PA COALITION FOR

CIVIL JUSTICE

REFORM

Testimony on HB 1010

February 25, 2020

Good morning Chairman Keller, Chairman Galloway and members of the committee. My name is Curt Schroder and I am the Executive Director of the Pennsylvania Coalition for Civil Justice Reform. The Pennsylvania Coalition for Civil Justice Reform is a statewide, nonpartisan alliance of organizations dedicated to bringing fairness to our courts by elevating awareness of civil justice issues and advocating for legal reform in the legislature.

HB 1010 addresses the serious problem of data breaches. We hear much discussion of data breaches in the news today. The Associated Press recently reported that the Justice Department charged four members of the Chinese military with breaking into networks of the Equifax credit reporting agency. Tens of millions of Americans had their personal information stolen making it one of the largest hacks in history to target consumer data.

While individual consumers were victims of this breach, so too was Equifax. In fact, any business, large or small, for profit or non-profit is

the victim of a crime when their security is breached. Every day businesses are under attack by bad actors seeking personal data for criminal purposes. The internet, smart phones, personal computers and other electronic devices have transformed the way commerce operates. Every company in Pennsylvania whether a small pizza shop, a multi-national corporation, or a non-profit service organization, stores data regarding its employees and customers. In our zeal to protect consumers, we must not punish the other victims of these criminal acts by imposing burdensome and unnecessary litigation.

HB 1010 encourages residents of Pennsylvania to file suit when their data is accessed through a breach. This is regardless of whether the individual suffers any actual monetary damage or loss. While an action at common law exists for victims of a data breach, HB 1010 goes well beyond the common law and creates unreasonable litigation risks for entities that took no action to harm to consumers.

The bill creates a separate, expansive right of recovery with:

- A duty for an entity to take "reasonable measures, consistent with the nature and size of the entity." While "reasonableness" is a concept often associated with negligence claims, it is a case study in vagueness. This standard offers no guidance to businesses of any particular size, whether non-profit or for profit, as to what steps they are expected to take to prevent a data breach. While lawyers might like to argue and wax eloquently about what constitutes reasonableness, there is no guidance in HB 1010 to help a business know whether it is in or out of compliance. Other statutes such as that found in New York use a reasonableness standard but also provide actual data protection standards to be met and provide the business entity with certainty so they know when they are living up to their responsibility under the law. This legislation should do the same.
- HB 1010 contains a 3 year statute of limitations which is longer than that found at common law;

- HB 1010 allows a minimum recovery of $5,000 even if the individual has not suffered monetary damage;
- HB 1010 subjects a victim of a crime to treble damages, that is, three times the actual damages or three times the enumerated $5000 minimum recovery. This creates a class action bonanza that only benefits trial lawyers;
- In addition to possibly paying three times the amount of damages, the crime victim must pay the plaintiffs' attorneys fees and costs;
- Arbitration agreements are voided, forcing the consumer and the business to endure the delays, inconvenience, conflict, and uncertainty that goes along with adversarial litigation proceedings;

This committee should ask itself: do we want to solve the very real problem of preventing data breaches, or do we want to create a litigation bonanza for trial lawyers through encouraging class action litigation. There is only one winner in class action litigation. And it is

not the plaintiff members of the class on whose behalf the suit is brought.

Studies have found that the overwhelming majority of class action members receive little or no benefit from class action lawsuits. Even when class actions are settled, the percentage of class members who actually receive a benefit is miniscule. The class action litigation system labors under an inherent conflict between the interests of the lawyers who bring these cases and the interests of class members. Too many cases are filed based on the ease with which a settlement may be extracted—with little or no focus on whether there is serious consumer harm. And too many cases are settled with illusory benefits to class members and large fees for lawyers. Recent court challenges to proposed settlements have illuminated the prevalence of these abusive practices.

Most class actions today are created not by injured consumers seeking redress but by plaintiffs' lawyers looking to recover substantial

amounts in attorneys' fees. Plaintiffs' lawyers have taken control of the consumer class action mechanism and turned it into a big business that uses the threat of expensive litigation and potentially ruinous damages to pry billions of dollars in settlements and hundreds of millions of dollars in legal fees from businesses each year.

And that is precisely the danger of this legislation. A company could be wiped out and ruined financially if the personal data of thousands of individuals is criminally stolen. 10,000 individual members of a class with a payment of $5,000 each pursuant to this bill results in $50,000,000 in damages. And that is BEFORE trebling which would bring the award to $150,000,000. And let's not forget the bill provides for attorneys' fees and costs on top of that. And who really benefits? The Plaintiffs' lawyers would get roughly one third or $50,000,000 of a trebled award while the consumer gets his or her $15,000 each. Or the attorneys would get $151,515,152 of a non- trebled award under this example while the consumer gets $5,000.

Data breaches victimize the individual consumer and the entity that is broken into by the criminal hacker. Both classes of crime victims deserve to be treated fairly. Is it "reasonable" to expect any business to be so secured that foreign military intelligence cannot penetrate it?

Perhaps the best argument against the vague reasonableness standard contained in HB 1010 has been raised by attorneys themselves. Just last week, the Legal Intelligencer contained an article reporting that more than 100 law firms have reported data breaches and the picture is getting worse. In the article, attorney Kevin Baker pointed out that the Rules of Professional Conduct require attorneys to take "reasonable steps to protect their clients' data." Attorney Baker argued that because the rules contain no specific technical requirements, attorneys are placed in the difficult position of trying to determine what is sufficient to meet the reasonableness standard when it comes to cybersecurity. Attorney Baker points out that what was considered reasonable yesterday is not reasonable today and today's standards will

be obsolete tomorrow. What is reasonable for a large firm may not be reasonable for a small practice and vice versa.

This legislation should not move in its current configuration. Consider using a standard with technical specifications with which businesses of all sizes can understand and comply. Avoid incentives to bring litigation with little benefit to the individual, a windfall to the attorneys, and a possible bankruptcy to the business.