The SHIELD Act

What Boards & Property Managers Need to Know

THE COOPERATOR NEW YORK
THE CO-OP & CONDO RESOURCE

BY DARCEY GERSTEIN 28 FEBRUARY 2020

Last summer, Governor Cuomo signed into law the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which requires all businesses and organizations in possession of electronic personal information about any resident of New York State to safeguard that information by March 21, 2020; the Act also expands requirements for reporting data breaches.

Attorney Jay L. Hack of the Manhattan law firm Gallet Dreyer & Berkey, LLP regularly advises clients facing these issues, and says that co-ops and certain incorporated condominiums qualify as 'businesses' covered by this law, as well as its predecessors, the General Business Law and the State Technology Law. (Hack says that it could be argued that unincorporated condominiums are not covered, but certainly their managing agents are—and as custodians of the condo's data, they must comply.)

The existing provisions under these laws already require organizations to protect certain types of personal information, but the SHIELD Act expands on those to include not only identifying information like name and address, but also "private" information such as biometric data; health information protected by the Health Insurance Portability and Accountability Act (HIPAA); and any account number, email address, or identification number and associated password, access code, security question and answer, or other secured access information.

The Act also expands on the definition of a "breach." Whereas previous laws determined that the unauthorized acquisition of protected data is considered a breach, the new law defines a breach as unauthorized access to the data, regardless of whether any information was in fact acquired. In this new definition, computerized private

information that is viewed by or communicated to an unauthorized person or system is considered a breach, and must be reported. This amendment went into effect in October of 2019.

Ensuring Compliance

Compliance with the SHIELD Act requires implementation of a data security program that includes administrative, technical, and physical safeguards that according to the Act, “[should be] appropriate for the size and complexity of the business, the nature and scope of the business’s activities, and the sensitivity of the personal information the business collects from or about consumers.”

Obviously, the application packages that co-ops (and to some degree, condos) require from prospective buyers include a great deal of private information, so boards and managing agents must take a critical look at how they collect, store, and purge that data. “I really think that everybody should do a risk assessment,” advises Hack. “Look at what you collect, look at the size of your business, look at the nature of your network. Look at who’s got access to your network.”

In fact, Hack goes so far as to suggest that co-ops stop collecting such sensitive information altogether. “Board packages should not have the credit report and tax returns in it,” he says. “Those are available from the managing agent. If someone really wants to go look at it...have a data room -- either physical or virtual. We do this in securities due diligence all the time; you can go look at the stuff, but you can’t copy or print it out.” But, he says, the fundamental question is, “Do you really need to ask for it in the first place?”

For example, “Why do you need a copy of their driver’s license?” Hack asks rhetorically. “Because you want to see how old they are and discriminate on the basis of age? Because you want to see their race and commit race discrimination?” He’s being facetious to make a point, but it’s a real problem he sees across industries. “Does big data exist because there’s a reason for it,” he asks, “or does big data exist because it’s just too easy to collect it?”

Hack sums up his **recommendations for residential boards** as follows:

- Don’t collect protected data you don’t need. If you do not have it, it can’t be stolen from you.

- Have a formal written policy on data disposal—and then follow it. Securely destroy or delete data you no longer need in conformance with the policy. (You don’t want to be in a situation in which someone argues that you went out of your way to destroy data as part of a cover-up.)

- Distribute protected data ONLY on a need-to-know basis.
  Does every director really need to know the social security number of an applicant to buy a unit? Does every director need a copy of the tax return?

- Conduct a risk assessment of your business and determine your cybersecurity risks based on the nature of what you do, the nature of the data you collect, and the nature of your computer systems. Once you know the risks, take appropriate action to mitigate those risks.

- Put it in writing—you should have a written cybersecurity plan.

Breach Notifications

SHIELD specifically states that “Any person or business owning or licensing computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach...to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement … or any measures necessary to determine the scope of the breach and restore the integrity of the system.”

There is an exception if the exposure of private information happened because of “an inadvertent disclosure by persons authorized to access private information,” and it is reasonably determined that such exposure is not likely to result in misuse of the information, or in financial or emotional harm. However, such a determination must be documented in writing and retained for five years after the exposure. And if the exposure involves more than 500 people, the determination must be provided to the state attorney general within 10 days of its drafting.

The Consequences of Noncompliance

Violations of the SHIELD Act are under the authority of the attorney general, and can incur civil penalties of $5,000 per violation. The New York Law Journal points out that “The Act specifically states that its data security requirements create no private right of action for any violations.”

Failure to report a data breach under the previous laws was subject to penalties of $10 per instance of violation, up to a maximum of $150,000. The SHIELD Act doubles the penalty recoverable by the attorney general to $20 per instance of failed notification, and increases the maximum penalty recoverable to $250,000. The Act also increases the time within which the attorney general may bring an action from two years to three years.