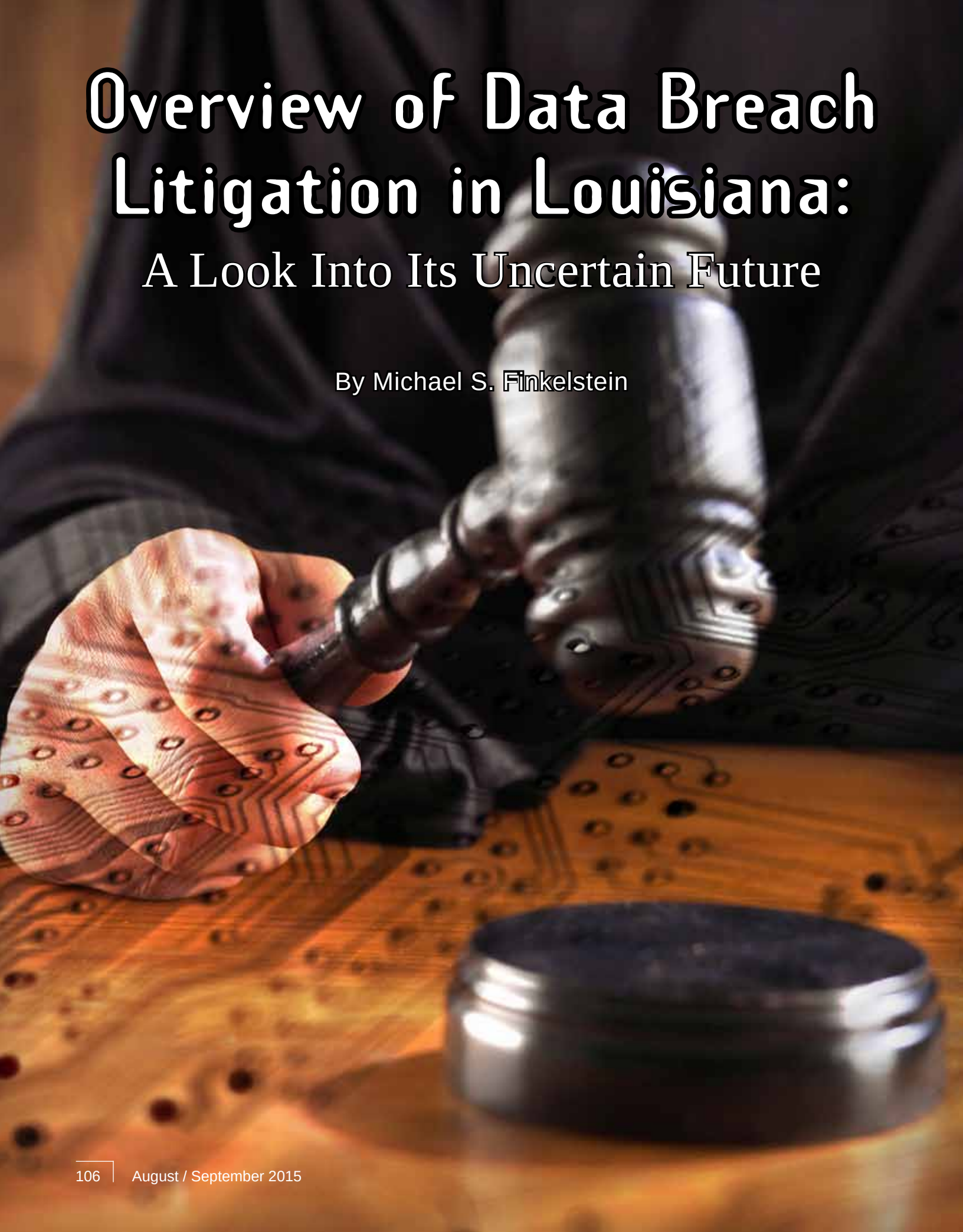
# Overview of Data Breach Litigation in Louisiana:

## A Look Into Its Uncertain Future

By Michael S. Finkelstein



Not often do entirely new practice areas emerge that span multiple fields of law. Such a phenomenon is occurring across America now as a new area of law sweeps the headlines of the nation's largest news providers and immediately captures the public's attention: Data Breach.


## Nuts and Bolts (and Bytes)

"Data breach" has been defined as an incident whereby an individual, application or service accesses, views or retrieves data, illegally or without authorization.[1] Data breaches are forms of a security breach specifically designed to steal data and publish that information in an unsecured location or utilize that information in an unauthorized manner. Affected information can include:

- personal identifiable information (PII, including information such as an individual's name, date of birth, Social Security number, credit/debit card numbers, account login credentials and driver's license numbers), responsible for 57.2 percent of data breach claims;[2]
- personal health information (PHI), responsible for 27.2 percent of data breach claims;
- trade secrets, responsible for 1.4 percent of data breach claims); or
- other information.[3]

After suffering a data breach, businesses or entities are required to notify affected individuals pursuant to the Louisiana Database Security Breach Notification Law, La. R.S. 51:3071 *et. seq*.

