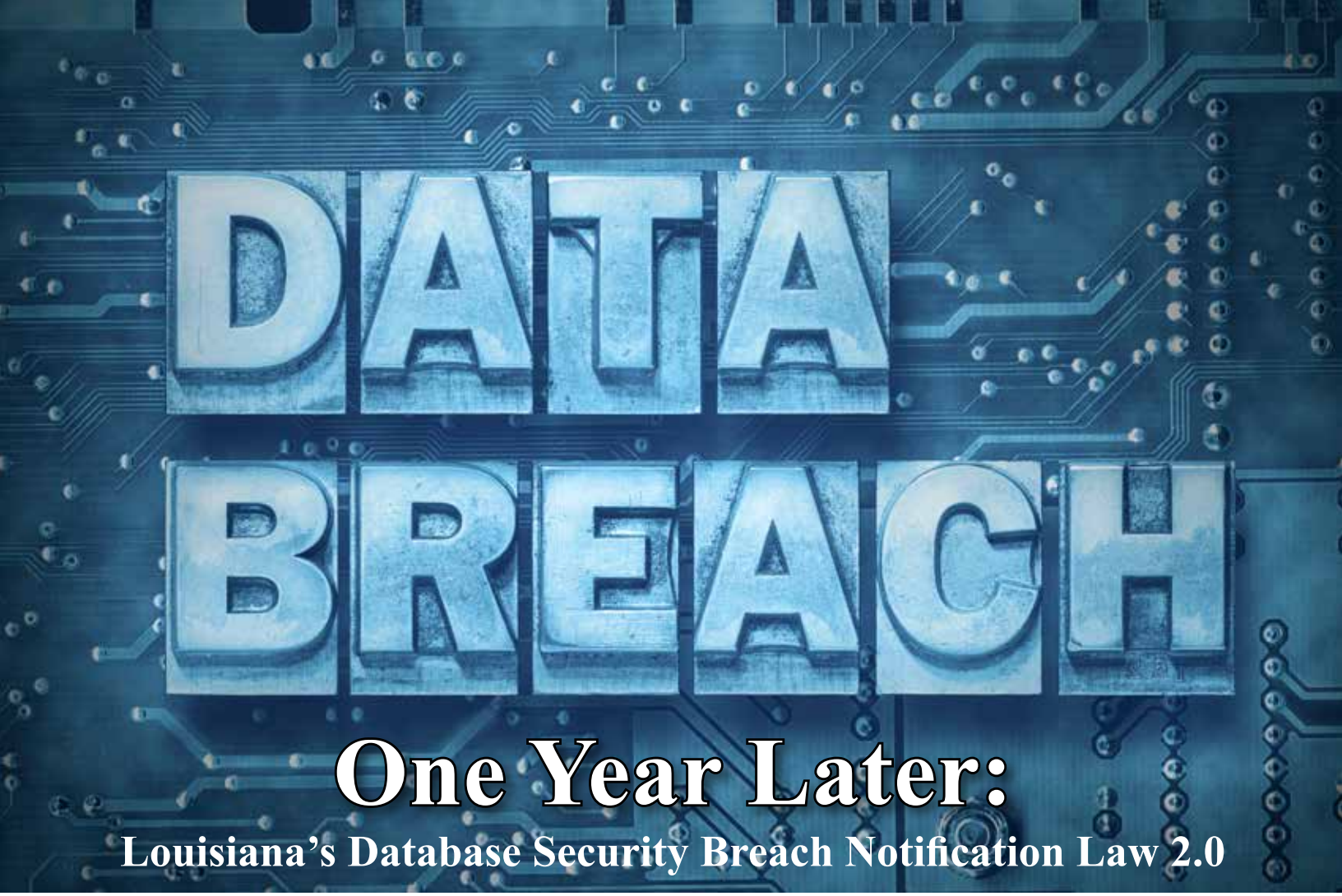

One Year Later:

Louisiana's Database Security Breach Notification Law 2.0

By Micah J. Fincher and Jessica C. Engler

Like the other 49 States, the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands, Louisiana has a data breach notification law.[1] First enacted in 2005, the Louisiana Legislature passed significant amendments to the law, which became effective on Aug. 1, 2018.[2] The amendments strengthened data protections for Louisiana residents by, among other things, adding affirmative obligations on businesses to safeguard personal information and setting a 60-day deadline for giving notice to individuals for most breaches. Left unchanged were deadlines to report breaches to the Consumer Protection Section of the Louisiana Attorney General's Office with regulations authorizing fines for tardy notices of up to $5,000 per day.[3] Further, while Louisiana's law had already created a private right of action for those harmed by untimely breach notifications,[4] the 2018 amendments deemed any violation of the law to be an unfair trade practice.[5] Yet despite expanded affirmative duties and enforcement rights, many businesses (including law firms) remain unaware of these changes. The one-year anniversary of the amendments merits a review first of the Louisiana's breach notification law as amended and then a discussion of enforcement of the amended law in the public and private sector.

