SQUIRE PATTON BOGGS

# Ohio Enacts Law Aimed at Incentivizing Compliance with Well-known Cybersecurity Industry Standards

A growing trend among businesses to reduce their exposure to cyberattacks has resulted in substantial improvements in cybersecurity, but has done little to halt the onslaught of post-breach litigation that calls into question the adequacy of the victim-business' controls.

Even organizations with the most robust and mature cybersecurity programs have little hope of avoiding exposure to tort-based litigation following a data breach.

In October 2017, Senate Bill 220 (S.B. 220) was introduced in an attempt to address this problem, aiming for Ohio to become the first state to offer a potential new affirmative defense for Ohio businesses facing post-breach litigation. Under the original bill, as long as an Ohio business created, maintained and complied with an internal "written cybersecurity program" in "substantial compliance" with one of many well-known cybersecurity industry standards, the business could potentially ward off allegations that it failed to implement reasonable information security controls to prevent the breach.

S.B. 220 is now set to go into effect on November 2, 2018. This update focuses on the major changes that S.B. 220 has seen over the 12 months from introduction to enactment – and what it means for all businesses processing Ohio residents' data.

## S.B. 220's Benefits Extend Beyond Ohio's Borders

One of the major changes to hit S.B. 220 since its introduction is the Ohio Legislature's decision to significantly expand the definition of "covered entity" by removing the framers' initial requirement that businesses must be operating in Ohio in order to avail themselves of the affirmative defense (the Ohio legislature has also clarified that S.B. 220 extends to financial institutions).

This change will have the effect of further incentivizing a wider group of businesses to invest in the maturity of their cybersecurity programs so as to be in a position to avoid breaches in the first instance, but also to leverage these investments in post-breach litigation whenever Ohio law applies.

That said, businesses should be mindful of the fact that Ohio law is unlikely to apply to all post-breach litigation. Whether by contract or a state's conflict of laws rules, when another state's law applies to a post-breach dispute, victim-businesses will be without the S.B. 220 affirmative defense even despite the best of efforts to comply with the statute.

## Compliance Becomes "Reasonable"

Sharing the spotlight with this expansion is the Ohio Legislature's decision to overhaul S.B. 220's compliance requirement. While the initial language of S.B. 220 required "substantial compliance" with industry standards, the final language uses a facially less-rigid approach, obligating businesses to "reasonably conform" their cybersecurity programs to industry standards.

This appears to signal the Ohio legislature's intent to avoid hyper-technical arguments of noncompliance. It also suggests that courts and litigants alike will be able to rely upon the extensive body of cases discussing "reasonableness" in other contexts. Yet, businesses should still expect to see plaintiffs challenging the scope and appropriateness of their cybersecurity programs post-breach.

All of the other cybersecurity program requirements from the original bill remain intact, except that the final language of S.B. 220 now requires a compliant cybersecurity program only "… with respect to the information it is meant to protect." The Ohio legislature has also expanded the list of approved industry standards to include the Payment Card Industry Data Security Standard (PCI-DSS) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

**As of November 2, "reasonably conforming" to any of the following industry standards will allow a business to avail itself of S.B. 220**:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- NIST 800-171
- NIST 800-53/800-53a
- Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework
- The Center for Internet Security (CIS) – Critical Security Controls
- ISO 27000 Family Standards – Information Security Management Systems
- PCI-DSS
- For regulated entities:
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Title V of the Gram-Leach-Bliley Act of 1999 (GLBA)
  - Federal Information Security Modernization Act of 2014 (FISMA)
  - HITECH

## Addition of "Restricted Information" Broadens Scope of Protections Afforded

Seeking to further incentivize covered entities to adopt robust internal cybersecurity programs in line with S.B. 220, the Ohio legislature has looked beyond the more traditional, breach-notification-triggering definition of "personal information" (e.g., first name or initial and last name, plus social security number or driver's license number) to regulate any information that:

- Alone or in combination with other information, including personal information that can be used to distinguish or trace an individual's identity **or** that is linked or linkable to an individual,
- Is not encrypted, redacted or otherwise made unreadable **and**
- The breach of which is likely to result in a material risk of identity theft or other fraud to person or property.

S.B. 220 refers to this as "restricted information." A business that expressly incorporates this new classification (in addition to the more traditional "personal" information) into its cybersecurity program will be able to leverage an even broader affirmative defense against post-breach allegations that the business failed to implement reasonable security controls.

## Preempting Criticism

Critics of affirmative defense statutes cite concerns that such statutes could be misinterpreted to impose liability on organizations that do not comply. For instance, one might ask through what lens a business should be viewed if it does not "reasonably conform" to one of the industry standards listed above.

To head this off at the pass, S.B. 220 expressly emphasizes the framers' intent to incentivize and encourage better security, and not to create some sort of "minimum cybersecurity standard that must be achieved" and against which organizations should be held when assessing their liability post-breach.

As the Conference of Western Attorneys General (CWAG) recently stated in a whitepaper on similar "Safe Harbor" regulations, "good cybersecurity is good business." According to CWAG, "[c]onsumers will frequent businesses that provide reliable data security," and "those that fail to provide privacy protections will fail." CWAG applauded Ohio's efforts with S.B. 220, noting business response and court treatment will be hot topics of interest over the coming years.

## What Does All of This Mean for Your Organization?

One thing is clear: if you process Ohio residents' "personal" or "restricted" information, there has never been a better time to align your cybersecurity program with the well-known cybersecurity industry standards listed in S.B. 220. Not only is doing so the best way to avoid a data breach in the first instance, it is also now a potential backstop when the unthinkable data breach happens and your business is hauled into court to explain why.

## Contacts


**Daniel E. Vinish**
Of Counsel, New York
T +1 212 872 9814
E daniel.vinish@squirepb.com

**Robin B. Campbell**
Partner, Washington DC
T +1 202 457 6409
E robin.campbell@squirepb.com

**Elliot R. Golding**
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirepb.com

**Leah G. Brownlee**
Of Counsel, Cleveland
T +1 216 479 8549
E leah.brownlee@squirepb.com

**David C. Blake**
Partner, Denver
T +1 303 894 6196
E david.blake@squirepb.com



The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations, nor should they be considered a substitute for taking legal advice.

© Squire Patton Boggs.

All Rights Reserved 2018