Nationwide
is on your side

Kirk M. Herath
VP, Chief Privacy Officer, Associate General Counsel

January 10, 2018

The Honorable Bill Coley
Ohio Senate
Chairman, Ohio Senate Government Oversight and Reform Committee
VIA ELECTRONIC SUBMISSION

Re: SB 220 (Hackett, Bacon) Provide legal safe harbor if implement cybersecurity program

Dear Chairman Coley,

On behalf of Nationwide, thank you for the opportunity to provide a letter in support of the Data Protection Act (SB 220). Nationwide, a Fortune 100 company based in Columbus, Ohio, is proud to provide 15,000 jobs in the state and 1.25 million policies to Ohio residents. SB 220 provides a simple incentive to Ohio businesses to establish or enhance data security to protect the personal information of Ohio consumers from potentially harmful cyber-attacks. Protecting confidential customer and business information is extremely important to Nationwide and its customers.

It's no secret that cyber-attacks happen and are doing so with greater frequency. Unfortunately, there is no single, perfect information security system in existence today that would allow consumers to reap the benefits of digital technologies, while preventing every potential cyber-attack. With ever more sophisticated and constantly evolving tools and methods at their disposal, cyber criminals are proving to be a formidable foe for both the public and private sectors. Therefore, the most appropriate way to protect sensitive customer and business information from cyber-attacks is to utilize a reliable and recognized information security framework. The Data Protection Act does exactly this.

SB 220 promotes the use of the National Institute of Standards and Technology's Cybersecurity Framework ("the NIST CSF"), as well as other nationally and internationally recognized and proven information security frameworks and standards. The NIST CSF was created through collaboration between government and the private sector to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on businesses. Furthermore, it enables businesses – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the most up-to-date and effective standards, guidelines and best practices of cyber risk management.

Information security frameworks (e.g., the NIST CSF, ISO/IEC 27000 series, COBIT 5, NIST SP 800-53, etc.) are very useful in creating an effective and scalable organization-wide information security program. To be effective, a security program must be compromised of many layers (e.g. logical, administrative and physical protection mechanism; procedures; business processes; and people) that all work together to provide reasonable protection for information assets. Frameworks like the NIST CSF provide companies with risk-based solutions to cybersecurity challenges and use risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity.

Companies conducting business in Ohio that utilize frameworks, such as NIST CSF, and other recognized statutory standards encouraged by SB 220, will without a doubt implement stronger and more sustainable cybersecurity programs, which will result in the better protection of the personal information of Ohio consumers and businesses. And, when such companies ultimately experience a data security breach, they will be better prepared to respond, recover and mitigate any potentially harmful effects to Ohio consumers. Again, thank you for your consideration of SB 220.

Sincerely,

Kirk M. Herath
VP, Chief Privacy Officer, Associate General Counsel

Cc: Ohio Senate Government Oversight and Reform Committee
Senator Bacon and Senator Hackett