PROFESSIONAL COUNSEL®

Advice and Insight into the Practice of Law®

Law Firm Data Breaches: A Legal Snapshot

Introduction

By now, attorneys recognize that data security has become a top concern for not just law firms themselves, but also 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

All 50 states, as well as Washington, D.C., Puerto Rico, Guam, and the U.S. Virgin Islands, have enacted statutes 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 in criminal or juvenile representations, for example – most attorneys 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,[1] 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. Law firms practicing internationally should also be mindful of any duties under foreign regulations, including the EU's General Data Protection Regulation (GDPR).

1 Encryption is the process of converting data into an un-readable or inaccessible format using a key or algorithm with the ultimate goal of protecting it from unauthorized access.

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, Connecticut, and Delaware statutes require entities to offer identity protection services to affected individuals for one year following a breach.

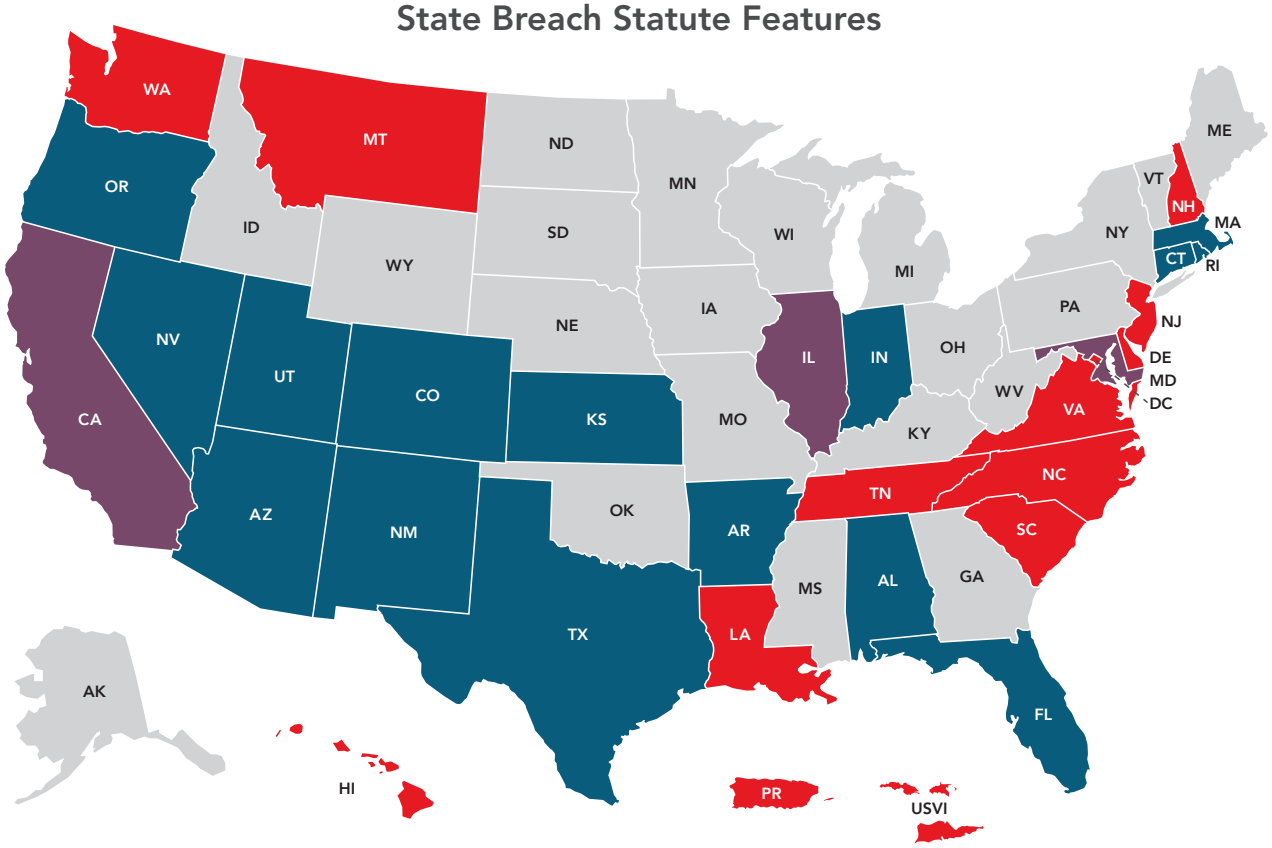
Private Causes of Action

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, nineteen states[2] 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[3] even mandate specific protocols with respect to storing, using, and transferring sensitive data.

Data security has become a top concern for not just law firms themselves, but also clients, regulatory agencies and state legislatures throughout the country.

State Breach Statute Features



- Private statutory cause of action (13 states + D.C., Puerto Rico, and U.S. Virgin Islands)
- Statutory duty to secure data (16 states)
- Both (3 states)

2 AL, AR, AZ, CA, CO, CT, DE, FL, IL, IN, KS, MD, MA, NV, NM, OR, RI, TX, UT
3 CT, NV, OR

In addition to the standards set forth in data breach laws, forty states[4] have adopted a statement addressing a duty of technological competence, mirroring language first promulgated in 2012 by the American Bar Association's (ABA) addition of Comment 8 to its Rule 1.1. Additionally, thirty-seven states[5] have adopted ABA Rule 1.6(c), which requires attorneys to make "reasonable efforts" to prevent unauthorized disclosure of confidential information.[6] 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.

While the parameters of what constitutes "reasonable" data security has 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.[7]

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.[8] 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.

