

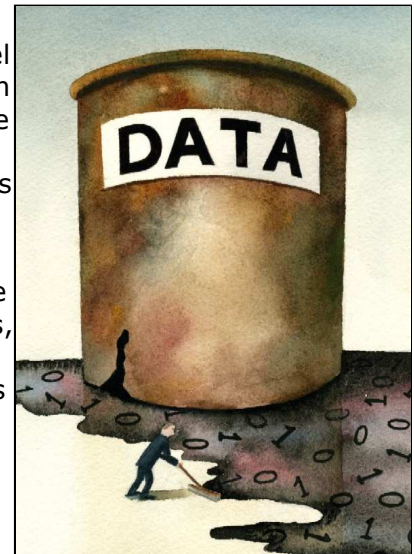
It's Not the Breach, It's the Cover-Up Using Digital Forensics to Mitigate Losses and Comply With Florida's Data Breach Notification Statute

by Dana J. Lesemann

Page 20

- *Replacing a stolen laptop: \$2,000.*
- *Violating Florida's Data Breach Notification Statute: Administrative fines up to \$500,000.*
- *Knowing how to protect yourself and your clients: Priceless.*

Everyone knows a story about a lost laptop or personal digital assistant (PDA) — the one that was left on the airplane or in the hotel room, or stolen out of a car. When employees lose equipment, it is an annoyance. But as of July 1, 2005, when Florida's data breach statute went into effect, if that lost laptop or PDA contains unencrypted personal information about Florida employees, customers, or business associates, the company may have to notify every Florida resident whose data was compromised.¹ Moreover, most companies have customers or advertise in more than one state. If they have an online presence, they could have customers or contacts in every state. Thus, it is incumbent on attorneys and their clients to become familiar with the data breach statutes not just in Florida, but in the other 36 states and the District of Columbia where data breach laws have been enacted — each potentially subjecting companies to financial penalties.²



Florida's data breach statute was passed as part of a wave of similar laws that has been sweeping the country.³ This data breach fever started on the West Coast after California's state Web site, which contained the Social Security numbers and other personal information of more than 250,000 state employees, was compromised in 2002. The state controller failed to notify affected employees.⁴ This breach — and the way it was handled — led to the enactment of the first data breach notification statute by the California Legislature later in 2002.⁵

In February 2005, Choicepoint, a commercial data broker, announced that it had unwittingly sold personal information regarding 145,000 individuals to a group of individuals engaged in identity theft. The company later said the breach in September had been uncovered in 2004 — five months before it had alerted the victims in California pursuant to the California statute. Victims in other states were left out of the notice since no legal mandate required notification. This strict compliance with the letter of the law was a public relations nightmare for Choicepoint when non-California victims found out they had been omitted from the notice. Other states addressed the omission by stepping up to ensure their residents enjoyed protections similar to those created by the California Legislature.⁶ A flood of similar disclosures soon followed,⁷ which triggered more data breach statutes.

An Overview of Data Breach Statutes⁸

- *Personal Information* — Florida, like most states, modeled its data breach statute, H.B. 481, after California's 2002 groundbreaking law, requiring notification to individuals if, as the result of a breach in a company's computer security, an individual's "personal information" is compromised.⁹

Florida, like California, defines “personal information” as a person’s first name or initial and last name in combination with any one of the following pieces of data when either the name or the data is unencrypted:

- Social Security number;
- Driver’s license 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 allow access to an individual’s financial account.¹⁰

Personal information does not include publicly available information that is available to the general public through federal, state, or local government records.¹¹ Florida’s new law requires that anyone conducting business in Florida and maintaining Florida residents’ unencrypted personal information on a computer system must notify those residents if that information has been “materially compromised.”¹²

The definition of “personal information” in the Connecticut,¹³ Delaware,¹⁴ Illinois,¹⁵ Louisiana,¹⁶ Minnesota,¹⁷ Montana,¹⁸ Nevada,¹⁹ New Jersey,²⁰ Rhode Island,²¹ Tennessee,²² Texas,²³ and Washington²⁴ statutes tracks the language in California and Florida. Other states include additional elements in the definition of “personal information”: The Arkansas²⁵ data breach notification statute encompasses medical information; Georgia²⁶ and Maine²⁷ include account passwords or other personal identification numbers or access codes and any items that, even without the first and last name, could put an individual at risk of identity theft. North Dakota expands on the California model to include an employer’s identification number, date of birth, mother’s maiden name, and digital signature or other electronic information.²⁸

New York, on the other hand takes a different approach. The statute simply — and sweepingly — defines personal information as “*any information* concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person,” plus the individual’s Social Security number, driver’s license number (or nondriver identification card number), account number, credit or debit card number, PIN, or other necessary code.²⁹

It is also worth noting that the data breach statutes in Hawaii,³⁰ Indiana,³¹ North Carolina,³² Massachusetts,³³ and Wisconsin³⁴ include written as well as electronic data within the scope of their notification requirements.

- *Breach of the Security System* — The Florida statute defines a “breach” of the security system as an “unlawful and unauthorized acquisition” of data that “materially compromises the security, confidentiality, or integrity of personal information.”³⁵ The statute provides little clarity, however, about what constitutes a breach that “materially compromise[s]” personal information. The relative gravity or “materiality” of a breach is not a function of the number of records or individuals whose personal information is compromised or whether any actual injury has occurred, but of whether any compromised record contains personally identifiable information. Thus, a breach of a system that contains “personal information” appears to be a *prima facie* case of a “material” breach.³⁶ For example, an ex-boyfriend who hacks into a computer system and targets the personal information of only his former girlfriend has effected a “material breach” of that system.