"Personal Information"

The Louisiana breach notification law's definition of "personal information" is limited to certain information for individual Louisiana residents that is not encrypted or redacted.[6] Computerized data qualifies as "personal information" if it includes the Louisiana resident's last name and first name (or first initial) in combination with one or more of the following:

- Social security number;
- Driver's license number or state identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account;
- Passport number; or
- Biometric data, including fingerprints and other unique biological characteristics used to authenticate an individual's identity to access a system or account.[7]

The last two categories – passport numbers and biometric data – were added by the 2018 amendments. These additions are consistent with recent changes made to other states' data breach notification laws.

Protecting Personal Information

Among the most significant additions to the law, the 2018 amendments introduced affirmative obligations to protect personal information.[8] These obligations apply to all persons and legal entities that either conduct business in Louisiana or own or license computerized data that includes Louisiana residents' personal information.[9] They must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[10] When disposing of records containing personal information, they must destroy the records "by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means."[11] Both of these requirements are one of several "best practices" of data management that are now enshrined in Louisiana law. They apply regardless of whether the person or entity has suffered a breach.

No regulations or official guidance are currently available for interpreting these new obligations, including what constitutes "reasonable security procedures and practices."[12] The Louisiana Attorney General's Office has generally commented that the interpretation may be informed by the Federal Trade Commission's guidance and jurisprudence from state courts, but each complaint made to its office would be handled on a case-by-case basis.

The Trigger: What is a "Breach?"

A "breach of the security of the system" occurs when the "security, confidentiality, or integrity of computerized data" is compromised resulting in, or has "a reasonable likelihood to result in," the "unauthorized acquisition of and access to personal information."[13] In other words, for an event to constitute a "breach," it must be reasonably likely that a Louisiana resident's personal information was both acquired and accessed without authorization. The definition excludes good faith acquisition of personal information by a person's employee or agent "for the purposes of" the employer or principal, but only if the personal information is not used for, or subject to, unauthorized disclosure.[14]

No Harm Exception

The law includes a safe harbor when a breach results in "no reasonable likelihood of harm," such as when an event technically qualifies as a breach but it is contained in a manner that makes the likelihood of identity theft or other harm unlikely. Notice of a breach is not required if the person determines after a reasonable investigation that "there is no reasonable likelihood of harm" to Louisiana residents.[15] If a person relies on the safe harbor, then he/she must retain a copy of the determination, in writing and with supporting documentation, for five years from the date of discovery of the breach.[16] Upon request, they must provide a copy to the Louisiana Attorney General.[17]

Who Gives Notice?

Following discovery of a breach, the law requires any person that "owns or licenses computerized data that includes personal information" to notify Louisiana residents "whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[18] If a person who does not own the data suffers a breach, then the person must give notice of the breach to the owner or licensee of the data,[19] who in turn must notify the affected Louisiana residents.[20] This statutory scheme ensures that affected individuals have a single point of contact, *i.e.,* the data owner or licensee, regarding the breach.

Timing of Notice to Residents

Louisiana residents have the right to receive notice of security breaches of computerized data that include their personal information.[21] The amendments added a 60-day deadline for most breaches: notice must be made "in the most expedient time possible and without unreasonable delay but not later than 60 days from the discovery of the breach."[22] The law permits delays in giving notice at the request of law enforcement or "to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system."[23] But if a person relies on either of those grounds to delay notice, the Louisiana Attorney General must be notified of the reasons for such delay within the 60-day period from discovery of the breach.[24] If additional time to provide notification is required, the Attorney General "shall allow a reasonable extension of time."[25] The law does not specify the contents of the notice to residents.

