2008

New Legal Frontier: Mass Information Loss and Security Breach

Chad Pinson

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation
https://scholar.smu.edu/scitech/vol11/iss1/3

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
New Legal Frontier: 
Mass Information Loss and Security Breach

Chad Pinson*

I. ONE IDENTITY THIEF, ONE VICTIM — A THING OF THE PAST

Over the past several years, “identity theft” has been a buzz phrase in the media and a fertile ground for lawsuits. The brazenness and ingenuity of the thieves who steal identities certainly makes for an intriguing story, and everyone can imagine themselves as a potential victim. Children steal the identities of their parents, and parents steal the identities of their children. Sophisticated identity-theft rings that have exhausted the identities of male victims begin to cross-dress to steal and use the identities of women. Waiters at restaurants use card-swipe machines to steal individual credit card numbers. ATM machines are compromised. Mailboxes are robbed. Purses and wallets are stolen. Checkbooks are intercepted before reaching their intended recipient.

Countless articles have been written on these crimes, their victims, the criminals who commit them, and even the law applicable to such crimes. Generally, although the facts may be sensational, the story is the same. One victim has his or her personal information, checks, or credit card stolen. The thief then makes purchases, opens accounts, and obtains goods and services in the name of the victim. The thief is rarely caught, and even more rarely sued in a civil case by the victim. Instead, the financial institutions and credit reporting agencies associated with the fraudulent accounts and purchases are sued by the identity-theft victim under a variety of legal theories, including claims under the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and various state common law theories of liability.

II. THE NEW FRONTIER — MASS DATA LOSS AND BREACH

What was once an aberration in the news and the courts has now become front-page news - the mass data loss or mass security breach. In the past two to three years, news articles and lawsuits related to mass data loss and mass security breaches have exploded into the forefront of public consciousness. There are countless stories of mass security breach or mass data loss on the front page of every paper in the country. The online Identity Theft Resource Center reports that, as of May 15, 2007, 110 breaches of databases containing sensitive information have been reported since the be-

* Chad Pinson is a partner at Baker Botts LLP specializing in commercial, privacy, financial transaction, class action, and consumer litigation. His interest in mass data security issues comes from his experience representing companies that handle sensitive consumer information in litigation across the country in matters including security breach, identity theft, embezzlement, financial fraud, privacy issues, and security policies. Special thanks to Van Beckwith, Ryan Bangert, Ian Roberts, Chris Johnston, and Charles Strecker at Baker Botts, and his supportive family - Crystal, Annalise, and Asher.
ginning of the year. In 2006 alone, over 312 separate incidents of mass data loss or mass security breach occurred, exposing the identifying personal or consumer information of over nineteen million individuals. And, in 2005-2006, at least seventy high-profile laptop thefts resulted in the loss and compromise of over thirty-two million consumer records.

For example, a consultant reviewing pension data for the Neiman Marcus Group had computer equipment stolen containing Social Security numbers, addresses, and salary information of around 160,000 employees.

The Texas Attorney General sued RadioShack, charging that the electronics retailer improperly disposed of thousands of customer records containing addresses and credit card numbers.

The computer network of TJX, the parent company of TJ Maxx and Marshalls, was hacked, exposing approximately forty-five million consumers’ credit and debit card numbers to the hackers.

CitiFinancial used UPS to send a box of computer tapes containing the personal identifiers and financial habits of its customers from New Jersey to a data processing center in Allen, Texas. The box of tapes, which contained Social Security numbers, account information, and other data on 3.9 million people, never arrived.

LexisNexis reported that the names, addresses, and Social Security numbers of about 30,000 people may have come into the possession of thieves. The information was stored on massive consumer databases, and

4. See Pamela Yip & Maria Halkias, Neiman Employees' Data Stolen: No Evidence that IDs were Target in Computer Equipment Theft, DALLAS MORNING NEWS, Apr. 25, 2007, at 1D.
5. See Barbara Ramirez, Store in Portland Sued by the State AG: Customers’ Financial Information was Found in Garbage Bin Out Back, CORPUS CHRISTI CALLER-TIMES, Apr. 3, 2007, at B1.
7. See Laura Smitherman, Missing Data is Latest in Rash of Breaches, Consumers are Warned to Head Off Identity Theft, BALT. SUN, June 8, 2005, at 1A.
8. Id.
was accessed by persons making unauthorized use of the passwords of legitimate subscribers.\textsuperscript{10}