The Florida definition of a security breach is different from the California model in one significant way: California omits the term “material,” defining a breach simply as an “unauthorized acquisition

of computerized data that compromises the security, confidentiality, or integrity of personal information.”³⁷ Nineteen states and the District of Columbia follow the California model.³⁸ Arizona,³⁹ Idaho,⁴⁰ Nevada,⁴¹ Oregon,⁴² and Tennessee,⁴³ like Florida, define a breach as one that “materially” compromises personal information. However, in these statutes, as in Florida’s, “materiality” is undefined.⁴⁴ Connecticut,⁴⁵ Indiana,⁴⁶ and North Dakota⁴⁷ do not mention materiality or injury to consumers, defining a security breach only as “unauthorized access to” or “acquisition of” computerized data.

Louisiana,⁴⁸ Hawaii,⁴⁹ Massachusetts,⁵⁰ Montana,⁵¹ New York, North Carolina,⁵² Ohio,⁵³ Pennsylvania,⁵⁴ and Wyoming⁵⁵ take a different tack, incorporating the prospect of injury to the consumer into the definition of a security breach. For example, Massachusetts defines “breach of the security system” as:

the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency *that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.*⁵⁶

New York lists specific factors that an organization may consider in determining whether consumers’ personal information has been acquired or is reasonably believed to have been acquired by an unauthorized individual including indications: 1) that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device; 2) that the information has been downloaded or copied; or 3) that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft.⁵⁷ In Vermont, notice is not required if the company establishes that misuse of the consumers’ personal information is not reasonably possible. However, the company is also required to provide notice of that determination and a detailed explanation for that determination to the Vermont attorney general or other relevant licensing agency.⁵⁸ In light of these and similar requirements in other states, as discussed below, companies seeking to determine whether consumers were injured or put at risk from a data breach would be wise to turn to outside experts in digital forensics to conduct the type of investigation and documentation that this type of inquiry requires.

- *Investigating the Data Breach* — In Florida, if a business undertakes an “appropriate” investigation or consults with relevant federal, state, and local law enforcement and “reasonably” determines that the breach has not — and likely will not — result in harm to the individuals whose personal information has been acquired and accessed, it need not notify those individuals.⁵⁹ In such cases, however, the statute requires that the business document its findings in writing and maintain the documentation for five years; failure to document or maintain the findings properly may result in a fine of up to \$50,000.⁶⁰ Similar provisions are included in the data breach statutes of Arkansas,⁶¹ Louisiana,⁶² and Oregon,⁶³ although only Oregon’s statute incorporates the requirement that any determination that there is no likelihood of harm to the consumers whose personal information has been acquired must be documented in writing and the documentation must be maintained for five years.⁶⁴

Ten states, however, *require* organizations to conduct a “reasonable” investigation of a security breach to determine whether there has been misuse of individuals’ information.⁶⁵ New Hampshire, for example, requires an entity to “immediately determine” whether misuse of individuals’ personal information has occurred. The statutes do not provide detail on what steps satisfy the requirements for a “reasonable” investigation.” Nevertheless, companies should be able to demonstrate

reasonableness through documenting the steps taken, the relevant expertise of the personnel performing the investigation, and adequate and thorough reporting of the relevant findings to appropriate senior management and government agencies. In short, companies undertaking an investigation to determine whether a breach of the security of their internal systems has or will lead to injury to their consumers' need to be ready to show what they did to make that assessment.

- *Providing Notice* — Absent an investigation or the involvement of law enforcement and the reasonable determination of no harm, Florida organizations suffering a material breach must notify the affected individuals in writing, by e-mail, or through substituted notice⁶⁶ in a time frame prescribed by the statute:

The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) and paragraph 10(a), or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.⁶⁷

The statute provides two complementary guidelines on when notice must be issued. Specifically, the notice must be made "without unreasonable delay" but, in any event, not later than 45 days after there is a "determination of a breach."⁶⁸ The 45-day countdown to provide notice may appear stringent at first blush, but, as written, it is subject to either tolling or nullification in the following circumstances. First, the 45-day countdown is tolled when the victimized company is taking "measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system."⁶⁹ These measures may take a substantial period of time and no outside time limit is specified in the statute. Second, the 45-day countdown for notice is nullified and no notification is required under Florida law if, after a reasonable investigation, the company determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed.⁷⁰

Similar language is found in 22 other state data breach statutes.⁷¹ However, most states do not impose strict time frames on investigations and notifications, and instead require action "without unreasonable delay." Thus, where there are no strict time limits, these clauses serve more as implicit authorization for investigation if none exists in the statute, and as a built-in explanation of what constitutes reasonable delay.

Only the data breach statutes in Ohio⁷² and Wisconsin⁷³ have the 45-day limits found in Florida's data breach statute. Ohio's statute contains a version of the caveat found in Florida's law that makes the rigorous time constraints "subject to the legitimate needs of law enforcement, *and* consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired and to restore the reasonable integrity of the data system."⁷⁴ However, the conjunctive between these two clauses means that companies in Ohio and the six other states that have similar clauses⁷⁵ need to coordinate with law enforcement from the onset of the investigation of a data breach to ensure that the 45-day notification requirement is tolled. The only exception to Wisconsin's requirements, on the other hand, is if a law enforcement entity requests that the organization delay providing notice in order to protect an investigation or homeland security.⁷⁶

By contrast, 28 states require a company to provide notice in the "most expedient time possible" and "without unreasonable delay" or "as soon as possible."⁷⁷ In the 10 states that require companies to undertake investigations, companies generally must first conduct a "reasonable and

prompt" investigation to determine the likelihood that personal information has been or will be misused; if so, they must then provide notice in the most expedient time possible.

