THE GIARDINELLI LAW GROUP, A P C

Courtside Newsletter

Cybersecurity & the Real Estate Agent:

The Fallout of a Data Breach

BY: KELLY A. NEAVEL, ATTORNEY AT LAW
ASHLEY A. RICHARDSON, LAW CLERK
CASEY MCINTOSH, PARALEGAL

In a world where we are living most of our lives online, the threat of a cyberattack looms at every turn. As consumers, we often think of how this could impact us. Companies like Target and Equifax have been hacked, while credit and debit card fraud occurs far too often for comfort. This access to our personal information—names, Social Security numbers, birth dates, addresses and credit card numbers—feels like a violation of our sense of security and, ultimately, our trust.

With hackers attacking every 39 seconds, cybersecurity is not something to scoff at. According to Symantec's 2016 Internet Security Threat Report, 43% of cyberattacks target small to mid-size businesses, with one out of every forty businesses at risk of becoming a victim of cybercrime. Hackers love small businesses because the owners, generally, do not think they will be targeted. As a result, small business owners do not go out of their way to protect themselves. When they do, they usually do not have the resources to employ high-end protection like larger companies.

Real estate brokerages are not exempt from small-business targeting. As a matter of fact, according to the California Association of REALTORS® (C.A.R.), they are a prime target due to the high dollar transactions, multiple clients, and both the real estate professional and client not paying attention to details. Phishing scams, leading to wire fraud, are still one of the most common ways in which a real estate professional may become involved in a cybercrime. However, in 2017 the use of ransomware—malware that locks down a person's device and requires payment to a hacker in order to be released—increased exponentially among cyberattacks.

What Can You Do?

Real estate professionals need to protect themselves and their businesses. Last September, our firm issued a *Courtside Newsletter* entitled "Cybersecurity: How Can You Protect Yourself as a Real Estate Broker or Agent." That article can be found on our website (www.glawgroupapc.com), and the tips and tricks listed there are still relevant today. Some key takeaways are:

- Use of passphrases rather than passwords. Passphrases are typically stronger, easier to remember, and more difficult for hackers to guess. They contain a string of random words, 20-30 characters in total. This random word association can help a user remember the passphrase. Try Diceware for word suggestions, or just pick three random things in front of you to create a passphrase.
- Brokers and agents should have a strong data security plan. According the Federal Trade Commission's brochure entitled "Protecting Personal Information: A Guide for Business" states that the plan should contain five key parts:
  1. Take stock. Know what information you have in your files and on your computer.
  2. Scale down. Only gather the Personally Identifiable Information (PII) that your brokerage needs. (PII is defined under Civil Code § 1798.82(h).)
  3. Lock it. Keep PII limited to only the individuals who need it. Any hard copy forms and information should be kept in a locked file cabinet and only authorized individuals should have access to the key. Digital information should be kept on a locked computer or on an encrypted drive.

Continued …

4. Pitch it. California law requires a real estate broker to retain all documents obtained in connection with a real estate transaction for three (3) years. This retention period runs from the date of closing, or the date of the listing if the transaction is not consummated. (Business & Professions Code § 10148). After the expiration of this retention period, a broker should shred paper documents, erase electronic records and drives, or otherwise modify the personal information on any records to make it unreadable or undecipherable through any means. (Civil Code § 1798.81).
5. Plan ahead. Know what to do if a security breach does occur. Be prepared to respond quickly with security measures and incident response experts already in place. Come up with a plan on how to inform your employees and clients if a cyberattack occurs. A speedy response is key, and communication will stave off speculation that could have its own set of consequences.

Employee education and training should also be top priorities. The best security software in the world will not protect your business if an employee clicks on a suspicious link in an email because they have not received proper training. The old adages stand true: communication is key, knowledge is power, and prevention is the best medicine. By keeping employees apprised of trending scams and having annual training about identifying and avoiding scams, your company will better protected from cyberattacks.

Financial and Legal Ramifications of a Breach

Not only are security breaches a hassle, they also have financial and legal impacts on both the victims and the business owners. According to the Ponemon Institute, the price tag for the loss a business for a single attack is approximately $690,000. This estimate is derived from:

- Direct theft;
- Loss of confidential information;
- Notification costs (see below);
- Systems recovery;
- Size of the breach (the more records that were stolen, the higher the costs of the breach. According to the "2017 Cost of Data Breach Study: United States" the average cost per record for a breach was $225);
- Damage to reputation; and
- Lost business costs, including downtime and the loss of clients.

Statistics also show that of those businesses that are attacked, 60% go out of business within the following six months.

Unless they impede a criminal investigation, disclosures and notifications must be made in the "most expedient time possible and without unreasonable delay." Data breach disclosure requirements are codified in Civil Code § 1798.29. They must also conform to the format outlined in Civil Code § 1798.29(d). For any notification that is sent to more than 500 California residents, a sample copy of the notification must also be sent to the Attorney General. (Civil Code § 1798.29(e)).

Although they may not have seen the breach coming, real estate professionals may be held liable on theories of negligence, breach of contract, breach of fiduciary duty, and a failure to warn. REALTORS® may be found liable for further violations of the Code of Ethics. The information gleaned from a real estate professional's database could be seen as even more detrimental and could result in legal, monetary, and reputational damage.

Conclusion

While there is no way to guarantee you or your business will not become a victim of a cyberattack, implementing best practices increases your chances of avoiding them. Both C.A.R. and the National Association of REALTORS®'s websites contain a wealth of information regarding security measures for REALTORS®, including a "Data Security and Privacy Toolkit" and a Legal Q&A. The financial and legal fallout of a cyberattack should be incentive enough to budget security measures, including employee training, to protect your assets and your good