## Data Breach Notification Requirements

Recognizing the need to protect their citizens, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring that individuals be notified in the event of a security breach involving personal information.[4,5] Louisiana Revised Statutes Title 51, "Trade and Commerce," Chapter 51, "Database Security Breach Notification Law," lists the requisite responsibilities for businesses and the duty to notify consumers of a security breach.

The law provides that any person, business or agency that owns or licenses computerized data that includes an individual's personal information shall notify affected individuals of the breach when it is reasonably believed or discovered that the data was acquired by an unauthorized person.[6] The law defines "personal information" as the individual's name when combined with at least one of the following — Social Security number, driver's license number, account number, credit or debit card number, and any combination, access code or password that would allow access to the individual's financial account.[7]

Notification of the breach must be made in writing or electronically.[8] Additionally, notification "shall be made in the most expedient time possible and without unreasonable delay," subject only to the permissible delay of the business working with a law enforcement agency as a part of a criminal investigation.[9] An exception to the notice requirement is permitted so that no notice is required "if after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers."[10]

The Louisiana law also provides that a civil action may be brought to recover *actual damages* resulting from the failure to timely notify an affected person that there has been a data breach resulting in the disclosure of his/her personal information.[11] While the statute attempts to create a civil remedy for failure to notify in the event of a data breach, the law falls short of providing true teeth for that action.[12] The development of data breach case law in Louisiana and across the country has not been friendly to plaintiffs.

## Filing Suit for Data Breach

Having been notified that their information has been compromised, affected individuals can bring actions for data breach. While data breach law is in its infancy in Louisiana, claims have been made under the headings of negligence, emotional distress, loss of privacy, invasion of privacy, identity theft, fear of identity theft, harassment, nuisance, fear and anxiety, among others.[13] These claims are analyzed under theories of negligence by the courts, employing Louisiana's duty/risk analysis.[14]

In *Ponder*, the case of first impression in Louisiana, the court noted that courts across the country have dismissed complaints alleging damages in the form of charges for identity theft monitoring and credit protection based on a finding that those plaintiffs do not meet the threshold of actual damages or a cognizable loss. This holding is grounded in the idea that no injury is incurred when a plaintiff is in "anticipation of a future injury that has not materialized."[15] In *Clapper v. Amnesty Int'l*, the U.S. Supreme Court cemented the notion that plaintiffs incurring costs to protect confidential information, even those undertaking burdensome and costly measures, do not necessarily satisfy the Constitution's Article III Case or Controversy Requirement.[16]

Assuming, however, that the complaint can satisfy the standing requirement, the courts have denied plaintiffs' recovery under numerous theories. In the cases thus far brought before the courts in Louisiana, even when the plaintiffs' information had been compromised by exposure to a third party, their information had not yet been utilized to, for example, incur fraudulent charges. Unable to prove concrete damages, the courts have ruled that the plaintiffs have not sustained actual injuries, finding instead that their injuries were "purely speculative" and denying the plaintiffs' relief.[17] Courts have rejected claims of misrepresentation and fraud based on not being pled with particularity[18] or the plaintiff not causally relying on the defendant's misrepresentation.[19] As to plaintiffs' emotional distress claims, the courts have ruled that defendants will not be held liable for merely negligent conduct without an accompanying physical injury.[20] However, in *Melancon*, the court did recognize the possibility for a case to proceed where the plaintiffs' heightened risk for identity theft or charges for medical monitoring are recognized as cognizable injuries.[21]

## Data Breaches as Class Actions

The high barriers to establishing a meritorious action in court beg the question of how and whether data breach claims brought by individuals or as class action lawsuits will develop this area of the law. With massive amounts of information being stolen from corporate databases, data breach litigation is ripe for claims to be brought as class actions. Perhaps also the class action is the best vehicle to pursue these claims, as private attorneys have the additional incentive of developing cybersecurity law under the "Private Attorney General" theory.[22] Classes must satisfy the requirements of Rule 23 of the Federal Rules of Civil Procedure: numerosity, commonality, typicality, and that the class representatives fairly and adequately protect the interests of the class.[23] Due to the nature of the information typically stolen in data breaches, the class action requirements will likely be satisfied in the event of a breach. Given the recent retraction of the courts in certifying class actions,[24] however, it seems that this avenue will also present its own challenges.