Form of Notice to Residents

When a person's system is breached, the law provides four ways to notify affected Louisiana residents. First, if the person maintains an information security policy for the treatment of personal information and that policy includes notification procedures, then he/she may provide notice in accordance with its policy and procedures.[26] The procedure, of course, must otherwise comply with the timing requirements of the law,[27] but the law does not require that the procedure specify the medium through which the notice is given (*e.g.*, the procedure may permit notice via email, telephone, etc.). Second, notice may be made by written notification.[28] Third, the law authorizes electronic notification in accordance with the Electronic Signatures Act (the ESA).[29] Because the ESA requires affirmative, informed consent in advance of the electronic notice,[30] such notice is often not a viable option. Fourth, the law permits "substitute notification" in circumstances where other means of notification would be burdensome or impossible, namely, sufficient contact information is not available, the cost of providing other means of notice would exceed $100,000, or the number of persons to be notified exceeds 100,000.[31] Substitute notice requires the person to give notice in three ways: by email, if available; by a conspicuous posting on the person's Internet site, if an Internet site is maintained; and by major statewide media.[32]

Notice to Attorney General

Regulations promulgated by the Office of the Attorney General also require notice to the Attorney General's Consumer Protection Section.[33] Under the regulations, if notice to "Louisiana citizens"[34] is required under the law, then "within 10 days of distribution" of such notice, the Attorney General must also receive written notice.[35] Failure to provide timely notice to the Attorney General may result in a fine of up to $5,000 per day.[36] The written notice to the Attorney General must include the names of all Louisiana citizens affected by the breach and detail the breach of the security of the system,[37] including the date of the breach, the date of discovery of the breach and the date of notice to Louisiana residents.

Private Enforcement

A person who suffered damages as a result of violations of Louisiana's breach notification law may bring a civil action against the violator. The law permits civil actions "to recover actual damages resulting from the failure to disclose in a timely manner" that there was "a breach of the security system resulting in the disclosure of a person's personal information."[38] Louisiana's Unfair Trade Practices and Consumer Protection Law[39] also permits plaintiffs to recover "actual damages" for any "unfair or deceptive method, act, or practice declared unlawful by" the law.[40] In a change that expands the grounds for actions by the Attorney General and private plaintiffs for violations of Louisiana's breach notification law, the 2018 amendments provide that a violation of the law "shall constitute an unfair act or practice pursuant to" Louisiana's Unfair Trade Practices and Consumer Protection Law.[41]

Exemption for Financial Institutions

The law includes a limited safe harbor for financial institutions. In 2005, federal regulators published "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice."[42] A financial institution that is subject to and in compliance with such federal interagency guidance, as amended, "shall be deemed to be in compliance with" the law.[43]

Enforcement Update

The 2018 amendments clarified the Louisiana Attorney General's authority to hold businesses accountable when they violate Louisiana's breach notification law. Yet, as of the submission date of this article, the Attorney General has not used the new law to take action against any Louisiana entities. The Attorney General's Office has, however, joined with other state attorneys general to bring cases involving multi-state breaches.[44]

There has also been limited activity in civil litigation. This may be because, even in cases involving clear violations of breach notification laws, claimants have historically had difficulty in proving the existence of actual damages specifically caused by such breaches. In past cases, Louisiana courts (like many other state and federal courts) have required data breach claimants to allege a nonspeculative, actual injury to establish legal standing.[45] Many courts, including Louisiana, have held that theft of personal information alone, leading to merely an increased *risk* of identity theft and subsequent emotional distress, does not constitute actual damages.[46] And because an individual claimant's information may have been compromised in multiple breach events, it may be difficult to prove that any single breach is causally linked to any specific instance of identity theft. As a result, even if a claimant is successful in proving that the entity was noncompliant with the law's data management obligations, the claim may still ultimately fail if the noncompliance did not cause the breach. Finally, the amended law includes no indication from the Legislature that the obligations may be applied retroactively; thus, it is unlikely that breaches or noncompliance that occurred prior to the effective date can establish a cause of action under the amended statute.

Despite the limited enforcement activity to date, we anticipate greater scrutiny of Louisiana businesses' statutory obligations to secure personal information, before and after breaches occur. To the extent that a business has not reviewed its data security practices since the 2018 amendments became effective, undertaking that exercise has become a necessary cost of doing business in Louisiana.

FOOTNOTES

1. *See* La. R.S. § 51:3071, *et seq*.
2. La. Act No. 382 (2018).
3. La. Admin. Code title 16, pt. III, § 701.
4. La. R.S. § 51:3075.
5. *Id.* § 51:3074(J).

