DiCello Levitt & Casey

Testimony in Opposition to S.B. 220
By Mark Abramowitz on behalf of Amy E. Keller, DiCello Levitt & Casey LLC
Co-Lead Counsel in *In re Equifax, Inc. Customer Data Security Breach Litigation*,
No. 17-md-02800 (N.D. Ga.)

Before the House Government Accountability & Oversight Committee
June 26, 2018

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

DiCello Levitt & Casey is a law firm with deep roots in the State of Ohio. Indeed, members of our firm, and our predecessor firm, have helped consumers, patients, individuals, and small businesses in this State for nearly 50 years.

Of note and of importance to this hearing, Amy E. Keller, one of the firm's partners, was appointed—and is currently serving—as co-lead counsel by federal Judge Thomas Thrash in the Northern District of Georgia to lead the litigation against Equifax for its 2017 data breach, which compromised the sensitive information of close to 148 million people and small businesses, including individuals from the State of Ohio.

Although our firm primarily stands up for the rights of consumers through the court system, we have also been retained by companies to investigate creative ways to limit their exposure, and we routinely represent small businesses with claims against large, corporate entities. Our firm has also been hired by various state Attorneys General to investigate and prosecute consumer complaints, and to obtain settlements or judgments against individuals and corporations who violate the law.

Our objective is not to prevent this Committee from protecting the rights of both consumers and businesses, but, rather, to work with this Committee to find a path that satisfies both of those goals. We do not believe, however, that this Bill, S.B. 220, will have that desired effect. This is the same message that I presented on May 9 to the Senate Government Oversight & Reform Committee and Chairman Coley.

S.B. 220 would not reduce the impact of a data breach, nor likely their frequency. While companies will certainly look to the various minimum standards that S.B. 220, following these voluminous standards—indeed, some more than hundreds of pages long—will not make data breaches any less prevalent. Rather, what S.B. 220 *will* do is increase the cost of litigation, and

ask federal and state court judges to become experts in data privacy and cryptology at the motion to dismiss stage of litigation. Although Attorney General DeWine stated in a letter dated May 16, 2018, that "[t]he 'safe harbor' is not automatic. . . [t]his is not a motion to dismiss issue, rather, it will be decided by the trier of fact at trial," the Fiscal Note & Local Impact Statement by Robert Meeker demonstrates that this is inaccurate: not only does the Bill serve to deter the filing of cases, but it allows trial court judges to "more promptly dispose of a case than it otherwise might have under current law." The Bill asks for trial court judges to become experts in data security and, to the extent a case actually gets filed, "promptly dispose" of it.

Unfortunately, the Bill does not guarantee that, by following certain criteria, data will be protected. This Committee need look no further than the Anthem data breach, announced on February 4, 2015, in which hackers broke into Anthem's servers and stole the personally-identifiable information of 78.8 million people. The information, which included names, birthdays, medical IDs, Social Security numbers, street addresses, email addresses, employment information, and income data, was not encrypted—nor was it, at that point in time, legally required to be. Anthem followed the minimum criteria promulgated by the Health Insurance Portability and Accountability Act ("HIPAA"), which is one of the standards that the Committee has proposed could provide a company with safe harbor in its Bill. *But HIPAA did not prevent the hack.* Indeed, many of the standards that the Committee proposes here are minimal "best practices" that will not foster innovation or incentivize companies to take proactive measures to protect individuals' most sensitive data.

As a result, individuals like you and me, who had no say in how companies store their information, are now compromised and perpetually at risk. They must be vigilant for the rest of their lives in protecting their credit—moreso than the average consumer—because a company decided not to encrypt their data.

Thankfully, a class action lawsuit was brought against Anthem that resulted in a meaningful settlement, providing credit monitoring for consumers, a settlement fund to pay identity theft claims, and additional measures that would ensure that consumers' credit would be protected for years to come. Anthem, as the company that elected *not* to safeguard the data, and who bore the risk of not investing in additional resources to secure the data that it elected to keep on Internet-accessible servers, is able to pay the settlement as a cost of doing business.