CardSystems Solutions Inc., which processes credit card and other payments for banks and merchants, was attacked by a virus-like computer script. Information on nearly forty million cardholders of multiple brands, including Mastercard and Visa, was potentially exposed.\textsuperscript{11}

ChoicePoint, a data storage company based in Georgia, inadvertently sold consumer information to a thief posing as an executive with a Los Angeles financial company. A subsequent investigation revealed that records on nearly 145,000 people were compromised.\textsuperscript{12}

The University of Georgia reported that a computer hacker entered a computer database and gained access to the Social Security numbers of approximately 1,600 employees. This followed closely on the revelation of a previous security breach during which hackers gained access to a server containing the names, birth dates, credit card information, and Social Security numbers of students who applied to the University since 2002.\textsuperscript{13}

Black Hills State University in South Dakota accidentally published the Social Security numbers of fifty-six students on its website.\textsuperscript{14}

A laptop containing the Social Security numbers of about 2,000 current and former school employees from Springfield City Schools in Ohio was stolen from a state auditor’s home.\textsuperscript{15}

An unencrypted disk containing the Social Security numbers, health plan identification numbers, and names of approximately 75,000 Blue Cross and Blue Shield customers disappeared. The disk was later recovered.\textsuperscript{16}

A Bank of America employee allegedly accessed customer profiles and supplied them to a sophisticated identity theft ring that may have stolen over

\textsuperscript{10} Id.

\textsuperscript{11} See Joe Del Bruno, Another Breach in Data Security: 40 Million Credit Card Customers of Various Brands May be Exposed, PHILA. INQUIRER, June 18, 2005, at A1.

\textsuperscript{12} See Bobby White, Few Laws Require Data Theft be Public, FT. WORTH STAR-TELEGRAM, June 26, 2005, at F1.

\textsuperscript{13} See Kelly Simmons, Hackers Breach Database at UGA, ATLANTA J. & CONST. Sept. 29, 2005, at C2.

\textsuperscript{14} Black Hills State University Meets With Students to Alert Them of Possible Identity Disclosure, U.S. ST. NEWS, Apr. 11, 2007.

\textsuperscript{15} Andrew McHinn, Stolen Laptop had info on Workers at Springfield Schools, DAYTON DAILY NEWS, Mar. 17, 2007, at A6.

\textsuperscript{16} Associated Press, Insurer Recovers Missing Data; Disc Had Information on 75,000 Empire Blue Cross Blue Shield Members, ALBANY TIMES UNION, Mar. 15, 2007, at E4.
$12 million from customer accounts over a two-year period. Just a year earlier, Bank of America lost, and was unable to locate, the backup tapes containing the identities of 1.2 million individuals, including their names and Social Security numbers. The University of Texas' computer system was hacked, and the identifying information of over 175,197,000 students, employees, and alumni was downloaded.

The University of Michigan Credit Union in Ann Arbor discarded, but failed to shred, documents containing the personal identifying information of some of its members, resulting in the identity theft of some of those members. The University of North Texas' computer system was accessed by hackers, exposing the personal identifiers of almost 39,000 students and alumni.

DSW Shoe Warehouse learned that the identifying information (or credit card numbers) of 1.4 million customers may have been stolen. The U.S. Department of Commerce admitted that 1,100 laptops were unaccounted for, including several that contain U.S. Census Bureau data such as names and social security numbers.

A U.S. Transportation Security Administration hard drive containing Social Security numbers and banking information of approximately 100,000 Homeland Security employees went missing from a secured area at T.S.A. headquarters.

