ARTICLE: CYBERSECURITY AND LOUISIANA'S DATABASE SECURITY BREACH NOTIFICATION LAW

By Nick S. Wise

Last year, the number of reported data breaches suffered by U.S. companies and government agencies increased by 40 percent from 2015.[1] One of the more well-known data breaches was revealed last September when Yahoo announced that hackers acquired the accounts of at least 500 million of its users from an attack that occurred in 2014.[2] The stolen user information included names, email addresses, telephone numbers, birth dates, encrypted passwords, and security questions.[3] A few months later, Yahoo announced the discovery of yet another data breach that occurred in August 2013 which may have resulted in the compromise of more than one billion user accounts.[4]

The costs that result from data breaches—not to mention the damage to a company's reputation—are no trivial matter. In 2016, the average cost of a data breach in the U.S. increased from approximately $217 per record to approximately $221 per record with the average total cost of a breach increasing from $6.53 million to approximately $7.01 million.[5] One such cost is the requirement under state and/or federal law to notify the affected individuals that their personal information has been compromised. Such laws are commonly referred to as data breach notification laws. California was the first state to pass such a law in 2002. Cal. Civ. Code § 1798.82. Many states soon followed California's model, including Louisiana, who enacted its own data breach notification law in 2005. These laws essentially require companies and state agencies to notify the individuals affected by a data breach after the breach is discovered.

LOUISIANA'S DATABASE SECURITY BREACH NOTIFICATION LAW

Louisiana's data breach notification law, La. R.S. 51:3071, *et seq.*, aptly named the "Database Security Breach Notification Law," is similar to the notification laws of other states. The Louisiana legislature enacted the law upon finding that the privacy and financial security of individuals are increasingly at risk due to the wide collection of personal information and that victims of identity theft must be notified so that they may act quickly to minimize the damage resulting from such crimes. La. R.S. 51:3072. The law applies to any person (statutorily defined as an individual, corporation, or other legal entity) that conducts business in Louisiana or that owns or licenses computerized data that includes personal information of a resident of the state.

---

1 Olga Kharif, *2016 Was a Record Year for Data Breaches*, Bloomberg (May 15, 2017, 10:00 AM), *https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked.*

2 Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, The New York Times (May 15, 2017, 10:30 AM), *https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html*.

3 *Id.*

4 Vindu Goel and Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, The New York Times, (May 15, 2017, 10:45 AM), *https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0*.

5 Ponemon Institute, LLC, 2016 Cost of Data Breach Study: United States, June 2016. *https://www.ibm.com/security/data-breach/.*

La. R.S. 51:3074. The law also applies to any Louisiana State agency that either owns or licenses such data. *Id*.

The notice requirement of the law is triggered upon the discovery of a "breach in the security of the system" containing computerized data that includes "personal information" that was, or is reasonably believed to have been, acquired by an unauthorized person. *Id*. Once such a breach is discovered, the person or agency who suffered the breach must notify the affected individuals "in the most expedient time possible and without unreasonable delay." However, notification is not required if the person or agency determines there is no reasonable likelihood of harm to customers after a reasonable investigation. *Id*.

The statute also imposes a requirement on any agency and person who maintains computerized data that includes personal information that is *not* owned by the agency or person to notify the owner or licensee of the information if the personal information was compromised through a security breach. *Id*.

PERSONAL INFORMATION

Notification is required only if the compromised computer data includes "personal information," which has a specific meaning under the statute. Personal information is defined as an individual's first name or first initial and last name with at least one of the following data elements: 1) social security number; 2) driver's license number; or 3) "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." La. R.S. 51:3073. Such information is only considered "personal information" under the statute when the name or data element is not encrypted or redacted. The statute also excludes information that is lawfully made available to the general public from government records. *Id*.

PROVIDING NOTICE

Once a security breach that compromises personal information is discovered, the person, business, or

agency who suffered the security breach must notify Louisiana residents whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. La. R.S. 51:3074. Notification may be provided by written notification or electronic notification. The statute also allows for "substitute notification" if certain conditions are met. Substitute notification includes email notification, conspicuous posting of the notification on the website of agency or person, and notification to major statewide media. A person or agency may only avail itself of one of the methods of substitute notification if the agency or person demonstrates that the cost of notification would exceed $250,000, the affected individuals to be notified exceeds 500,000, or the agency or person does not have sufficient contact information of the affected individuals. The statute also prescribes that notification must be made in the "most expedient time possible and without unreasonable delay," however, law enforcement has the power to delay the notification if it determines that notification would impede a criminal investigation. *Id*.

