NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Carl Szabo, Policy Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
www.netchoice.org

Rep. Elaine Nekritz, Chair
House Judiciary Civil Committee
245-E Stratton Office Building
Springfield, IL 62706

May 12, 2015

RE: Opposition to SB 1833 – Personal Info Protection

Dear Chair Nekritz and members of the committee:

We ask you not to move SB 1833.

Industry has for years worked with legislatures and attorneys general to protect consumer information and provide breach notifications. Today, Illinois residents enjoy robust data breach notification.

However, we worry the expansions proposed in SB 1833 will result in unintended consequences that cause residents to ignore important notices and further exposes them to phishing attacks. At the same time, SB 1833 will cost small and mid-size businesses money they can little afford.

SB 1833 discourages Illini from paying attention to the truly important notices.

Data and our own experiences show that focus decreases on individual notices when overall notification increases. This means that if Illini receive too many notices about data breaches, they are more likely to ignore the notice of data breaches that create real threats of financial or physical harm. This is why most states have data breach notification laws that require notice only when there is a likelihood of such actual harms.[1]

Unfortunately, SB 1833 lacks a "harm trigger" and would require notice even when no harm is likely to occur. Moreover, SB 1833 requires notice even when non-sensitive personal information is taken.

Today, Illinois's data breach law limits "personal information" to only truly sensitive information like social security numbers and login plus passwords to financial accounts. However, SB 1833 changes the definition of personal information to include non-sensitive

[1] States with a harm trigger: Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Vermont, Washington, West Virginia, Wisconsin, Wyoming

information like "consumer marketing information." This means Illinois is equating the sensitivity of an SSN to an interest in football.

The effect of SB 1833 means that Illinois residents will receive data breach notices even when there is no likelihood of any harm and this over-notification will result in residents ignoring the important notices.

SB 1833 increases Illinois citizen's exposure to phishing attacks.

Bad actors not only attempt to hack into a system, but they also rely on tricking unaware consumers into turning over login information. An effective way is through phishing attacks timed with data breach notices.

When a data breach occurs, bad actors impersonate the breached company and send out fake electronic notices. These fake notices ask the user to "reset" login information, fraudulently collect it, and then use it cause real harm.

Under SB 1833, the number of data breach notices will increase. This means that bad actors have even more opportunities to engage in these phishing attacks and threaten Illinois residents.

SB 1833 treats victimized businesses as bad actors and imposes new costs on your small and mid-size businesses.

It is easy to blame a company whose data was stolen. However, this runs contrary to the way we typically address a theft: the victim is rarely blamed for being robbed. But that is what happens under SB 1833. SB 1833 treats victimized business as bad actors.

If a business fails to use reasonable security to protect consumer data that business may be liable under federal and state law. However, when a business using industry security standards is hacked, that business must engage in tens-of-thousands of dollars in legal fees and notification expenses. In addition, the business's reputation becomes tarnished. Is this how we should treat victims of a crime? To add insult to injury, SB 1833 would impose more of these costs even when the data stolen can't be used to cause any financial or physical harm.

Instead, we should only force businesses to notify consumers when the theft of personal information results in a likelihood of real harm – not information about the consumer's interest in football.

For these reasons we ask that you not move SB 1833. We appreciate your consideration of our views, and please let us know if we can provide further information.

Sincerely,

Carl Szabo
Policy Counsel, NetChoice