Several recent examples of law firms being subject to litigation highlight the significant risk posted by data breaches, particularly when claims against law firms survive attempts at dismissal. In *Guo Wengui v. Clark Hill, PLC*, Clark Hill was retained to represent a prominent Chinese businessman and vocal political dissident in his asylum application.[9] The client warned the law firm that he was the target of sophisticated cyberattacks led by his native country and requested that the law firm take special precautions to protect his information by not storing his information on their servers.[10] The law firm agreed to do so as part of its engagement agreement, but failed to take those steps to protect his confidential information.[11] Within two weeks, the law firm's servers were hacked, resulting in the client's information being taken and disseminated, despite the client's warnings and their agreement.[12] The client sued the firm for damages related to lost business opportunities, increased vulnerability, and abandoning him during the course of his asylum petition.[13] Although the two parties later reached a settlement,[14] the law firm faced other repercussions which included significant time and financial expenditures, loss of attorney-client and work product privileges, and considerable negative media attention.

In *Hiscox Insurance v. Warden Grier LLP*, a small law firm which defended insureds on behalf of Hiscox was sued by the insurance company after it learned that the law firm suffered a data breach involving sensitive information related to Hiscox's insureds two years after the breach occurred.[15] During the intervening two years, the law firm failed to notify Hiscox of the breach or that its insureds' sensitive information had been compromised.[16] Hiscox only learned of the breach after an employee saw a social media post discussing the breach.[17] After conducting its own investigation into the breach and notifying its insureds, Hiscox filed suit alleging breach of fiduciary duty and breach of contract among other claims, and ultimately sought $1.5 million in damages stemming from the firm's delayed breach response.[18] Although the law firm ultimately escaped liability after receiving a favorable verdict following a jury trial, other courts and juries may have decided a case with similar facts differently. Further, the law firm nonetheless suffered other various adverse consequences, including the expenditure of significant time, resources, and money through discovery and trial, loss of a long time client, considerable unfavorable media coverage, and loss of reputation.

4 AK, AZ, AR, CO, CT, DE, FL, HI, ID, IL, IN, IA, KS, KY, LA, MA, MI, MN, MO, MT, NC, ND, NE, NH, NJ, NM, NY, OH, OK, PA, SC, TN, TX, UT, VA, VT, WA, WV, WI, WY

5 AK, AZ, AR, CO, CT, DE, FL, IA, ID, IL, KS, LA, MA, MI, MN, MO, MT,NC, ND, NH, NJ, NV, NY, OH, OK, OR, PA, SC, SD, TN, UT, VA, VT, WA, WI, WV, WY

6 The American Bar Association provides Jurisdictional Rules Comparison Charts on the Model Rules of Professional Conduct and the various jurisdictional modifications, which can be accessed here.

7 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).

8 *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.").

9 *Guo Wengui v. Clark Hill, PLC*, 440 F. Supp. 3d 30 (D.D.C. 2020).

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.*

14 *See* Kwok Ch. 11 Trustee Gets OK To Settle Retainer Dispute.

15 *Hiscox Ins. Co. v. Warden Grier, LLP*, 474 F. Supp. 3d 1004 (W.D. Missouri 2020).

16 *Id.*

17 *Id.*

18 *Id.*

A New York law firm was also recently the subject of a regulatory action with the New York Attorney General's Office in which it agreed to a $200,000 fine based on allegations that the firm maintained "poor data security measures" that made it vulnerable to a 2021 data breach which compromised sensitive information of more than 60,000 New York residents contrary to both state law and HIPAA requirements.[19] The settlement required the law firm to implement stronger cybersecurity protocols including encrypting certain information, updating its data collection and retention practices, and to maintain an information security program that is regularly updated with changes in technology and security threats.[20]

Conclusion

These cases cited above are just a few of the growing number of actions filed against law firms stemming from data beaches or cyber-attacks.[21] While the threat of malpractice stemming from a data breach continues to evolve, an attorney's duty to his or her clients to protect their data, and the potential exposure for not doing so, has never been clearer. Failing to employ reasonable data security protocols can place your firm in the crosshairs of government agencies, disciplinary authorities, or litigation and, more importantly, jeopardize the security of your clients and reputation of your business.

19 New York State Attorney General Press Release, March 27, 2023.
20 *Id.*
21 *See also Whalen et al v. Gunster, Yoakley & Steward*, No. 9:24-CV-80612 (S.D. Florida 2024); *In re Orrick, Herrington & Sutcliffe, LLP Data Breach Litigation*, 3:23-cv-04089 (N.D. California 2023); *In re Mondelez Data Breach Litigation*, 1:23-cv-03999 (N.D. Illinois 2023).

This article was authored for the benefit of CNA by:

Christopher Heredia

Christopher Heredia is a Risk Control Consulting Director for CNA's Lawyers Professional Liability Program. He is responsible for developing content for CNA's Risk Control services by providing guidance to CNA's insureds on risk control and professional responsibility-related issues. Prior to joining CNA, Chris was an attorney with Am Law 100 firm in Chicago where he focused his practice in legal ethics, law firm risk management, and commercial litigation. Prior to his time in private practice, Chris served in the public sector, first as an Assistant State's Attorney with the Cook County State's Attorney's Office in Chicago, and later as Litigation Counsel for the Illinois Attorney Registration and Disciplinary Commission where he worked to regulate the legal profession in Illinois. He is admitted to practice in Illinois, the U.S. District Court for the Northern District of Illinois, and the U.S. Supreme Court.

About CNA Professional Counsel

This publication offers advice and insights to help lawyers identify risk exposures associated with their practice. Written exclusively by the members of CNA's Lawyers Professional Liability Risk Control team, it offers details, tips and recommendations on important topics from client misconduct to wire transfer fraud.

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