- *Penalties* — Under the Florida data breach statute, failure to provide notice when it is required subjects the company to harsh penalties: administrative penalties of \$1,000 a day for the first 30 days and up to \$500,000 if the company does not notify affected individuals within 180 days.⁷⁸ The statute assigns enforcement of the penalties to the Department of Legal Affairs and does not provide a private right of action.⁷⁹

Consumers in California,⁸⁰ Hawaii,⁸¹ New Hampshire,⁸² North Carolina,⁸³ Washington State,⁸⁴ and Washington, D.C.⁸⁵ do have a private right of action under their state data breach statutes. In 14 other states, companies that do not comply with the statute face civil penalties ranging from \$500 a violation in Maine⁸⁶ to a maximum of \$750,000 in Michigan,⁸⁷ and a range of penalties in between.⁸⁸

Finally, in 21 states the attorneys general may institute suit for actual damages or injunctive relief against organizations or individuals that violate the data breach statute.⁸⁹

- *Enforcement and Litigation Under the Data Breach Statutes* — In the four years since the first data breach statute was passed in California in 2003, few state or federal complaints have been filed under the data breach statutes. In Florida, the Office of the Attorney General lists on its Web site one active public investigation involving Certegy regarding, inter alia, the adequacy of the notice the company provided with respect to a July 2007 breach of the records of 2.3 million consumers stolen by a former Certegy employee and sold to numerous data brokers and marketers.⁹⁰ In addition, the Florida attorney general is a part of a multistate civil investigation into the security breach reported by the TJX Companies, the parent company of TJ Maxx, Marshalls, HomeGoods, and A.J. Wright stores. The TJX breach affected information regarding credit and debit card sales transactions in TJX's stores in the United States, Canada, and Puerto Rico during 2003, as well as such information for these stores from mid-May through December 2006.⁹¹ TJX also faces numerous individual and class action suits filed by consumers across the country.⁹² Both the private litigation and the public enforcement actions appear to be focused on claims arising under TJX's failure to protect consumers' personally identifiable information, not on the company's failure to notify the victims upon the discovery of the breach.⁹³

In California, plaintiffs filed a federal class action suit against Cardsystems, Merrick Bank, Visa, and MasterCard for negligence and failing to notify consumers regarding a 2005 data breach in federal district court; the judge remanded the case to state court in October 2006 and did not rule on the merits of the claim.⁹⁴

In addition, as noted above, in 2006, ChoicePoint was sued by the FTC, but that action was brought under the FTC Act for unfair and deceptive acts or practices.⁹⁵ A class action suit alleging that Old National Bancorp's negligence led to a 2005 data breach was recently rejected by the Seventh Circuit on the grounds that "without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."⁹⁶ Although the plaintiffs relied on a theory of negligence for their claim, the Seventh Circuit looked to the Indiana data breach statute and ruled that:

[t]he provisions of the statute applicable to private entities storing personal information require only that a database owner *disclose* a security breach to potentially affected consumers; they do not require the database owner to take any other affirmative act in the wake of a breach. If the

database owner fails to comply with the only affirmative duty the duty to disclose — the statute provides for enforcement *only* by the [a]ttorney [g]eneral of Indiana. It creates no private right of action against the database owner by an affected customer. It imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow.⁹⁷

The paucity of reported cases on the data breach statutes may be due to the effectiveness of the notifications that companies are providing after a breach or maybe because state enforcement agencies and consumers have failed to take advantage of a legal tool that has been provided to them. However, 23 state statutes, including Florida, also contain language allowing companies to take “any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system”⁹⁸ and 10 state statutes include language requiring companies to undertake reasonable investigations to determine the scope of the breach. Thus, when companies face a data breach — and the prospect of litigation — it would be in their best interest to consider how they will approach such an investigation and the stakes at risk.

Using Digital Forensics to Investigate a Data Breach

An organization confronting a data breach likely will turn first to its internal system administrators but would be well-advised not to stop there when investigating the incident and evaluating its potential harm. Given the stakes of such digital investigations, many organizations in these difficult circumstances find it prudent to employ experts in digital forensics and investigation to determine whether the breach has not — and likely will not — result in harm to the individuals whose personal information has been acquired and accessed. While there are many reasons why using outside experts may be preferable, three stand out. First, IT professionals, who have no digital forensics training or experience, often mishandle evidence and can inadvertently do more harm than good. Second, a company’s system administrators or IT consultants may have inadvertently contributed to the data breach, which could put their job in jeopardy, and thus may have an incentive not to disclose all of the circumstances surrounding the breach. Third, even if no conflict exists, most internal IT departments simply lack the required expertise to conduct the sort of sophisticated investigation necessary to meet the statute’s adequacy requirement.

- *Conflict of Interest* — An internal IT group may be hesitant to admit that the breach was caused by an internal security weakness for fear that any blame for the vulnerability leading to the breach will be placed at their feet. In fact, IT personnel may even be concerned about suspicions of complicity in the data compromise. For example, if a company discovers that customer sales data may have been illicitly copied from a shared file server, its first step might be to work with the IT department to determine if the data was downloaded to an identifiable computer in order to determine whether the company must notify its customers. However, members of the IT department might be reluctant to cooperate or conduct a thorough investigation if they fear being held responsible for failing to secure the data from an unauthorized user who was able to connect to a file server. In one case, a company that experienced a data breach fired its IT consultants because they failed to apply security patches to e-commerce systems, exposing their customer database with credit card numbers to unauthorized access. Thus, relying solely on an IT department to conduct this type of investigation may not result in the type of “appropriate” investigation contemplated by the Florida Legislature in F.S. §817.5681(10)(a) or the legislatures in the other states that require or permit investigations.⁹⁹

- *Investigative Inexperience* — Competency poses an even greater issue. When networks are compromised and sensitive data are exposed, investigators need a wide range of skills to preserve and analyze volatile digital evidence. Members of an IT team rarely have the forensic skills necessary to analyze log files and network traffic, properly collect and examine volatile digital evidence, and use state-of-the-art forensic analysis techniques and tools to reconstruct events surrounding the data breach. Untrained responders frequently make matters worse because mistakes and perceived negligence can create added liability. For example, privacy violations

during an investigation may not only undermine a case, but can also open the organization to countersuits.

