CNA

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW®

Law Firm Data Breaches: A Legal Snapshot

Introduction

By now, attorneys recognize that law firm data security has become a top concern for clients, regulatory agencies and state legislatures throughout the country. Countless firms have suffered data breaches, from solos to Big Law, but beyond the initial headlines, early settlements and sealed records have left a paucity of case law governing post-breach liability. As a result, many attorneys are left to wonder about the aftermath of a data breach and their potential exposure in an area of law that is rapidly evolving and far from settled.

State Data Breach Laws

Nearly every state, with the exception of only Alabama and South Dakota, has enacted a statute requiring notice of a data breach to affected individuals. While these laws share the same basic framework, they contain several differences as well. These often substantial variations, coupled with the requirement that a business comply with the statute of the state where each affected individual resides, means that avoiding regulatory fines following a breach is a burdensome process, particularly for multijurisdictional law firms.

A typical data breach statute will apply to any business or entity in the state that owns, licenses, or maintains certain classes of information. These categories always consist of social security numbers, driver's license numbers, and financial account numbers, but some statutes also include information related to medical conditions, health insurance coverage, or even biometric data like fingerprints or retinal scans. Although some law firms may not be considered a "covered entity" pursuant to the statutory definition—attorneys specializing criminal or juvenile representations, for example—most attorneys will necessarily maintain their clients' tax returns, medical reports, financial records, and other sensitive documents that subject them to their state breach statute.

Beyond varying definitions of covered entities and covered information, statutes may or may not contain exemptions for encrypted information, exceptions based upon compliance with federal laws such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach Bliley Act (GLBA), or requirements that an entity contact certain government agencies in addition to their affected clients. Perhaps the most important variation concerns whether the statute includes a harm threshold provision, which permits a business to circumvent notification requirements following a determination that the breach will likely not result in any harm to consumers. Even among state laws providing a harm threshold, statutes differ on whether this determination requires documented consultation with law enforcement.

Statutory penalties vary as well, and may be calculated based on the number of affected individuals, the number of days that notice was delayed, or may amount to one large fine per breach. In any event, civil penalties can quickly escalate to six figures and caps on the total penalty, where they exist at all, fall anywhere between $150,000 and $750,000. In addition to monetary penalties, the California and Connecticut statutes require entities to offer identity protection services to affected individuals for one year following a breach, and Delaware has approved a similar provision that will take effect in April of 2018.

Law firm data security has become a top concern for clients, regulatory agencies and state legislatures throughout the country.

Private Causes of Action

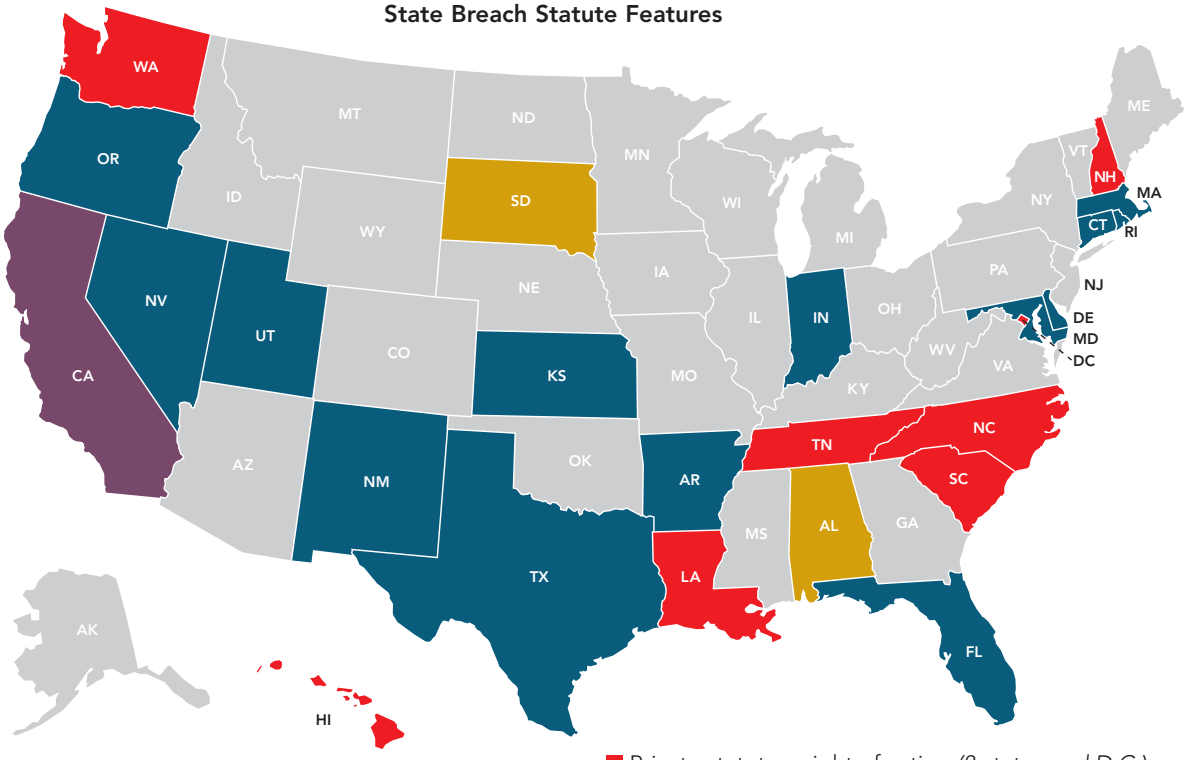
Apart from regulatory consequences, a law firm that suffers a data breach could face a civil action brought by an affected client. While the majority of state breach notification laws leave enforcement to the state attorney general, and either remain silent on private rights of action or outright prohibit them, eight states and the District of Columbia permit affected individuals to bring civil actions for actual damages resulting from a violation.