## The Future of Data Breach Actions in Louisiana

Though the existing case law has not been favorable for plaintiffs seeking to bring an action for data breach, it is instructive on what prospective claims may look like.[25] In *Melancon*, the court sets forth several avenues for recovery, opening the possibility for a claim to proceed if an actual injury is incurred. Sustaining actual damages, such as fraudulent credit transactions, thus becomes a requirement for a plaintiff to maintain an action against the person or business that suffered the breach. Furthermore, "[i]n order to have suffered an actual injury, [a plaintiff] must have had an unreimbursed charge on [his] credit card."[26] When plaintiffs bring their contemplated action, they can include damages for future credit monitoring and identity theft monitoring, which will naturally follow from having actually suffered the fraud. But, with the possibility of PHI or trade secret information being stolen as a part of a data breach, the opportunity is open for the litigation to develop outside of the PII spectrum. Muddying the water for the courts is the fact that damages for disclosure of PHI would be far more speculative, as quantifiable damages cannot be easily determined.

While Louisiana courts have not yet arrived at a negligence analysis of a data breach claim, it can be expected to proceed similar to a recent analysis by the 11th Circuit applying Florida law.[27] As for the merits of a cognizable negligence claim under Louisiana law, the legal battle will likely proceed with plaintiffs asserting that the breach was preventable, and defendants countering that they acted reasonably to prevent the harm.

## Not All Businesses Are Created Equal

As a part of the debate regarding which standard will apply, the duties of diligence and competence carried by a large business will inevitably be far more onerous than those imposed on small businesses. As the law evolves in this area, the standard of "reasonableness" by which actions are measured will become more burdensome on large businesses due to their access to complex technology, or the idea that they can and should be using complex technology to safeguard their information. Smaller businesses, however, lacking access to the same complex technology, will be held to a far more lenient standard.

## A Heightened Risk: Attorneys and Susceptibility to Data Breach

Attorneys are prime targets for cyber attacks given that they often possess their clients' confidential and personal information. While all attorneys should be aware of the risks inherent in maintaining con-

fidential client information, attorneys in certain practice areas should be especially aware of the omnipresent threat posed by a data breach. Attorneys maintaining their clients' medical records or those attorneys possessing proprietary client information, such as pending patents, trade secrets or other similarly-sensitive information, should take extra steps to ensure that they have the proper technology and systems in place specifically designed to protect and safeguard their clients' information.

Under the Louisiana Rules of Professional Conduct, attorneys have a duty to provide competent representation to their clients, which includes safeguarding and protecting their confidential client information.[28] Competence in this area likely includes a duty on the attorney to understand, on some level, the technology being utilized in the representation. Attorneys should be aware of the capabilities and limitations of the services and devices they use and should exhibit caution when making decisions and implementing policies on where and how to store and access confidential information. With so great a risk of exposure stemming from a data breach lawsuit, how are attorneys and other businesses to respond when faced with an ever-present threat of liability? Just as they usually do: by purchasing insurance.

## The Evolving World of Cybersecurity Insurance

In addition to their regular business liability insurance and malpractice policies, attorneys possessing sensitive information and businesses of all kinds should make sure they are covered under a Data Breach/Cybersecurity Liability Insurance Policy. Over the past few years, insurance companies have started to specifically exclude electronic data loss from their traditional insurance policies, forcing businesses to purchase additional insurance specific to data security. These cybersecurity policies cover the costs of the data loss and can include hiring investigators, credit monitoring for affected individuals, and enlisting public relations professionals to help contain the damage done to the affected company's reputation.[29] With potential post-data-breach costs reaching millions of dollars per organization, paying a premium for a cybersecurity liability policy can be a crucial purchase to protect a business's bottom line.[30]

With the security of a data liability insurance policy in place, businesses can rest assured that their exposure is limited, while any data breach claims against them are handled efficiently under their insurance coverage. Similarly, these insurance policies incentivize plaintiff attorneys to pursue data breach claims, allowing for the further development of data security law in Louisiana.

## FOOTNOTES

1. Data breach, *www.techopedia.com/definition/13601/data-breach* (last visited July 22, 2015).

2. Aggregating the numbers from the *NetDiligence Study* for credit/debit card, financial and PII categories.

3. Mark Greisiger, *NetDiligence 2013 Cyber Liability & Data Breach Insurance Claims: A Study of Actual Claim Payouts* (2013), *www.netdiligence.com/files/CyberClaimsStudy-2013.pdf*.

4. Security Breach Notification Laws, *www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx* (last visited July 22, 2015).

5. Bills to establish a federal data breach notification standard have been proposed, though none have as yet passed through Congress. To date, there is no federal data breach notification standard.