6. *Id.* § 51:3073(4)(a). The definition of "personal information" excludes "publicly available information that is lawfully made available to the general public from federal, state, or local government records." *Id.* § 51:3073(4)(b).

7. *Id.* § 51:3073(4)(a).

8. *See* La. R.S. § 51:3074(A),(B) (2019).

9. *Id.* § 51:3074(A). Also, as noted above, the definition of "personal information" under section 3073(4)(a) is limited to Louisiana residents.

10. *Id.* § 51:3074(A).

11. *Id.* § 51:3074(B).

12. Other states that require persons to affirmatively protect personal information have created detailed guidance for compliance. For example, Massachusetts requires a comprehensive information security program, risk assessments, security policies for employees, overseeing outside service providers, securing user authentication protocols for computer access, encryption of personal information traveling across public networks, reasonable monitoring systems, etc. *See generally* 201 Mass. Code Regs. 17.00 (2019).

13. *Id.* § 51:3703(2).

14. *Id.*

15. La. R.S. § 51:3004(I) (2019).

16. *Id*.

17. *Id*.

18. *Id.* § 51:3074(C).

19. *Id.* § 51:3074(D).

20. *Id.* § 51:3074(C).

21. *Id.* § 51:3074(C).

22. *Id.* § 51:3074(E).

23. *Id.* § 51:3074(E),(F).

24. *Id.* § 51:3074(E).

25. *Id*.

26. *Id.* § 51:3074(H).

27. La. R.S. § 51:3074(H) (2019); *see also Id.* § 51:3074(E).

28. *Id.* § 51:3074(G)(1).

29. *Id.* § 51:3074(G)(2); *see also* 15 U.S.C. § 7001 (2019).

30. *See id.* § 7001(c)(1).

31. La. R.S. § 51:3074(G)(3) (2019).

32. *Id.* § 51:3074(G)(3)(a)-(c).

33. La. Admin. Code title 16, pt. III, § 701 (2019).

34. While the law requires notice to Louisiana "residents," *see* La. R.S. § 51:3074(C) (2019), the regulations require notice to the Attorney General "[w]hen notice to Louisiana *citizens* is required pursuant to R.S. 51:3074." La. Admin. Code title 16, pt. III, § 701(A) (2019).(A) (*emphasis added*).

35. *Id.*§ 701(B).

36. *Id*.

37. *Id.* § 701(A).

38. La. R.S. § 51:3075 (2019).

39. *Id.* § 51:1401, *et seq.*

40. *Id.* § 51:1409.

41. *Id.* §§ 51:3074(J), 51:1405(A).

42. *See* 70 Fed. Reg. 15736 (Mar. 29, 2005).

43. La. R.S. § 51:3076 (2019).

44. *See e.g.,* Allison Grande, "States Secure $900K Deal in First Coordinated HIPAA Suit," Law360 (May 29, 2019, 9:16 PM EDT), *www.law360.com/articles/1163999/states-secure-900k-deal-in-first-coordinated-hipaa-suit*; Press Release, Louisiana Department of Justice, Settlement with Uber over Data Breach Announced by Attorney General Jeff Landry (Sept. 27, 2018) (available at *www.ag.state.la.us/Article/9602/5*).

45. *See, e.g.,* Bradix v. Advance Stores Co., Inc., 17-0166 (La. App. 4 Cir. 8/16/17), 226 So.3d 523, 528 (affirming exception of no right of action because, among other things, plaintiff failed to allege that someone successfully stole his identity).

46. *See id.*; *see also,* Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793 (M.D. La. 2007); Melancon v. La. Office of Student Fin. Assistance, 567 F. Supp. 2d 873 (E.D. La. 2008).

Micah J. Fincher is an associate and registered patent attorney in the New Orleans office of Jones Walker LLP. He focuses his practice on data security and privacy, intellectual property and financial services regulation. (mfincher@joneswalker.com; Ste. 5100, 201 St. Charles Ave., New Orleans, LA 70170)

Jessica C. Engler, CIPP/US, is an associate and registered patent attorney in the New Orleans office of Kean Miller LLP. She focuses her practice on data security and privacy, intellectual property and construction litigation. (jessica.engler@keanmiller.com; Ste. 3600, 909 Poydras St., New Orleans, LA 70112)