More recently and here in Ohio, AultWorks Occupational Medicine, Aultman Hospital, and some Aultman physician offices had a data breach affecting 42,600 patients. Through this breach, hackers were able to steal the personal health and identification information of these people. The breach occurred when several employees opened emails containing a virus. This should not have happened and HIPAA compliance did not prevent it—despite Attorney General DeWine's May 16, 2018's letter to the Senate Government Oversight and Reform Committee.

However, despite the harmful affect this can have on these 42,600 Ohioans, S.B. 220, would strip away from them the right to redressed for any losses that would come from this breach.

The safe harbor that S.B. 220 would provide would shift the cost of a company's use of minimum criteria in safeguarding data to the individual consumers—who have no choice in what security measures the company chooses, how the company stores data, who the company provides that data to, and how long that company keeps their data. The safe harbor is bad for companies, it's bad for consumers, and thus, it's bad for the State of Ohio.

The purpose of lawsuits arising from data breach incidents is *not* to bankrupt companies. Rather, these lawsuits ensure that companies factor the potential for data falling into the wrong hands (and the legal exposure for such incidents) as part of their investment into cyber security protocols. Attorneys who bring data breach lawsuits want to work with these companies to ensure that they can provide the necessary protection to consumers whose data is compromised. Importantly, class action settlements provide something of value to companies who are sued: releases for current and future claims related to the breach. The company is able to ensure that its liability is limited, and assure its investors that any exposure related to a breach has an end point.

Some may say that S.B. 220 would also limit the liability for companies because it would become increasingly difficult to sue them. The problem with this logic is that it ignores patchwork, state-by-state legislation enacted regarding data breaches. Most data breaches affect consumers nationwide—such as the current litigation that my firm is co-leading against Equifax. Those lawsuits are brought by consumers *and* small businesses on behalf of nationwide classes. At the motion to dismiss stage, S.B. 220 would require judges in federal courts in different parts of the Country to decide whether a company "complied" with one of several different best practices—wading through hundreds of pages of technical documents—in order to address the issue at the motion to dismiss stage. S.B. 220 would require federal and state court judges to become experts or prospectively analyze expert reports, something that is not contemplated by the Federal Rules of Civil Procedure or the Ohio Rules of Civil Procedure at the pleadings stage, and which could create a conflict with the Class Action Fairness Act for nationwide cases, and the authority afforded to judges to run their dockets and set case deadlines. Moreover, any resulting opinion on a motion to dismiss could be appealed, resulting in additional litigation costs.

It is also important that the Committee not lose sight of small businesses and financial institutions when considering this Bill. As I explained earlier, my firm is co-leading the litigation against Equifax, which *also* includes actions *on behalf of small businesses and Financial Institutions* who were detrimentally affected by Equifax's data breach. While the mediaf focuses much of its attention on how individuals were affected by the 2017 breach, the

consolidated litigation *also* seeks damages on behalf of small businesses and financial institutions who were harmed by the breach—small businesses owned by one or two individuals, who were unable to obtain a loan, had to pay for small business credit monitoring, or had to pay for a small business credit report because of the breach. Financial institutions have been refunding fraudulent charges to their credit card holders and issuing them new cards.

S.B. 220 would have a chilling effect on allowing small businesses and financial institutions to pursue their claims against companies like Equifax. *Make no mistake: this Bill would ultimately hurt, not help, small businesses and financial institutions.*

While the purpose of S.B. 220 is an admirable one, providing a safe harbor, which would require judges to decide this issue at the motion to dismiss stage, would be disruptive, costly, and will lead to inconsistent rulings and increased litigation costs. S.B. 220 will not end data breaches; rather, it will shift the cost of those breaches to the consumers, who have no say in how companies store their data and will give companies a free pass for their bad behavior.

Litigation is an effective tool to discourage sloppy data security, and also enables companies to cap their liability, obtain releases from affected consumers, and ensure that their consumers are protected. Rather than providing companies with a safe harbor, the Committee should work with attorneys to strengthen consumer protection laws, and follow the guidance from states and countries enacting strict cyber security protocols to prevent data breaches. S.B. 220 does not do that and should thus not be enacted.

Thank you for your time and consideration.