

December 2017

## Cybersecurity and the Protection of Personally Identifiable Information: Are You Prepared?

*By David T. Podein, Esq.*



Cyberattacks and data breaches can occur with any personal or business computer connected to the internet—and there is no reason for condominium and homeowner associations (“community associations”) to believe they will fly under the radar of potential hackers.

In fact, community associations often are in possession of a significant amount of personally identifiable information (“PII”) and other sensitive information pertaining to their residents. Just think of the types of information on a tenant/resident application and a purchaser/new owner application: prior addresses, email addresses, birthdates, information about family members (including children), employment information, credit reports, bank/check account information (check for the application fee), copies of drivers’ licenses, and sometimes much more!

The Florida Information Protection Act (“FIPA”), which is codified in Florida Statute Section 501.171, is broad enough to apply to community associations and businesses alike. FIPA addresses the following key topics that directors and management teams should be aware of:

- “Personal information” includes an individual’s name with any one or more of the following data elements for that individual: social security number, driver’s license or similar number issued on a government document for identification, financial account number or credit card number, and/or any information regarding an individual’s medical history or diagnosis by a health care professional. Personal information also includes a user name or email address, in combination with a password or security question and answer that would permit access to an online account.
- “Breach of security” or “breach” means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Additionally, FIPA mandates strict reporting requirements in the event of a breach of security involving personal information. Depending on the nature and size of the breach of security, the party will have to report to the Florida Department of Legal Affairs, the individuals potentially affected, and/or credit reporting agencies.

A violation of FIPA shall be treated as an unfair or deceptive trade practice in any action brought by the Florida Department of Legal Affairs against the subject entity or third-party agent. There are also strict civil penalties for violations of FIPA: \$1,000 for each day up to the first 30 days following certain violations, and thereafter, \$50,000 for each subsequent 30-day period or portion thereof for up to 180 days. If the violation continues for more than 180 days, then the penalty may amount to but cannot exceed \$500,000. Many community associations outsource most of the management and recordkeeping functions to a licensed community association manager and/or

professional management company. It is essential that the board of directors, with the assistance of legal counsel and an insurance consultant, review and negotiate any contracts (management company, vendors, information technology, etc.) that involve protection of the association's official records (including residential information).

### Key Points to Consider

Have you and the association's legal counsel confirmed the scope of your management company's liability and indemnification duty to the association in the event the company's network suffers a cyberattack/breach of security of personal information? These issues should be considered during the contract bidding and negotiation process. Clearly drafted clauses in the management contract (and also for third-party vendors of the association handling data/personal information) should spell out the specific duties and responsibilities of the parties.

Does the association and/or management company have insurance coverage for these potential events, and if so, what are the coverage amounts and the scope of the coverage? Insurance coverages and exclusions involve complex issues that could fill an entire article. The insurance industry has been relatively quick to provide new insurance products in this area. Associations/directors should consult with their legal counsel and insurance consultant regarding both first-party and third-party coverages for breach of security incidents.

Does the association and/or management company have written cybersecurity policies and—of equal importance—is there a written emergency plan with specific steps, points of contact, emergency personnel, etc. for addressing a cyberattack/breach of security?

Do not assume the management company or other third-party vendor has these procedures in place. Request copies of their respective cybersecurity policies and emergency plans. Associations should consult with their information technology professionals and legal counsel when reviewing these items.

Cybersecurity and the protection of personally identifiable information will only increase in importance as more and more of the interactions and business between residents/owners and community associations move into the digital realm. Diligent

directors should seek out professional advice and consultation from information technology professionals, legal counsel, and insurance consultants to make informed decisions on these important issues.

“



## David T. Podein

Partner at Haber Slade

*David T. Podein is a partner at the law firm of Haber Slade. He concentrates his practice in the areas of real estate, financing/secured transactions, community association law, and construction law. David can be reached at [dpodein@dhaberlaw.com](mailto:dpodein@dhaberlaw.com). The author gratefully acknowledges the assistance of Haber Slade Paralegal Louis Goetz in connection with the preparation of this article. The firm is located on the internet at [www.haberslade.com](http://www.haberslade.com).*

”