- *Nonforensic Handling of Digital Evidence* — The first reaction of an untrained individual when faced with a data breach is to examine the computers in question in an effort to determine what occurred. Delving into a digital investigation without taking the necessary steps to preserve the evidence in a forensically sound manner can alter or obliterate digital evidence that may be crucial to the investigation. Something as simple as changing the “last accessed” dates on the compromised computer system may make it impossible to ascertain whether an intruder gained unauthorized access to the data at issue. In addition, even if evidence of illegal activity is found, failures to handle digital evidence in a forensically sound manner can prevent an organization from taking legal action against the culprit or making a successful criminal referral to law enforcement.

One of the keys to forensic soundness is documentation. A solid case is built on supporting documentation that reports on where the evidence originated and how it was handled. In addition to characteristics of the evidence source, such as the time on a computer hardware clock or the number of sectors of a hard drive, an audit log and chain of custody enables an independent examiner to authenticate the evidence and assess its integrity and completeness.

An alternative method of conducting an “appropriate” investigation is using the assistance of outside digital forensic examiners and investigators who are able to interview members of the IT department and examine potentially compromised computer systems, without any perceived or actual conflict of interest. For example, the first step in the scenario outlined above might be to interview the appropriate members of the IT group on how their file security policies, if they exist, are implemented. Next, after preserving available digital evidence in a forensic manner, the investigators would forensically analyze the computers and any network-level logging in an attempt to determine when the file had been accessed, and what computers were connected to the file server at that time. That, in turn, might lead the examiners to image and analyze the computers connected to the file server around the time of the data breach. The result of the forensic analysis is a fuller picture of how, when, and by whom the data was accessed — in a documented and evidentiary sound form. This investigation and analysis will put the company in the best position possible to determine whether personal identifying information was on the drive and whether they are required to make any notifications under the Florida statute.

- *Encrypted Data: An Exception to the Notification Requirement* — The next step in evaluating whether the data breach will likely result in harm to the individuals whose personal information was acquired and accessed is determining the difficulty a thief might have in restoring the personal data. Under the Florida statute — and each of the other data breach statutes — a company is not required to report a data breach if the compromised information is encrypted.¹⁰⁰ Florida’s statute, like 24 other states and the District of Columbia, however, does not set forth any standard for encrypting the personal information.¹⁰¹ Under these statutes, any algorithm, no matter how weak can be held out as “encryption,” even though it may be vulnerable to a basic attack. For example, the industry standard is now 128-bit encryption, which protects data against “brute-force decryption attacks,” through the use of a computer to exhaustively calculate and try every possible encryption key one by one. A laptop that is protected by weak encryption, however, will succumb to such attacks quickly and that “encryption” may be essentially worthless in the hands of a technically sophisticated attacker.

On the other hand, the lack of a standard could also be interpreted as saying that data that are very difficult and expensive — such as compressed backup tapes containing credit card data that require specialized programs to restore — are de facto encrypted. Thus, in order to determine whether a loss of unencrypted backup tapes will “likely result in harm” to any individuals whose personal information was stored on those tapes, a digital forensics team would look at 1) the cost and availability of the back-up tape hardware needed to read the tapes; 2) the cost and availability of the back-up software used to create the tapes; 3) whether the volume of the data would pose

any difficulty for a skilled attacker; 4) how much of the data was in a compressed or proprietary format, or was spanned across multiple tapes; and 5) what impact the format would have on reading the data.

- *Documenting the Findings* — If the company determines that there has been *no* material breach or that a breach will not result in harm to the affected individuals, the Florida statute requires that it document those findings in writing and maintain that documentation for five years.¹⁰² Organizations that fail to properly document their findings and maintain those findings for five years face administrative fines of up to \$50,000.¹⁰³ Moreover, a failure to maintain basic forensic standards could lead to a later finding that the organization's determination that there was no material breach was not, in fact, "reasonable."¹⁰⁴ If the organization failed to notify Florida residents based on that determination, it could face administrative fines of up to \$500,000.¹⁰⁵

Where the stakes are so high, an organization facing a data breach is well advised to consult an outside expert with extensive experience in conducting such investigations rather than undertaking such an effort on its own, most likely for the first time. Relying on consultants who are credentialed, published, and certified in digital forensics, who have testified in court on similar issues, and who provide peer-reviewed work will give credence to findings regarding the organization's obligation to provide notice to consumers.

- *Before the Breach* — Tools are readily available to help mitigate the losses associated with data breaches. Deploying encryption software that meets industry standards serves two purposes. First, F.S. §817.5681(1)(a) requires organizations to notify individuals only when "unencrypted" personal information is compromised.¹⁰⁶ Thus, organizations should consider deploying encryption software to encrypt personal information to protect consumers and avoid the burdensome notification requirements. In addition, deploying encryption software that meets industry standards will protect the organizations' own proprietary information.

Second, legal and IT departments should also work together to create a data map before a breach happens. Identifying where a company's data are located before an incident is crucial so that digital forensic examiners are able to identify what information has been lost or compromised.

Finally, companies should prepare their IT systems as a source of evidence to support effective incident handling. Organizations that do so put themselves in a better position to mitigate the increasing costs and penalties associated with the exposure of sensitive data. Organizations that lack forensic preparedness generally find that they are unable to answer fundamental questions relating to breaches of security, including whether sensitive information was exposed, how and when the security breach occurred, and who was responsible. Determining whether sensitive information has been exposed can make the difference between having to disclose and not.