20. See Stolen Data Leads To Identity Theft, COMPUTERWORLD, June 12, 2006, at 10.
21. See Josh Baugh, Server Hacked at UNT: Denton 39,000 Told To Take Precautions, Check for Identity Theft, DALLAS MORNING NEWS, Aug. 9, 2005, at 1B.
In two separate incidents, the loss or theft of laptops from the Department of Veteran's Affairs created a politically charged story, and placed the personal information of over twenty-six million veterans at risk.25

III. A REALISTIC SCENARIO IN THE MODERN MASS-DATA-BREACH ENVIRONMENT

It is 10 p.m., and your mobile phone is ringing. Whether you are a lawyer that represents consumers, or in-house counsel for a business that houses the personal information of either employees or consumers, the contents of the phone call will be the same. The only differences will be the messenger—a victimized consumer, a very nervous IT manager, or a stern FBI or Secret Service agent—informing you that a very large database containing sensitive personal information about your client, employees, or your customers has been compromised.

If you fall on one side of the problem, your mind races: “How many names were on that database?” A few phone calls later and you have the answer: approximately 250,000. You ask yourself the crucial questions: How did this happen? What do I do next? What is my company’s potential exposure?

If you fall on the other side of the problem, you have similar questions: How do I protect my client from further harm? Can I bring a claim against the company who allowed the data to be exposed? What claim? How much is this case worth?

This is no longer an implausible scenario. The loss of highly sensitive personal information has become unnervingly commonplace. Thieves are now targeting this sort of information as never before. Large amounts of data are making their way onto tiny disks and laptops that do not enjoy the same sort of protection and security as typical corporate mainframes. Corporations are communicating more and more through electronic transmission of data, and are also increasing their presence on the internet. All of these factors, and many others, suggest mass data loss and mass security breaches are here to stay, with more incidents, not less, occurring in the future.

IV. CORPORATE DUTIES AND EXPOSURE IN A MASS BREACH OR DATA LOSS

The costs associated with mitigating these security breaches can be staggering.26 When credit card information is compromised, accounts must be checked for discrepancies and closed, and new cards issued. When social security numbers are compromised along with personal identifying informa-


tion, identity theft looms large as a troubling possibility. Unlike credit card information, the loss of personal identifying information along with social security numbers may require years of vigilant monitoring, if not entire lifetimes, as identity thieves may lay in wait for years before striking.27

Parties who bear the cost of repairing the damage caused by information security breaches have been actively seeking to shift these costs to the organizations in control of the systems that were compromised. To date, what has emerged from these efforts is a patchwork approach without a unifying theme. A number of states have enacted statutes requiring possessors of personal information to take reasonable measures to safeguard the information, and to notify individuals when their information is compromised.28 Federal lawmakers have proposed similar measures.29 In addition to these legislative approaches, individuals whose information has been compromised have sought legal redress against organizations from which their information was taken using a variety of statutory and common law theories.30 These cases may prove to be the leading edge in an effort to set new standards for the care and safeguarding of personal information.

This article elucidates the legal risks faced by organizations that hold sensitive personal information by examining in detail these emerging sources of potential liability. These risks may be analyzed by first addressing the duties placed on such businesses by existing and proposed state and federal statutes. The current mix of statutes — evolving on an ongoing basis — sets forth broad guidelines regarding the implementation of reasonable data security measures, and imposes notification requirements on businesses that suffer data security breaches. Second, this article examines liability exposure under existing statutory and common law frameworks. The extent of this exposure to risk remains highly uncertain. However, current litigation is likely to begin the process of clarifying the boundaries within which businesses must operate in order to minimize their exposure to liability for information loss.

V. IMPLICATIONS AND POTENTIAL CLAIMS

The news accounts of mass data breach and loss possess a unifying theme: each scenario presents the specter of liability for an entity that has suffered information loss via some form of a data security breach. Businesses experiencing such losses must quickly and accurately conduct a two-part analysis if liability is to be minimized or avoided altogether. First, the

27. See Daniel J. Solove, Identity Theft, Privacy, and The Architecture of Vulnerability, 54 Hastings L.J. 1227, 1246 (2006) (noting "Once the card is cancelled, the crime ends. With identity theft, the crime can continue, for personal information works like an 'access card' that cannot be readily deactivated.").

28. See infra notes 23-58 and accompanying text.

29. See infra notes 59-65 and accompanying text.

30. See infra notes 66-130 and accompanying text.
affected business must assess its duties to the affected consumers under state and federal statutory law. Second, the affected business must recognize grounds for potential liability under both statutory and common law frameworks. To be sure, these twin considerations implicate overlapping bodies of law, and are far from distinct. However, this framework is a useful tool for businesses faced with making snap decisions in the face of uncertainty.