Not only must a person or agency notify the individuals affected by the data breach, but the person or agency must also notify the Louisiana Attorney General. Under La. Admin Code. tit. 16, pt. III, § 701, written notice detailing the breach of the security system, including the names of all Louisiana citizens affected by the breach, must be provided to the Consumer Protection Section of the Attorney General's Office whenever notice is required under the statute. Failure to provide timely notice may be punishable by a fine not to exceed $5,000 per violation. Notice is timely if it is received within 10 days of distribution of the notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation. *Id*.

RECOVERY OF DAMAGES BY AFFECTED INDIVIDUALS

Louisiana's Database Security Breach Notification Law also provides for a civil action to recover damages resulting from a person or agency's failure to notify the affected individuals in a timely manner. La. R.S. 51:3075. Thus far, causes of action brought under the statute have tended to be unsuccessful due to the plaintiffs' inability to show they suffered any actual damages as a result of the data breach.

In *Ponder v. Pfizer, Inc.*, Pfizer discovered a data breach that compromised the personal information of approximately 17,000 former and current employees. 522 F. Supp. 2d 793, 794 (M.D. La. 2007). The data was stored on a Pfizer laptop computer and was exposed to individuals outside the company through an unauthorized file-sharing software installed on the laptop. An investigation revealed "that certain files containing [employee] data were accessed and copied." *Id*. at 794. On June 1, 2007, Pfizer notified the affected employees of the breach via written letter which included details of the breach and steps that Pfizer had taken to protect the privacy and security of employees. *Id*. at 794. The letter further advised employees to monitor account statements and credit reports for unusual activity. *Id*. at 795. One of the affected employees filed a class action alleging general claims of negligence and violation of Louisiana's Database Security Breach Notification Law. *Id*. at 795. Specifically, the complaint alleged that nine weeks elapsed between the unauthorized disclosures and the notification to plaintiff and that this was not a timely manner under the statute. *Id*. at 796. The damages claimed included "fear and apprehension of fraud, loss of money, and identity theft; the burden and the cost of credit monitoring; the burden and the cost of closing compromised credit accounts and opening new accounts; the burden of scrutinizing credit card statements and other statements for unauthorized transactions; damage to their credit; loss of privacy and other economic damages." *Id*. at 795.

Pfizer filed a motion under Fed. R. Civ. P. 12(b)(6) to dismiss the complaint. The court found that the plaintiff's complaint did not allege that his personal information was actually used by an unauthorized person or that any money had been taken unlawfully from his accounts, but it merely alleged that the plaintiff had the burden of monitoring and bearing the cost if his personal information was used in an illicit manner. *Id*. at 796. The district court recognized this issue was one of first impression in Louisiana and, considering case law from other jurisdictions, held that the complaint failed to allege that plaintiff suffered any actual damages on the ground that the plaintiff was unable to allege an unauthorized individual used his personal information to his detriment. *Id*. at 798.

Similarly, in *Pinero v. Jackson Hewitt Tax Service Inc.*, the plaintiff brought an action against Jackson Hewitt alleging negligent mishandling of her confidential personal information and violations under the Louisiana Database Security Breach Notification Law. 594 F. Supp. 2d 710, 714 (E.D. La. 2009). The district court dismissed the plaintiff's claims for failure to allege any cognizable damages suffered from any breach. Instead, the damages asserted were based on the speculative future injury of identity theft. *Id*. at 717. The court also dismissed the plaintiff's claim under the Louisiana Database Security Breach Notification law because the plaintiff's personal information was not compromised as a result of a *computer* breach as required by the statute but rather as a result of improper disposal of paper records. *Id*. at 717.

CYBERSECURITY INSURANCE

Because a data breach can have a significant negative impact on a business's bottom line, businesses of all sizes should consider securing insurance policies to mitigate these risks. Some traditional commercial policies provide coverage for costs associated with data breaches while others specifically exclude such coverage.[6] Therefore, businesses should not assume that their general commercial policies cover injuries resulting from data breaches but instead should closely review their policies to confirm whether or not they are covered for such harm. If a business determines its general commercial policy does not cover data breaches, then it should consider obtaining additional coverage through a cyber insurance policy that specifically covers data breaches and other cybersecurity risks. Cyber insurance may provide coverage for the following types of expenses associated with a data breach: computer forensics; privacy or security breach notification and response; crisis management; and data loss or destruction.[7] This coverage may also include costs associated with complying with data breach notification laws. The policies may also cover legal expenses and liability in the event of litigation. Because a data breach can remain undetected for years, the applicant may want to obtain retroactive coverage for such undetected events.[8]

---

[6] Judy Selby, Cyber Insurance: Insuring for Data Breach Risk, Practical Law Practice Note 2-588-8785.

[7] *Id.*

[8] *Id.*