Conclusion

Data breach statutes in Florida and throughout the country present a web of conflicting obligations for companies and their lawyers that may potentially expose organizations to millions of dollars in fines and civil liability if obligations under the laws are ignored or misunderstood. The data breach statutes in Florida and throughout the country allow companies to forego notifying individuals whose personal information may have been compromised if the company "reasonably" determines that the breach did not — and likely will not — result in harm to those individuals. Although the statutes do not provide detail on what steps satisfy the requirements for a "reasonable" investigation," companies should be able to establish reasonableness by documenting the steps taken, the relevant expertise of the personnel performing the investigation, and adequate and thorough reporting of the relevant findings to appropriate senior management and government agencies.

Companies that undertake this task on their own face extraordinarily high stakes in terms of potential fines and risk to their reputation should the company rely on untrained personnel or individuals with conflicts of interest. Thus, when a laptop, PDA, or hard drive containing sensitive client or customer data goes missing or when servers containing such data are compromised, companies are well-advised to minimize their risk of fines by relying on experts in digital forensics to investigate the origin, nature and extent of the breach, and provide a determination as to whether the breach resulted in harm to individuals whose personal information has been compromised.

¹ Fla. Stat. §817.5681(5). The statute excludes from the definition of “personal information” publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

² See cites and discussion of relevant provisions of the state data breach laws *infra*.

³ Consumers Union, Notice of Security Breach State Laws, www.consumersunion.org/campaigns/Breach_laws_May05.pdf.

⁴ See, e.g., Anthony D. Milewski, Jr., *Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide*, 2 Shidler J. L. Com. & Tech. 19 (Apr. 14, 2006), available at www.ictjournal.washington.edu/Vol2/a019Milewski.html, and sources cited within.

⁵ Cal. Civ. Code §§1798.80 *et seq.* See also Milewski, *Compliance with California Privacy Laws* at 19.

⁶ Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress*, www.ftc.gov/opa/2006/01/choicepoint.shtm. In 2005, the FTC required Choicepoint to pay \$15 million in fines and redress relating to the data breach.

⁷ See Privacy Rights Clearing House, A Chronology of Data Breaches, www.privacyrights.org/ar/ChronDataBreaches.htm.

⁸ The Privacy Law Blog maintained by Proskauer Rose LLP contains links to most of the statutes cited here. See privacylaw.proskauer.com/2007/08/articles/security-breach-notification-l/breach-law-data/#more. Although Oklahoma enacted a data breach notification statute in 2006, its provisions apply only to state agencies, boards, commissions, or other units or subdivisions of the state government. See O.S. §3113.1. Because of the limited applicability of Oklahoma’s data breach statute, this article omits any discussion of its substantive provisions.

⁹ Fla. Stat. §817.5681, *et seq.*

¹⁰ Fla. Stat. §817.5681(5).

¹¹ Fla. Stat. §817.5681(1)(a). Compare to Cal. Civ. Code §1798.82(e), which defines “personal information” in California’s data breach statute. For the purposes of the “criminal use of personal identification information” (identity theft), both the Florida and California statutes define “personal information” much more broadly and include biometric data, medical records, passport number, postal or e-mail address, telephone number, and many other pieces of information. Fla. Stat. §817.568(1)(f)(1); Cal. Penal Code §530.5.

¹² Fla. Stat. §817.5681 (4).

¹³ Conn. Gen. Stat. §36a-701b, at §3(2).

¹⁴ Del. Code. Ann. Tit. 6, §§12B 101-104 , at §12B-101(3).

¹⁵ 815 ILCS 530/5.

¹⁶ La. Rev. Stat. Ann. §§3071, at §3073(3)(a).

¹⁷ Minn. Stat. §325E.61, at §1(e).

¹⁸ Mont. Code Ann. §30-14-1704, at §7(1).

¹⁹ NRS 603A.220.

²⁰ N.J. Stat. Ann. §56:8-163, at §10.

- ²¹ R.I. Gen. Laws, §11-49.2-1, at 11-49.2-5(c).
- ²² Tenn. Code Ann. §47-18-2107, at (a)(3).
- ²³ Tex. Bus. & Com. Code Ann. §48.103.
- ²⁴ Wash. Rev. Code Tit. 19, at §2(1).
- ²⁵ Ark. Code Ann. §4-110-103.
- ²⁶ Ga. Code §10-1-911(5).
- ²⁷ 10 Maine Rev. Stats. §1347(6).
- ²⁸ N.D. Cent. Code §51-30-01(2)(a).
- ²⁹ N.Y. Gen. Bus. Law. §899-aa(1)(a)-(b) (emphasis added).
- ³⁰ Haw. Rev. Stat. Tit. 2/Act. 135.
- ³¹ IC 24-4.9-2-2 (2)(a).
- ³² N.C. Gen. Stat. §75-65(a).
- ³³ Mass. Rev. Stats., §93H 1(a).
- ³⁴ See Wis. Stat. §895.507(b). In fact, Wisconsin’s data breach statute never mentions electronic data or computer systems, but requires an organization to notify all consumers — not merely Wisconsin residents — if it becomes aware that someone has acquired personal information without authorization to do so. See Wis. Stat. §895 507(2).
- ³⁵ Fla. Stat. §817.5681(4). A standard provision, also found in Florida, is the exemption for the good faith acquisition of personal information by an employee or agent of the person, which is considered not to be a breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use. See Fla. Stat. §817.5681(4).
- ³⁶ See Eric Friedberg and Michael McGowan, *Lost Back-Up Tapes, Stolen Laptops and Other Tales of Data Breach Woe*, *The Computer & Internet Lawyer* (Oct. 2006).
- ³⁷ §1798.82(d).
- ³⁸ The 19 states that define “security breach” without referencing “materiality” are Arkansas, see Ark. Code Ann. §4-110-103(1)(A); Colorado, see Col. Rev. Stat. §6-1-716(a); Delaware, see Del. Code Ann. Tit. 6, §12B-101(a); Georgia, see Ga. Code Ann. §10-1-911(1); Illinois, see 815 ILCS 530/5; Indiana, see IC 24-4.9-2-2; Kansas, see Kan. Stat. Ann. §50-7a01(h); Maine, see Me. Rev. Stat. Ann. Tit. 10, §1347(1); Maryland, see Md. Code Ann. §14-35-4(A)(1); Michigan, see MCL §445.63(3)(b); Minnesota, see Minn. Stat. §325E.61, Subdiv. 1(d); Nebraska, see Neb. Rev. Stat. §87-802(1); New Hampshire, see N.H. Rev. Stat. Ann. §359-C:19 V; New Jersey, see N.J. Stat. Ann. C.56:8-161(10); Rhode Island, see R.I. Gen. Laws §13-44102; Texas, see Tex. Bus. & Com. Code Ann. §48.103; Utah, see Utah Code Ann. §13-44-102(1)(a); Vermont, see Vt. Stat. Ann. Tit. 9, §2430(8)(A); Washington, see Wash. Rev. Code §19.255.010(4); District of Columbia, see D.C. Code §28-3851(1).
- ³⁹ Ariz. Rev. Stat. §44-7501.
- ⁴⁰ Idaho Code §28-51-104(2).
- ⁴¹ NRS 603A.020.
- ⁴² S.B. 583, §2(1)(a).
- ⁴³ Tenn. Code. Ann. §47-18-2107(b).
- ⁴⁴ See notes 29 through 33.
- ⁴⁵ Conn. Gen. Stat. §36a-701(b).
- ⁴⁶ IC 24-4.9-2-2.
- ⁴⁷ Haw. Rev. Stat. Tit. 26/Act. 135.
- ⁴⁸ La. R.S.A. §3073(2).