A. Duties Under State and Federal Statutory Law

Thus far, state legislatures have been very eager to pass legislation that imposes duties on entities that suffer mass data loss or a mass security breach. Federal law, however, has lagged behind.

1. Duties Under State Statutory Law

The recent proliferation of high-profile security breaches has prompted a number of states to enact statutes setting standards for safeguarding personal information, and notifying individuals when their information is compromised. This tidal wave of security breaches that prompted the current legislative response was itself precipitated by the passage in 2003 of California’s law requiring businesses that own or license personal information about a California resident to disclose any breach of the security of that information to the resident.

a) The California Data Security and Notification Law

The California law has served as a model for many of the data security laws subsequently passed by other states. Accordingly, any discussion of statutory sources of liability facing organizations engaged in the collection or retention of sensitive personal information must begin with this law.

The California data security law sets forth three general requirements relevant to businesses dealing with personal information. These require-

31. See infra notes 23-58 and accompanying text.
32. See infra notes 59-65 and accompanying text.
33. See infra notes 23-58 and accompanying text.
34. See Bob Zeller Jr., Data Security Laws Seem Likely, So Consumers and Businesses Vie to Shape Them, N.Y. TIMES, Nov. 1, 2005, at 3C (noting that “California’s data security notification law is largely credited with forcing companies nationwide to tell consumers about data breaches”); see also Editorial, Digital Safeguards, BALT. SUN, June 13, 2005, at 10A ("We’re more often learning about these security breaches because of a 2003 California law requiring customer notification.").
35. See supra Part VII.
37. §§ 1798.81, 1798.81.5, 1798.82(a).
ments may loosely be classified as: (1) notification, (2) reasonable security, and (3) data destruction. These requirements have been adopted in varying degrees by other states, and serve as a blueprint for federal legislation.

(1) Notification

By far the most prominent provision in the statute, California’s notification law provides that:

Any agency, person, or business who conducts business in California, and that owns or licenses computerized data containing personal information, shall disclose “any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The notification must be made “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data systems.” Notification “may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.” “Breach of the security of the system” is defined as an “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.” An exception to this definition is made for “[g]ood faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business

38. §§ 1798.81, 1798.81.5, 1798.82(a).
39. This language suggests that a security breach of non-computerized records would not trigger the duties and liabilities of the statute.
40. Because the California statute is limited to the loss or exposure of unencrypted information, at least some recent high-profile mass data loss incidents would not have triggered the California statute.
41. However, if the computerized data is not “owned” by the business, but rather is merely being “maintained” on behalf of an owner or licensee, the maintaining entity must notify the owner or licensee “of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82(b).
42. § 1798.82(a).
43. § 1798.82(c).
44. § 1798.82(d).
New Legal Frontier

... provided that the personal information is not used or subject to further unauthorized disclosure."45 "Personal information" is defined as:

[A]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(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.46

Personal information does not include information made lawfully available to the public from "federal, state, or local government records."47 Once the notification requirement is triggered, the agency may provide notice either in writing,48 by e-mail,49 or by substitute notice.50 Substitute notice may be made if the agency, person, or business demonstrates "that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information."51 Substitute notice consists of "e-mail notice when the agency has an e-mail address for the subject persons, conspicuous posting of the notice on the agency's Web site page, if the agency maintains one, [and,] notification to major statewide media."52 The statute further provides that:

an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of [the statute], shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in

45. Id.
46. § 1798.82(e).
47. §§ 1798.29(f), 1798.82(f).
48. §§ 1798.29(g)(1), 1798.82(g)(1).
49. §§ 1798.29(g)(2), 1798.82(g)(2). If electronic notice is given, the requirements regarding electronic records and signatures provided for in § 7001 of Title 15 of the United States Code must be met. Id.
50. §§ 1798.29(g)(3), 1798.82(g)(3). When the cost of providing notice exceeds two hundred and fifty thousand dollars ($250,000), the affected class exceeds 500,000, or sufficient contact information does not exist, substitute notice may be given. Id.
51. Id.
52. §§ 1798.29(g)(3)(A)-(C), 1798.82(g)(3)(A)-(C), 1798.29(g)(3)(A)-(C).
accordance with its policies in the event of a breach of security of the system.53

