SB 220 – Cybersecurity safe harbor
Testimony by Curtis Fifner
For the Ohio Association for Justice
Before the House Government Accountability & Oversight Committee
June 26, 2018

Chair Blessing, Vice Chair Reineke, Ranking Member Clyde and Members,

Thank you for the opportunity to provide opponent testimony on Senate Bill 220. My name is Curtis Fifner. I am a trial lawyer and a member of the Ohio Association for Justice, the state bar association for attorneys who help people get back on their feet financially after they have been injured in a car collision or in the workplace, by a defective product, or as a result of a medical error, or those who have been damaged because their identities have been stolen in a data breach.

I want to begin, Mr. Chairman, by acknowledging there is value in encouraging business entities to do the right thing and implement cybersecurity protections. We appreciate the intentions behind SB 220 and don't want our testimony to be interpreted as a rejection of their well-meant objective.

The question is: Will this special legal protection work as intended?

Will a business executive who has decided not to spend the money to implement cybersecurity … or who doesn't have the time as he or she races from project to project, trying to drum up orders, and meet payroll … will a state law establishing an affirmative defense to legal claims serve as the tipping point that causes a business executive to implement cybersecurity protection? We doubt it.

At the heart of this proposal is an incentive, an affirmative defense against legal claims, which can be asserted by any business entity that complies with the NIST cybersecurity framework (NIST stands for National Institute of Standards and Technologies under the US Department of Commerce) or certain other industry cybersecurity frameworks, as defined in 1343.03 (starting in line 105). But the legislation doesn't even require full compliance. It says the compliance shall be deemed, and the affirmative defense shall attach, if an entity "reasonably complies" (see Sec 1354.03 starting in line 105). While the term "reasonable" is fairly well-established in tort law, interpretations of the term in this context will, it is safe to say, be the subject of litigation for years to come. The question courts will be asked is: How vigorous a cyber security protection framework would prudent person adopt under a given set of circumstances?

In the Senate I testified that the affirmative legal defense proposed by this legislation would serve as a high legal hurdle making it very difficult for people that suffer damages to succeed with a legal claim under state law. The affirmative defense creates a basis for a motion to dismiss a claim even before the injured plaintiffs get an opportunity to present their case. I am pleased to say that Attorney General DeWine has set the record straight, in writing, that the proposed affirmative defense is not a motion to dismiss issue. I'll be glad to supply the committee with a copy of the Attorney General's letter, if you wish. To make the legislation clear, we strongly urge you to adopt an amendment to bring the bill in line with what Attorney General DeWine says; the proposed affirmative defense is not to be used in a motion to dismiss.

While the proposed affirmative defense and the term "reasonable compliance" won't stop legal claims from being filed, they are almost certain to increase legal costs. At the outset of litigation, thousands of claims may be filed, mountains of evidence collected, hours of depositions taken, just to determine if the breached corporation was in reasonable compliance with NIST (or other cyber security standards) and deserves the affirmative defense.

If a damaged party is able to clear the legal hurdle by showing the entity was NOT in reasonable compliance, and therefore the affirmative defense does not apply, next the plaintiff has the burden to show the defendant was negligent. Virtually all of these legal actions are brought under state law. Negligence is the primary legal theory most often asserted, followed by actions alleging violations of consumer protection, breach of contract, unjust enrichment and fraud. Only a fraction of these claims are brought under the Federal Stored Communications Act, which is the only cause of action where the federal courts will have jurisdiction.

Past history indicates this bill would excuse from accountability major corporations that are breached. Across the country in 2016 just 27 defendants faced data breach litigation. None of these were small companies; all were major corporations. Almost all (89%) involved a breach of sensitive information like Social Security numbers, medical treatment information, and health insurance information. To the best of our knowledge, this legislation, if followed, would not have prevented a single major data breach. We would expect that if this were the case, supporters of this bill would have pointed this out at some point throughout this process.

If this legislation is enacted, it excuses and defeats all the acts by these companies, regardless of how negligent, reckless, or willful, that caused millions of people to have their personal information stolen. It results in the companies qualifying for this immunity essentially being blessed by the State of Ohio as innocent and shifting the costs away from the only entity with the power to have stopped the data breach in the first place.

Instead, this burden is placed directly onto the backs of Ohio citizens and other companies that trusted the breached company with their information so they could get a loan, rent an apartment, or engage in the basic necessities of living in the 21st century. This is not about pain and suffering or punitive damages. It is about holding companies accountable when their negligent or reckless conduct results in an Ohio citizen's protected personal information being compromised. We believe that an Ohio citizen should have some form of recourse when that individual has to spend years dealing with the fraudulent tax returns filed in their name, the destruction of their credit, and even the threat of a fraudulent concealed carry licenses obtained in their name.

Contrary to testimony that you heard that consumer groups have not come forward to express their opposition to SB 220, many of our nation's major consumer organizations wrote the Senate committee to express their opposition to the bill. Among those groups were the Consumer Federation of America, Consumer Action, Defending Rights & Dissent, US Public Interest Research Group, Patient Privacy Rights, the Privacy Rights Clearinghouse and the Digital Privacy Alliance. These groups all support our position that this bill will not reduce the impact of a data breach, nor likely the frequency. And it provides consumers with no redress for tort-based causes of action.

We invite you to take a step back and think through the possible consequences of this legislation. This is a first-of-its kind legislation, not enacted by any other state, so we don't know what the outcomes will be. However, we do know that the bill would serve as a significant impediment to recovery for consumers and small businesses who suffer real damages. And we believe the bill will not make a difference in the number of companies that implement cybersecurity protections.

Thank you, Mr. Chairman and members, for listening to our views on SB 220. If you have questions, it would be my pleasure to continue our conversation.