Testimony of

Brian Young

Public Policy Manager

of the National Consumers League

on

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

Before the

Council of the District of Columbia

Committee of the Whole

November 12, 2019

John A. Wilson Building

Room 412

1350 Pennsylvania Avenue, NW

Washington, DC 20004

11:00 am

Chairman Mendelson and distinguished Councilmembers of the District of Columbia, the National Consumers League appreciates the opportunity to present the following testimony to the Committee of the Whole in support of The Security Breach Protection Amendment Act of 2019 and the need for the Council of the District of Columbia to take action to protect District residents from the scourge of data breaches.

Founded in 1899, the National Consumers League (NCL) is the nation's pioneering consumer organization. Headquartered here in the District, our non-profit mission is to advocate on behalf of consumers and workers in the District, the United States and abroad.[1] Through NCL's Fraud.org campaign, NCL offers free fraud counseling, and educates consumers across the country on how to protect themselves in the aftermath of data breaches.[2]

Sadly, there has been no shortage of data breaches. Equifax, Capital One, Yahoo!, Marriott, Anthem, JP Morgan Chase, and thousands of others have all compromised consumers personal information, putting all of us at greater risk of identity fraud and other crimes. In fact according to the Identity Theft Resource Center (ITRC), there have been around 11,000 data breaches and over 1.6 billion compromised records since 2005.[3] That number appears to be growing. In the ITRC's latest report, they observed a year over year increase of 126 percent in

[1] For more information, visit www.nclnet.org.
[2] For more information, visit https://www.fraud.org/
[3] Identity Theft Resource Center. "Data Breaches." 2019. Online: https://www.idtheftcenter.org/data-breaches/

2018 of the number of compromised records which contained sensitive identifiable information.[4]

In the aftermath of a data breach, fraudsters, scammers, and identity thieves manipulate the breach data to further harm consumers. Leaked login credentials are often used to access other accounts that use the same username and password combination. Data obtained via a breach can be used to craft more convincing phishing emails, conduct social engineering attacks on call centers, open new lines of credit and steal consumers' tax refunds, to name just a few of the harms that can stem from breaches.

DC residents are not immune to this threat. A survey conducted by Wallet Hub, a personal finance website based in the District, found that when compared to the 50 other states, the District of Columbia had the highest cases per capita of identity theft and fraud in the nation.[5] It is for these reasons that we are strongly supportive of the Security Breach Protection Amendment Act of 2019, which would help better safeguard the data security of District residents.

First, this bill extends the definition of personal information to cover extremely sensitive data that if controlled by scammers, could wreak havoc on consumers. Without this bill, information including passport or military ID numbers; health information; biometric data

[4] Identity Theft Resource Center. "2018 End of Year Data breach Report." January 28, 2019. Online: ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

[5] McCann, Adam. "2019's States Most Vulnerable to Identity Theft and Fraud." Wallet Hub. October 16, 2019. Online: https://wallethub.com/edu/states-where-identity-theft-and-fraud-are-worst/17549/#main-findings

such as an individual's voice or finger print or other unique biological characteristics; and DNA profile information would not receive the protection it deserves.

Second, this legislation will provide meaningful improvements to the District's breach notification standard. Under this section District residents will be notified what types of data were potentially compromised, and be given the information they need to contact the business directly as well as educational information on how they can receive a credit freeze free of charge and protect themselves from identity theft.

Third, this bill empowers the Attorney General's office to proactively help breach victims via a requirement to promptly notify the Attorney General's office of a breach.

Finally, this consumer protection bill will help stop breaches before they happen by requiring holders of personal data, to take reasonable steps to secure and safeguard the data they have been entrusted with. As technology changes, so do cybersecurity best practices. NCL appreciates the regulatory flexibility that this bill provides to ensure that businesses are encouraged to take proactive steps to secure user data. When breaches happen, it is often because the business did not utilize current best practices to secure data, and yet, it is the consumer that bears the price for the business' misstep. Consumers cannot and should not be expected to carry the load when it comes to protecting the data they share with businesses and other organizations.

As the problem of data breaches continues to grow, so does the risk to Washingtonians of falling victim to identify theft, and other types of fraud. While this bill does not address critical

issues like how businesses obtain and share data, and the control consumers need to have over this process, the Security Breach Protection Amendment Act off 2019 will take meaningful steps to compel businesses to responsibly handle District residents' data. Likewise, this bill provides meaningful disclosures and educational materials that consumers need to avoid fraud.

NCL believes that each councilmember has a unique opportunity to safeguard District residents' data, and thus urges the Council of the District of Columbia to quickly pass and implement this critical consumer protection bill.

Thank you for your time.