(2) Implementation of Security

In addition to requiring notification in the event of a security breach, California law requires businesses that own or license personal information about Californians to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information,” and “to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”54 This section defines “personal information” the same way as in the notification provision, except “medical information” is included as an additional type of data businesses are required to secure.55 Moreover, the definition specifically excludes information that is “lawfully made available to the general public from federal, state, or local government records.”56

The law also excludes certain statutorily defined entities from its coverage, as well as a “business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section.”57 For such businesses, “[c]ompliance with that state or federal law shall be deemed compliance with this section with regard to those subjects.”58

The law also requires a “business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party” to “require by contract that the third party implement and maintain reasonable security procedures and practices.”59 Thus, the law reaches beyond companies that merely own personal information by requiring the addition of specific contractual language to information sales and licensing agreements.

(3) Record Destruction

Finally, the California law requires businesses to:

take all reasonable steps to destroy, or arrange for the destruction of a customer’s records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the

53. §§ 1798.29(h), 1798.82(h).
54. § 1798.81.5(b).
55. § 1798.81(d)(1)(D).
56. § 1798.81(d)(3).
57. § 1798.81(e)(5).
58. Id.
59. § 1798.81(c).
personal information in those records to make it unreadable or undecipherable through any means.\(^\text{60}\)

(4) Private Right Of Action

Along with the duties of the California statute, the law also provides that “any customer injured by a violation of this title may institute a civil action to recover damages.”\(^\text{61}\) “Customer” is defined as “an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.”\(^\text{62}\) In addition, “any business that violates, proposes to violate, or has violated” any provision of the California law may be enjoined.\(^\text{63}\) Notably, however, the law does not provide a cause of action for an individual who does not meet the strictures of the “customer” definition, yet whose personal information is compromised while in the possession of a business.

With respect to enforcement, the California law provides that any customer injured by a violation of any of the provisions discussed above may institute a civil action to recover damages.\(^\text{64}\) In addition, any business that “violates, proposes to violate, or has violated” any provision of the California law may be enjoined.\(^\text{65}\)

(5) Lingering Questions

While path-breaking in many respects, the California statute fails to address a host of important questions, and is rife with ambiguities. First, by requiring notification when a business “reasonably believes” that a California resident’s personal information has been acquired by an unauthorized person, the statute implies that businesses may be charged with inquiry notice of security breaches. This, in turn, raises the question of whether the statute creates an implicit duty on the part of businesses to conduct regular inspections of their databanks for possible security breaches. Perhaps even more troubling, the statute mandates notification regardless of whether the breach creates any real risk or threat that actual harm will befall the persons whose information is (or is reasonably believed to be) compromised. Risk-averse businesses may engage in preemptive notification, causing needless paroxysms of anxiety among the general public. In fact, in many cases, a high-profile mass data loss or mass security breach does not result in a single case of individual consumer identity theft resulting in actual economic damage to the consumer.

\(^{60}\) § 1798.81.
\(^{61}\) § 1798.84(b).
\(^{62}\) § 1798.80(c).
\(^{63}\) § 1798.80(e).
\(^{64}\) § 1798.84(b).
\(^{65}\) § 1798.84(e).
Second, once a business has determined that a breach has occurred, the statute provides little guidance as to what constitutes “expedient” notification. Nor does the statute indicate whether the expediency of the notice should be measured from the time that a business actually discovers the breach, or from the time that a business should have discovered the breach. The indeterminacy inherent in the statute’s command that notice be expediently given is compounded by the allowance for reasonable delay for the purpose of taking measures necessary to determine the scope of the breach and restore reasonable data system integrity. The tension between the command of expedient notice and the allowance for reasonable delay cannot be definitively resolved by reference to the language of the statute, giving rise to the need for judicial interpretation and situational decision-making.