- ⁴⁹ Haw. Rev. Stat. Tit. 26/Act 135, §2, §-1.
- ⁵⁰ Section 16, Ch. 93H, §1(G) of the Acts of 2007.
- ⁵¹ Mont. Code. Ann. §30-14-1704(4)(a).
- ⁵² N.C. Gen. Stat. §75-61(14).
- ⁵³ Ohio Rev. Code Ann. §1349.19(A).
- ⁵⁴ S.B. 712, §2(a).
- ⁵⁵ W.S. 40-12-501(a).
- ⁵⁶ Section 16, Ch. 93H, §1(G) of the Acts of 2007 (emphasis added).
- ⁵⁷ N.Y. Gen. Bus. Law, §899-aa(c).
- ⁵⁸ Vt. Stat. Ann. Tit. 9, §2435(d)(1).
- ⁵⁹ Fla. Stat. §817.5681(10)(a).
- ⁶⁰ Fla. Stat. §817.5681(10)(a)-(b).
- ⁶¹ Ark. Code Ann. §1167, §4-110-105(d).
- ⁶² La. R.S.A. §3074(G).
- ⁶³ S.B. 583, §2(7).
- ⁶⁴ *Id.*
- ⁶⁵ The 10 states that require organizations to conduct an investigation upon discovering a data breach are Arizona, see Ariz. Rev. Stat. §44-7501A; Connecticut, see Conn. Gen. Stat. §36a-701 (b); Idaho, see Idaho Code §§28-51-105; Kansas, see Kan. Stat. Ann. §§70-7102; Maine, see Me. Rev. Stat. Ann. Tit. 10, §1348; Maryland, see Md. Code Ann. §14-3504(B)(3); Nebraska, see Neb. Rev. Stat. §87-803(1); New Hampshire, see N.H. Rev. Stat. Ann. §359-C:20 I(a); Utah, see Utah Code Ann. §13-44-202(1)(a); and Wyoming, see W.S. §40-12-501(a).
- ⁶⁶ Fla. Stat. §817.5681(6).
- ⁶⁷ Fla. Stat. §817.5681(1)(a).
- ⁶⁸ *Id.*
- ⁶⁹ *Id.*
- ⁷⁰ See Fla. Stat. §817.5681(10)(a).
- ⁷¹ The 22 states with similar provisions are Arkansas, see Ark. Code Ann. §4-110-105(d); California, see Cal. Civ. Code §1798.82(a); Colorado, see Col. Rev. Stat. §6176(2); Georgia, see Ga. Code Ann. §10-1-912(a); Hawaii, see Haw. Rev. Stat. Tit. 26/135 §-2; Illinois, see 815 ILCS 530/10(a); Kansas, see Kan Stat. Ann. §50-7a02; Louisiana, see La. Rev. Stat. §3074; Maine, see Title 10, §1348.1; Maryland, see Md. Code Ann. §3504(D)(1); Michigan, see MCL §445.72(12)(4); Minnesota, see Minn. Stat. §325E.61, Subdiv. 1(a); Montana, see Mont. Code Ann. §30-14-1704 (1); Nevada, see NRS 603A.220(1); New Jersey, see N.J. Stat. Ann. §56:8-163(12)(a); New York, see N.Y. Gen. Bus. Law, §899-aa(2); North Dakota, see N.D. Cent. Code §51-30-02; Pennsylvania, see S.B. 712 §3(a); Rhode Island, see R.I. Gen. Laws, §11-49.2-3; Tennessee, see Tenn. Code Ann., §47-18-2107(d); Texas, see Tex. Bus. & Com. Code Ann. §48.103(b); and Utah, see Utah Code Ann. 13-44-202(2).
- ⁷² Ohio Rev. Code Ann. §1349.9(B)(2).
- ⁷³ Wis. Stat. §895.507(3).
- ⁷⁴ Ohio Rev. Code Ann. §1349.9(B)(2).
- ⁷⁵ The six other states that have similar clauses are Connecticut, see Conn. Gen. Stat. §36a-701b (b); Idaho, see Idaho Code §§28-51-105; Nebraska, see Neb. Rev. Stat. §87-803(1); Delaware, see Del. Code Ann. Tit. 6, 12B-102(a); Indiana, see Ind. Code §24-4.9-3-3; North Carolina, see N.C. Gen. Stat. §75-65; and Oregon, see SB 583, §3(1).
- ⁷⁶ Wis. Stat. §895.507(3).