6. La. R.S. 51:3074.

7. La. R.S. 51:3073.

8. *Id.*

9. *Id.*

10. La. R.S. 51:3074(G).

11. La. R.S. 51:3075.

12. Breaches may be subject to different standards depending on the nature of the compromised material. Breaches involving PHI-protected medical records implicate standards under HIPAA (Health Insurance Portability and Accountability Act of 1996; Pub. L. 104-191(F)(C)(1171)(4)) and HITECH (Health Information Technology for Economic and Clinical Health Act; 45 CFR 160.103), whereas breaches affecting the federal government are actionable under the Privacy Act of 1974 (5 U.S.C. § 552a).

13. Melancon et. al v. Louisiana Office of Student Financial Assistance, et al., Civil Action Nos. 07-7712, *c/w* 07-9158 567 F.Supp.2d 873 (E.D. La. 6/5/08); *see also*, Ponder v. Pfizer, Inc., 522 F.Supp.2d 793 (2007).

14. Melancon, *id.*; *citing* Mathieu v. Imperial Toy Corp., No. 94-C-0952 (La. 11/30/94) 646 So.2d 318, 321-22; *see also*, La. Civ.C. art. 2315, 2316.

15. Ponder, 522 F.Supp.2d at 797; *quoting* Forbes v. Wells Fargo Bank, N.A., 420 F.Supp.2d 1018 (D. Minn. 2006); *see also, e.g.* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7 Cir. 2007); Hendricks v. DSW Shoe Warehouse, Inc., 444 F.Supp.2d 775 (W.D. Mich. 2006); Kahle v. Litton Loan Servicing, L.P., 486 F.Supp.2d 705 (S.D. Ohio 2007).

16. Clapper v. Amnesty Int'l, 568 U.S. ____, 133 S.Ct. 1138 (2013).

17. *See, e.g.* Ponder, 522 F.Supp.2d at 797-98, *citing* Kahle v. Litton Loan Servicing L.P., 486 F.Supp.2d 705 (S.D. Ohio 2007).

18. Fed. R. Civ. P. 9(b) requires that fraud be alleged with particularity.

19. In re LinkedIn user Privacy Litigation, No. 5:12-CV-03088 EJD (N.D. Cal. 3/6/13).

20. Melancon, 567 F.Supp.2d at 874-75; *citing* Nesom v. Tri Hawk Int'l, 985 F.2d 208, 211 (5 Cir. 1993); Moresi v. State, Dept. of Wildlife & Fisheries, 567 So.2d 1081, 1095-96 (La. 1990); Rivera v. United Gas Pipeline Co., 697 So.2d 327, 328 (La. App. 5 Cir. 1997).

21. Melancon, 567 F.Supp.2d at 876; *citing* Arcilla v. Adidas Promotional Retail Operations, Inc., 488 F.Supp.2d 965, 972 (C.D. Cal. 2007); Bourgeois v. A.P. Green Indus., Inc., No. 97-C-3188 (La. 9/4/98), 716 So.2d 355.

22. Associated Industries of New York State v. Ickes, 134 F.2d 694, 704 (2 Cir. 1943) (Judge Jerome Frank, the first to recognize the "private attorney general" theory).

23. Fed. R. Civ. P. 23.

24. *See, e.g.*, Wal-Mart Stores, Inc. v. Dukes, et al., 564 U.S. ____, 131 S.Ct. 2541 (2011).

25. *See* Belle Chase Auto Care, Inc. v. Advanced Auto Parts, Inc., 2009 WL 799760 (E.D. La. 2009); Pinero v. Jackson Hewitt Tax Service, Inc., 594 F.Supp.2d 710, 2009 WL 43098 (E.D. La. 2009).

26. In re Barnes & Noble Pin Pad Litigation, No. 12-cv-8617 (N.D. Illinois 9/3/13).

27. Resnick v. AvMed, Inc., 693 F.3d 1317 (11 Cir. 2012).

28. Louisiana Attorney Rules of Professional Conduct, R. 1.1, 1.3, 1.6.

29. Dierdre Fernandes, "More firms buying insurance for data breaches," *The Boston Globe* (Feb. 17, 2014), *www.bostonglobe.com/business/2014/02/17/more-companies-buying-insurance-against-hackers-and-privacy-breaches/9qYrvlhskcoPEs5b4ch3PP/story.html*.

30. *NetDiligence 2013 Cyber Liability Study.*

*Michael S. Finkelstein is an attorney in the New Orleans firm of Wolfe, Begoun & Pick, L.L.C. He focuses his practice on plaintiff personal injury litigation, maritime law, FLSA claims, class actions, and Internet and cybersecurity law. A native of New Orleans, he received his BA degree in history and philosophy from Louisiana State University and his JD degree, along with a Diploma in Comparative Law, from LSU Paul M. Hebert Law Center. (mfinkelstein@wbplaw.com; www.wbplaw.com; Ste. 100, 818 Howard Ave., New Orleans, LA 70113)*