Third, once a business has determined that a breach has occurred and is prepared to give notice, it must determine the type and extent of notification warranted under the circumstances.66 The statute provides little guidance regarding the content of the notification, and leaves open the possibility that “inadequate” notice will be deemed a failure to notify. For example, must a company merely inform persons affected by the breach that a breach has occurred, or must it offer advice regarding appropriate defensive or remedial steps a person may take — such as contacting a credit reporting agency or purchasing credit monitoring — to mitigate any possible negative outcomes? Moreover, businesses faced with the challenge of identifying the proper information to relay to affected persons must simultaneously contend with the task of deciding which persons to notify. To take but one example, who must be notified when a business determines that an unauthorized person viewed, but did not download, a large quantity of personal information? How certain can the business be that the information was “acquired” by the unauthorized person? Does the length of the view make a difference?

Fourth, the statute indicates that businesses may circumvent the notification requirement merely by encrypting their databanks.67 The statute is silent, however, as to whether minimum standards apply to the type of encryption used, or whether any type of encryption is sufficient to take advantage of this “safe-harbor” provision. In addition, the statute provides no guidance as to whether notification is necessary if a business reasonably believes that an unauthorized person has the ability to decipher encrypted data. For instance, what if the unauthorized person is a current or former employee who has access to the data; or what if the hacker acquires the key to decoding the cipher text?

Lastly, with respect to the requirement that businesses implement reasonable security measures, the statute fails to provide any indication regarding the type of measures required.68 One may infer from the notification

66. § 1798.82(g).
67. §§ 1798.81.5(d)(1), 1798.82(a), (e).
68. § 1798.81.5(a)-(c).
statute that encryption is *per se* a reasonable security measure. The statute provides no guidance, however, as to whether or how far a business must extend its protective efforts beyond the implementation of encryption. Businesses faced with this requirement are left adrift by the statute's penurious nature.

Despite these and other shortcomings, the California statute has served as a model for numerous state legislatures seeking to enact data security legislation. Although tracking the California statute in many respects, several of these statutes contain variations on the California theme worth examining in detail.

**b) Representative Statutes of Other States**

Since the passage of the California statute in 2003, a number of other states have enacted data security statutes modeled closely on the California law. Over thirty states now have either passed legislation governing some aspect of a mass security breach/data loss, or have legislation pending. As a general rule, these states have adhered closely to the structure of the California statute by requiring notification to consumers upon discovery of a breach in the security of a data system containing the consumers' personal information. Many of these states, however, have included innovations in their statutes differentiating their notification and security requirements from those implemented in the California statute.

**1) Element Of Harm**

One of the most noteworthy innovations is the inclusion of a "harm" requirement. States adopting the "harm" standard differ from California in that they require notification only in the event that the security breach is likely to result in some form of harm to the affected individuals, whereas the California statute requires notification in the event of a "breach" without considering whether harm may result. Florida's statute provides an illustrative example of this requirement. The Florida statute provides that:

notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for five years.69

The harm requirement represents an effort by states to rationalize the notification requirement; such states seek to reduce "overnotification" by requiring notification only when harm is likely to result. This rationalization may cause long-term difficulties, however, as it introduces an additional un-

defined variable into the notification process. While potentially burdensome, the California statute (and those following its lead) possesses the virtue of unambiguous certainty — if a security breach occurs, then notification is required.

States adopting the harm requirement place upon businesses the responsibility of determining in a relatively short period of time the potential long-term effects of a security breach. Given that an erroneous assessment of no harm followed by a decision not to notify is likely to result in civil liability, businesses faced with this choice are likely to err on the side of notification until some judicially defined parameters are established for judging the likelihood of harm and the reasonableness of such assessments. The upshot, however, is that in the long-term, the "harm" requirement will likely dampen "over-notification," making instances where notification is provided all the more effective by making them more rare.

(2) **Threshold Level Of Affected Consumers**

A second innovation found in a number of state statutes is a requirement that a business provide notice to consumer reporting agencies upon discovery of an information security breach affecting more than a threshold number of persons. A good example of this type of provision may be found in the Texas data security statute, which provides that:

> [i]f a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. 1681a, that maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.70

Provisions such as this would seem to promote efficiency by requiring a single actor to provide notification regarding the same information to both consumers and all credit reporting agencies nearly simultaneously, as opposed to relying on each individual consumer to contact all of the credit reporting agencies separately. However, it is unclear precisely what actions may/must be taken by credit reporting agencies upon receipt of such notification.