⁷⁷ The 28 states that require a company to provide notice in the “most expedient time possible” and “without unreasonable delay” or “as soon as possible” are Arkansas, see Ark. Code Ann. §4-110-105(d); California, see Cal. Civ. Code §1798.82(a); Colorado, see Col. Rev. Stat. §6176(2); Connecticut, see Conn. Gen. Stat. §36a-701b(b); Delaware, see Del. Code Ann. Tit. 6, 12B-102(a); District of Columbia, see D.C. Code §28-3852(a); Georgia, see Ga. Code Ann. §10-1-912(a); Hawaii, see Haw. Rev. Stat. Tit. 26/Act 135, §-2; Illinois, see 815 ILCS 530/10(a); Indiana, see Ind. Code §24-4.9-3-3; Louisiana, see La. Rev. Stat. §3074; Massachusetts, see Ch. 82 of the Acts of 2007, Ch. 93H(3); Michigan; see MCL §445.72(12)(4); Minnesota, see Minn. Stat. §325E.61, Subdiv. 1(a); Montana, see Mont. Code Ann. §30-14-1704(1); Nevada, see NRS 603A.220(1); New Jersey, see N.J. Stat. Ann. §56:8-163(12)(a); New York, see N.Y. Gen. Bus. Law, §899-aa(2); North Carolina, see N.C. Gen. Stat. §75-65; North Dakota, see N.D. Cent. Code §51-30-02; Oregon, See SB 583, §3(1); Pennsylvania, see S.B. 712 §(3)(a); Rhode Island, see R.I. Gen. Laws, §11-49.2-3; Tennessee, see Tenn. Code Ann., §47-18-2107(d); Texas, see Tex. Bus. & Com. Code Ann. §48.103(b); Utah, see Utah Code Ann. 13-44-202(2); Vermont, see Vt. Stat. Ann. Tit. 9 §2435(b)(1); Washington, see Wash. Rev. Code §19.255.010(1).

⁷⁸ Fla. Stat. §817.5681(1)(b). The sanctions for failure to notify, however, apply per breach and not per individual affected by the breach. *Id.*

⁷⁹ See Fla. Stat. §817.5681(11).

⁸⁰ See Cal. Civ. Code §1798.84.

⁸¹ *Id.*

⁸² N.H. Rev. Stat. Ann. §359-C:21.

⁸³ N.C. Gen. Stat. §75-65-(i).

⁸⁴ Wash. Rev. Code. 19.255(10)(a).

⁸⁵ D.C. Code §28-3853(a).

⁸⁶ Me. Rev. Stat. Ann., Tit. 10 §1349.2.

⁸⁷ Mich. S.B. 309, §12 (13-14).

⁸⁸ In Arizona, companies face civil penalties up to \$10,000, see Ariz. Rev. Stat. §44-7501(H); Hawaii, civil penalties up to \$2,500 for each violation, see Haw. Rev. Stat. Tit. 25/Act 135 §-3; Idaho, fines of up to \$25,000 per breach, see Idaho Code §28-51-107; Indiana, civil penalties up to \$150,000 per deceptive act; see IC 24-4.9-4-2.

⁸⁹ The 14 states in which state attorneys general have authority to bring suits for damages or injunctive relief are Arkansas, Ark. Code Ann. §4-109-108; Colorado, Col. Rev. Stat. §6176(4); Connecticut, Conn. Gen. Stat. 36a-701b(g); Delaware, Del. Code Ann. Tit. 6, §12B-106; Illinois, 815 ILCS 530/20; Kansas, Kan. Stat. Ann. §50-7a02(g); Louisiana, La. Rev. Stat. Ann. §3075; Maine, Me. Rev. Stat. Ann. Tit. 10 §1349.2; Maryland, Md. Code Ann. §14-3508; Massachusetts, Ch. 93H, §6; Minnesota, Minn. Stat. Subdiv. 6; Nebraska, Neb. Rev. Stat. §87-806; Nevada, NRS §603A.920; New Jersey, C.56:8-166; North Carolina, N.C. Gen. Stat. §75-65(i); North Dakota, N.D. Cent. Code §51-03-07; Ohio, Ohio Rev. Code Ann. §1349.19(I); Pennsylvania, S.B. 712 §8; Tennessee, Tenn. Code Ann., 47-18-2106; Texas, Tex. Bus. & Com. Code Ann. §48.201; Utah, Utah Code Ann. §14-44-301(4); Vermont, Vt. Stat. Ann. Tit. 9 §2435(g); Wyoming, W.S. 40-12-502(f).

⁹⁰ See Active Public Consumer-related Investigation of Certegy Check Services, Inc., Case No. L07-3-1109, myfloridalegal.com/_85256309005085AB.nsf/0/8B92E22923AF376C852573240063987E?Open&Highlight=0,data,breach.

⁹¹ The Commonwealth of Massachusetts Office of the Attorney General, Massachusetts Attorney General Martha Coakley Leads Multi-state Investigation Into TJX Security Practices, www.mass.gov/?pageID=pressreleases&agId=Cago&prModName=cagopressrelease&prFile=2007_02_07_tjx_investigation.xml.

