Statement of Elizabeth Wilkins
Senior Counsel for Policy
Office of the Attorney General

Before the

The Committee of the Whole
The Honorable Phil Mendelson, Chairperson

Public Hearing

"Bill 23-215, Security Breach Protection Amendment Act of 2019"

November 12, 2019
Time 11:00am
Room 412
John A. Wilson Building
1350 Pennsylvania Avenue, NW
Washington, District of Columbia 20004

Good afternoon Chairman Mendelson, Councilmembers, staff, and residents. I am Elizabeth Wilkins, and I serve as the Senior Counsel for Policy for the Office of the Attorney General ("OAG"). I am pleased to appear on behalf of Attorney General Karl A. Racine before the Committee of the Whole to testify on OAG's proposed bill, the Security Breach Protection Amendment Act of 2019. The bill before the Committee today makes significant advances in our ability to protect District consumers in the new data economy.

The security of consumers' data is becoming an increasing concern in our new digital era. By consumer data, we mean any personal information that may be collected on a consumer. We used to think primarily about, say, social security numbers collected by banks. But we have seen an explosion of the breadth of information collected on people, as well as significant changes in the ways that data is collected and stored. The more data that's out there, the more attractive it is to those who would misuse it, and the greater risk that consumers might suffer the consequences.

Our office has seen this dynamic in the frequency and increasing size of data breaches. A data breach occurs when sensitive or confidential information is intentionally or accidentally released by a company or an individual. These releases of information may happen because of insufficient security protections or as a result of hacking or cyber attacks. Recent years have seen some of the largest

and most serious data breaches in history, including the Equifax breach, which exposed the personal information of over 143 million people, including nearly 350,000 District residents.

Consumers caught in the crosshairs of these data breaches risk identity theft and other types of fraud. They may suffer financial harm, loss of significant time and resources, and even harassment.

Under our current laws, District consumers are not sufficiently protected. The District adopted our data breach laws in 2007—a lifetime ago in terms of the digital economy and cybersecurity. Many states have updated their laws to reflect these changes, and it is time the District did so as well.

After closely studying data breach laws in other jurisdictions and the latest innovations in this policy arena, our office proposed the bill at issue today, the Security Breach Protection Amendment Act of 2019. With this bill, we can protect our consumers here in the District and be coequal partners with our fellow state attorneys general in policing national cybersecurity issues.

If this bill becomes law, it would require companies that hold consumer data to do two things: maintain reasonable security procedures to safeguard consumer data, and notify consumers and the Attorney General of a breach. Certain key

reforms ensure that the law is crafted to keep up with current data practices, protect consumers, and create the right incentives:

(1) Current law protects a narrow swath of personal information that was at issue over ten years ago when our original bill was passed. This bill updates the definition of personal information to include additional sensitive information, some of which has been the subject of recent data breaches: passport number, taxpayer identification number, military ID number, health information, biometric data, genetic information and DNA profiles, and health insurance information. This update ensures the law better protects the growing breadth of sensitive information consumers may have at risk.

(2) Current law dictates that even where data is acquired without authorization, it does not constitute a breach if the data at issue has been rendered secure by appropriate cybersecurity techniques. The bill clarifies that a breach nevertheless *does* occur if the unauthorized access has undermined the efficacy of that security. This provision plugs a loophole to ensure that entities can be held accountable where their security measures are inadequate and consumers have been put at risk.

(3) Current law requires that companies notify consumers of a breach. This bill inserts requirements for the content of that notification to consumers, including a requirement that it include a statement informing residents of the right to obtain a security freeze at no cost (pursuant to federal law) and, where appropriate, the right to identity theft prevention services. This increased information ensures that consumers are armed with the information they need to protect themselves.

(4) The bill also requires notification of a breach to the Attorney General. This provision brings the District's law into line with that of most other states and ensures that OAG can take swift action in case of a breach affecting District residents.

(5) The bill requires persons and entities that own, license, maintain, license, or otherwise possess personal information to implement and maintain reasonable security procedures and practices. This is crucial: Given the amount of data we now entrust to third parties, we must ensure that those entities treat that data with the appropriate care.

(6) The bill adds a requirement that in the case of a breach of social security numbers, the company must provide 2 years of identity theft prevention services. Again, we want to ensure above all else that consumers are protected.

(7) The bill makes a violation of the data breach law a violation of the Consumer Protection Procedures Act (CPPA), the District's main consumer protection statute. This provision confirms that violations of the data breach law can be addressed through enforcement under the CPPA, ensures that there are real teeth to our law, and creates the appropriate incentives for companies to safeguard the data of their consumers.

Advances in the digital economy and in other states' policies around data breaches mean that the District is behind the times. We need this modernization of our data breach law in order to ensure that District residents are protected.

Thank you for the opportunity to testify, and I am happy to answer any questions that members may have.