Even in jurisdictions without such provisions, an affected individual may bring a malpractice suit sounding in negligence and using the breach statute to establish the appropriate standard of care. At present, fifteen states[1] have enacted statutes that address breach prevention in addition to notice, and require businesses to implement and maintain reasonable data security measures. Four of these states[2] even mandate specific protocols with respect to storing, using, and transferring sensitive data.

In addition to the standards set forth in data breach laws, twenty-eight states[3] have amended their rules of professional conduct to include a duty of technological competence, first promulgated in 2012 by the American Bar Association's (ABA) addition of Comment 8 to its Rule 1.1. Additionally, thirty states[4] have adopted ABA Rule 1.6(c), which requires attorneys to make "reasonable efforts" to prevent unauthorized disclosure of confidential information. Although state ethics rules are primarily tools for attorney discipline, they are admissible in most jurisdictions as evidence of the relevant standard of care in malpractice litigation.

Attorneys might also be subject to litigation based upon an alleged breach of contract. Clients may cite language in the engagement letter promising confidentiality and discretion, or allege that an "implied contract" was created between the parties that charged the attorney with preventing unauthorized access to client data. Given the endless spate of high-profile data breaches, these types of claims will likely become more common as a greater number of clients, especially corporate clients, insist on specific contractual provisions addressing data security.

State Breach Statute Features



- Private statutory right of action *(8 states and D.C.)*
- Statutory duty to secure data *(15 states)*
- Both *(California only)*
- No statute *(Alabama & South Dakota)*

1 AR, CA, CT, DE, FL, IN, KS, MD, MA, NV, NM, OR, RI, TX, UT
2 CT, MA, NV, OR

3 AZ, AR, CO, CT, DE, FL, ID, IL, IA, KS, MA, MN, NE, NH, NM, NY, NC, ND, OH, OK, PA, TN, UT, VA, WA, WV, WI, WY
4 AK, AZ, AR, CO, CT, DE, FL, ID, IL, IA, KS, LA, MA, MI, MN, MO, NV, NH, NJ, NY, ND, OH, OR, PA, TN, UT, VA, WA, WV, WI

While the parameters of what constitutes "reasonable" data security have begun to crystallize in recent years, the more difficult hurdle for a client alleging malpractice related to a data breach is proving damages. Federal appellate courts continue to grapple with the concept of a data breach causing an "injury-in-fact" for standing purposes and are currently split on whether the real damage from a data breach—the risk of future identity theft—is too speculative.[5]

Where claims survive dismissal for lack of standing, the few courts that have proceeded to analyze the cause of action itself have found that the alleged harm could not form the basis of a negligence action.[6] A forensic analysis following a data breach can indicate what information was compromised, but unanswered questions regarding where the data ended up, who possesses it and for what purpose make successfully proving a claim a difficult prospect, at least based on current precedent.

5 Compare *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016); *Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688 (7th Cir. 2015); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (granting standing) with *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017); *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (denying standing).

6 *See Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 316CV00014GPCBLM, 2016 WL 6523428 (S.D. Cal. Nov. 3, 2016) (after finding standing, dismissing the plaintiff's negligence claim for failing to allege personal injury or property damage); *Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *9 (S.D.N.Y. June 25, 2010) ("Even assuming, *arguendo*, that Plaintiffs could be said to have standing, . . . Plaintiffs' alleged increased risk of identity theft is insufficient to support Plaintiffs› substantive claims.").

Conclusion

The threat of malpractice stemming from a data breach remains murky, but an attorney's duty to his or her clients to protect their data has never been clearer. Failing to employ reasonable data security protocols can place your firm in the crosshairs of government agencies and disciplinary authorities and, more importantly, jeopardize the security of your clients and reputation of your business.

This article was authored for the benefit of CNA by:
Matthew Fitterer

Matthew Fitterer is a Risk Control Representative for CNA's Lawyers Professional Liability Program. He is responsible for providing risk control guidance to CNA insureds in the form of written publications, online and live presentations, and direct consultations. Prior to joining CNA, Matt worked in the Chicago-area as an attorney for a small law firm specializing in criminal defense and civil rights litigation, and for a solo practitioner focusing on commercial litigation. Matt is licensed to practice law in Illinois and has been designated as a Commercial Lines Coverage Specialist (CLCS) by the National Underwriter Company.

CNA

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com.