⁹² The actions filed against TJX, the parent company of TJ Maxx, include *Robinson v. TJX Companies, Inc., et al.*, 07-cv-02139 (N.D. Ill.); *Arians, et al. v. TJX Companies, Inc., et al.*, 07-cv-10769 (D. Mass.); *Massachusetts Bankers Ass’n, et al. v. TJX Companies, Inc., et al.*, 07-cv-10791

(D. Mass.); *Wardrop v. TJX Companies, Inc., et al.*, 07-cv-00430 (W.D. Mich); *Taliaferro, et al. v. TJX Companies, Inc., et al.*, 07-cv-00388 (S.D. Ohio); *Lack, et al. v. TJX Companies, Inc., et al.*, 07-cv-00233 (E.D. Tex.); *Lamb, et al. v. TJX Companies, Inc., et al.*, 07-cv-00379 (W.D. Mo.); *Roberts, et al. v. TJX Companies, Inc., et al.*, 07-cv-02887 (N.D. Ill.); and *Mace v. TJX Companies, Inc., et al.*, (D. Mass.), which has been administratively designated as the lead case with respect to all actions pending in the District of Massachusetts, which have been consolidated.

⁹³ In addition, a Miami man charged by the Office of Statewide Prosecution pleaded guilty to charges arising out of his involvement in an identity theft ring that used personally identifiable information stolen from that data breach. In the scam, the defendant coordinated the use of counterfeit cards with stolen credit card data to purchase gift cards at Wal-Mart or Sam's Club. This defendant and other co-conspirators then redeemed the gift cards to purchase jewelry and electronic equipment. According to the Office of the Attorney General, the total loss from the scheme could be \$3 million. See Office of the Attorney General, Ringleader of ID Theft Operation Sentenced to 5 Years in Prison, myfloridalegal.com/__852562220065EE67.nsf/0/3D930E6715D0935D85257355005143E9?Open&Highlight=0,data,breach.

⁹⁴ *Parke v. Cardsystems*, 2006 U.S. Dist. LEXIS 77241 (N.D. Cal., Oct. 11, 2006).

⁹⁵ See Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress*, www.ftc.gov/opa/2006/01/choicepoint.shtm.

⁹⁶ *Pisciotta v. Old National Bancorp*, 2007 U.S. App. LEXIS 20068 at *27 (7th Cir.).

⁹⁷ *Id.* at *18-19.

⁹⁸ See note 69.

⁹⁹ See section in text subtitled, "Investigating the data breach."

¹⁰⁰ For the relevant provisions exempting encrypted data when determining whether notification to consumers is required, see Arizona, Ariz. Rev. Stat. §7501 (A); Arkansas, Ark. Code Ann. §110-103(7); California, Cal. Civ. Code §1798.81.5(d)(1); Colorado, Col. Rev. Stat. §6-1-716(d)(1); Connecticut, Conn. Gen. Stat. §361-701b(a); Delaware, Del. Code Ann. Tit. 6, §12B-101(2); Florida, see Fla. Stat. §817.5681(1)(A); Georgia, see Ga. Code Ann. §10-1-911(5); Hawaii, see Haw. Rev. Stat. Tit. 26/Act 135 §1; Idaho, see Idaho Code §28-51-1-104(2); Illinois, see 815 ILCS §530.15; I.C. 2.4-4.9-3-1; Kansas, see Kan. Stat. Ann. §50-7a01(h); Louisiana, see La. Rev. Stat. Ann. §3073(4)(a); Maine, see Me. Rev. Stat. Ann. Tit. 10 §1347(6); Maryland, see Md. Code Ann. §14-3501(D); Ch. 93H, §(1)(a); Michigan, see MCL §445.72(1); Minnesota, see Minn. Stat. §325E.61, Subdiv. 1 (e); Montana, see Mont. Code Ann. §30-14-1704(1); Nebraska, see Neb. Rev. Stat. §87-802(3); Nevada, see NRS §603A.040; New Hampshire, see N.H. Rev. Stat. Ann. §359-C:19 (IV); New Jersey, see N.J. Stat. Ann. §C.56:8-161(10); New York, see N.Y. Gen. Bus. Law, §899-aa (1)(b); North Carolina, see N.C. Gen. Stat. §75-61(14); North Dakota, see N.D. Cent. Code, §51-30-01(2)(a); Ohio, see Ohio Rev. Code Ann. §1349.19(a)(7)(a); Oregon, see Ore. S.B. 583 §11(a); Pennsylvania, see S.B. 712, §2; Rhode Island, see R.I. Gen. Laws, §11-49.2-3; Tennessee, see §47-18-21-07(b); Texas, see Tex. Bus. & Com. Code §48.002(2); Utah, see Utah Code Ann. §13-44-102(1)(a); Vermont, see Vt. Stat. Ann. Tit. 9, §2430(5); Washington, see Wash. Rev. Code, §19.255.00(5); Wisconsin, see Wis. Stat. §895.507(1)(b); Wyoming, W.S. §40-12-501(a)(vii) (Wyoming's statute refers to information that is "redacted" rather than "encrypted"); District of Columbia, see D.C. Code §28-3851 (instead of referring to encryption, the D.C. Code says that data that has been "rendered secure so as to be unusable by an unauthorized third party shall not be deemed to be a breach of the security of the system").

¹⁰¹ The states that do not provide any definition for encryption are Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Louisiana, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Rhode Island, Tennessee, Texas, Utah, Washington, Wisconsin, Wyoming, and the District of Columbia.

¹⁰² Fla. Stat. §817.5681(10)(a).

¹⁰³ Fla. Stat. §817.5681(10)(b).

¹⁰⁴ See Fla. Stat. §817.5681(10)(a).

¹⁰⁵ See Fla. Stat. §817.5681(1)(b).

¹⁰⁶ Fla. Stat. §817.5681(1)(a).

Dana J. Lesemann is vice president and deputy general counsel at Stroz Friedberg, LLC, a consulting and technical services firm focusing on digital forensics, electronic discovery, and cyber-security investigations. Ms. Lesemann is grateful to her colleagues for their assistance in developing this article, particularly the research of Tivan Amour and Steven Mecca.

[Updated: 02-26-2008]

© 2005 The Florida Bar |