt Maryland law.[1] As Maryland Attorney General, I have seen first-hand the harm that data breaches and identity theft cause consumers. I support additional focus on these issues in Congress. A strong, national law on data breach notification and a larger role for the federal government in data security will help better protect consumers. However, greater federal protection should not come at the expense of the important role states already play protecting consumers from data breaches and identity theft.

In the past ten years, nearly 5,000 data breaches have compromised more than 815 million records nationwide.[2] These records contain sensitive financial information, Social Security numbers and medical records, and the breaches expose consumers to identity theft. One study found that the breach of a Social Security number increases a consumer's risk of identity theft by 18 times.[3]

Identity theft has been the largest category of consumer complaints received by the Federal Trade Commission for fifteen consecutive years.[4] In 2013, fraud related to credit, debit

[1] There are eight bills currently pending before Congress relating to data security and data breach notification: S. 177 – Data Security and Breach Notification Act of 2015; S. 961 – Data Security Act; S. 1027 – Data Breach Notification and Punishing Cyber Criminals Act of 2015; S. 1158 – Consumer Privacy Protection Act of 2015; H.R. 580 – Data Accountability and Trust Act; H.R. 1704 – Personal Data Notification and Protection Act of 2015; H.R. 1770 – Data Security and Breach Notification Act of 2015; and H.R. 2205 – Data Security Act of 2015.
[2] Privacy Rights Clearinghouse, "Chronology of Data Breaches," accessed March 13, 2015.
[3] National Consumers League, "The Consumer Data Insecurity Report: Examining the Data Breach – Identity Fraud Paradigm in Four Major Metropolitan Areas," p. 14, June 2014.
[4] Federal Trade Commission, "Press Release: Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014," Feb. 27, 2015.

or gift cards resulted in $11 billion in losses.[5] Full-blown identity theft involving the use of a Social Security number can cost a consumer $5,100 on average.[6]

The Maryland Office of the Attorney General Identity Theft Unit regularly receives complaints from consumers who have been victims of identity theft. My office helps consumers remove fraudulent charges from their financial accounts and repair bad credit caused by identify theft. We have also worked hard to ensure data collectors take steps necessary to protect consumers' information.

Maryland law, like that of many other states, requires a business to take reasonable steps to protect sensitive consumer data. *See* Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501 through 14-3508 (2013 Repl. Vol.). We need to be vigilant to deter negligence and error, which research shows are the primary causes of data and security breach incidents.

It important to note that not all data breaches are the result of third-party hacks. According to Experian, the nation's largest credit reporting agency, "[e]mployees and negligence are the leading cause of security incidents."[7] Similarly, a 2013 Ponemon Institute study found that "[e]mployee or contractor negligence and system error or malfunctions are the two primary types of data and security breach incidents experienced by organizations," whereas "[m]alicious insiders and external attacks (exfiltration) are less prevalent."[8]

To ensure that businesses act reasonably when they collect, maintain and use consumers' data, my office has regularly investigated the causes of data breaches and has taken action against businesses that have failed to adequately protect the sensitive data entrusted to them by consumers. In recent years, my office has taken action against a finance company that disposed of thousands of consumers' applications for financing by throwing them in a dumpster. We have taken similar actions against a regional retailer, a national pharmacy chain, and a Maryland physician's office, each of which improperly disposed of sensitive credit and medical records, thereby placing consumers at risk. Currently, we are investigating significant data breaches involving consumers' Social Security numbers, medical records, insurance records and other private information. This consumer data was taken by hackers when the businesses failed to comply with their own security policies, ignored security warnings, neglected to apply critical patches, and failed to take other necessary measures to safeguard consumers' information. The weaknesses generated by companies' poor security practices are inevitably exploited by cybercriminals, putting consumers' personal information at risk.

Our constituents want more protection of their personal information, not less. Preempting state law would make consumers less protected than they are right now. Placing enforcement authority and regulatory authority entirely with the federal government would

---

[5] Javelin Strategy & Research, "2014 Identity Fraud report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends," p. 17, February 2014.
[6] Today, "Data breaches cost consumers billions of dollars," June 5, 2013.
[7] Experian Data Breach Resolution, "2015 Second Annual Data Breach Industry Forecast," pg. 6, http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182.
[8] Ponemon Institute, "The Post Breach Boom," pg. 2, Feb. 2013.

hamper the effectiveness of any national law on data breach notification and data security. Too many breaches occur for any one agency to respond effectively to all of them. Some breaches will be too small to be a priority at the federal level, yet such breaches could have a large impact in a particular state or region. State attorneys general must have the authority to investigate such breaches, and they should be able to continue to require notification to their offices. Moreover, without state data breach laws and their notification requirements, there would be far less information available to the public about data security and the need for consumers to be vigilant about the misuse of their personal information.

If Congress does choose to preempt the states in some fashion, it should do so as narrowly as possible, as it has done in the past. Any preemption of state law must be narrowly tailored to preempt only those state laws that are inconsistent with federal laws, and then only to the extent of the inconsistency. Preemption should be limited to the timing, manner, and content of the notices provided to consumers.

Congress has taken this narrow approach to preemption previously. In the Gramm-Leach-Bliley Act, which regulates the security practices of financial institutions, Congress only preempted state laws that are inconsistent with federal law and then only to the extent of the inconsistency.[9] It protects a state statute "if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under [federal law]."[10] Congress took a similar approach for health information in the Health Information Technology for Economic and Clinical Health (HITECH) Act, which preempts only those provisions of state law that are contrary to the federal standard,[11] as well as in the Fair Credit Reporting Act (FCRA), which preempts state laws "to the extent that those laws are inconsistent . . . and then only to the extent of the inconsistency."[12]

To ensure that any federal data breach notification law is effective and consumers are afforded the best protection, it is crucial that state attorneys general maintain their enforcement authority under their states' laws, and that any preemption provisions be narrowly tailored. As you and your colleagues debate these issues, we hope you take into consideration the comments we have provided here. Through our work on data breach investigations we understand the complexity of these issues and want to ensure that the progress made at the state level is not lost.

Sincerely,

Brian E. Frosh
Attorney General

[9] 15 U.S.C. § 6807(a).
[10] 15 U.S.C. § 6807(b).
[11] 42 U.S.C. § 1320(d-7).
[12] 15 U.S.C. § 1681t.