(3) **No Private Right of Action Under State Statute**

In addition to these innovations, a number of states have adopted statutes that provide only for administrative enforcement of their provisions. Unlike California, which explicitly provides a statutory cause of action for individual consumers in the event that a business fails to abide by the strictures of the data security law, the statutes of these states are silent as to the

---

ability of individual consumers to pursue claims against offending businesses. For example, New York’s data security statute provides:

[W]henever the Attorney General shall believe from evidence satisfactory to him that there is a violation of this article he may bring an action in the name and on behalf of the people of the State of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation.71

States providing only for administrative enforcement of their data security statutes likely will not bar pertinent common law causes of action by aggrieved consumers. However, the statutes themselves will not serve as a source for duty or liability in those cases.

(4) Unique Innovations

In addition to those discussed above, a number of additional statutory innovations have been adopted by individual states. The Nevada data security statute provides:

[A] data collector who provides notification may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector.”72 If the data collector prevails, it “may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney’s fees and costs and punitive damages when appropriate.73

The Florida data security statute provides that in the event of a breach of security, “[n]otification must be made no later than forty-five days following the determination of the breach . . .”74 This provision is significant in that it establishes a firm deadline for providing notice. The Florida statute also provides for administrative fines of $1,000 per day for the first thirty days of nondisclosure, $50,000 for each thirty-day period thereafter up to 180 days, at which time a maximum fine of $500,000 is imposed.75 The Rhode Island data security statute provides for a private cause of action for violations, additional civil penalties for “willful, intentional, or reckless” violations, and provides a safe harbor for businesses that provide notice “within ninety (90) days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, re-

73. Id.
74. FLA. STAT. ANN. § 817.5681(1)(a) (2005).
75. Id. at § 817.5681(b).
spectively." 76 Finally, New York's data security statute sets forth mandatory contents for any notice given, including "contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization." 77

Although the data security statutes of the several states closely track each other in both structure and content, they differ on a number of important points. Due to these differences, businesses possessing personal consumer information of residents from multiple states should develop a detailed understanding of the nuances of multiple state statutes in order to craft an effective response to a security breach. The compliance difficulties generated by this dizzying multiplicity of statutes cries out for a preemptive and comprehensive federal solution. At present, however, businesses are left with the unenviable task of canvassing a vast array of statutes any time they experience a potential data security breach or data loss.

c) Basic Corporate Compliance with Multiple State Laws

The momentum generated by the recent enactment of laws dealing with the maintenance and loss of personal information is likely to gain strength over the coming months and years, particularly if additional instances of information security breaches by high-profile businesses are discovered. Businesses that store or deal with personal information on employees, customers, or individuals residing in multiple states must keep pace with each of these laws and their individual nuances. The companies best-positioned to negotiate these new laws are those that (1) adopt robust information security practices and policies including the use of encryption or redaction and require third-party information customers and business partners to do the same, (2) institute additional practices and policies to insure that data stored on non-mainframe devices such as laptops, disks, and magnetic tapes is transferred and maintained in a secure manner, (3) take care to dispose of unneeded personal information in accordance with the most stringent state law standards, (4) monitor their systems and databases for instances of data breach or data loss, and (5) provide timely and appropriate notice to both consumers and law enforcement authorities upon learning of any actual mass data loss or data breach.

2. Proposed Federal Statutory Law

In light of the proliferation of high-profile mass data compromise, as well as the favorable reception of state laws requiring notification of information security breaches and requiring reasonable security measures, federal lawmakers have proposed a number of bills setting national information security standards. These bills reflect the diversity of views and approaches

76. R.I. GEN. LAWS § 11-49.2-9(d).
evident at the state level. Significantly, many of these bills contain provisions that would preempt many, if not all, of the previously mentioned state laws discussed above.

a) Senate Bill 1178

For example, Senate Bill 1178, introduced by Senators Smith, Stevens, Inouye, and Pryor, was approved by the Committee on Commerce, Science, and Transportation on April 25, 2007. The bill applies to any “sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes sensitive personal information.”

“Sensitive personal information” is defined as:

an individual’s name, address, or telephone number combined with 1 or more of the following data elements related to that individual:

(i) Social security account number, taxpayer identification number, or an employer identification number that is the same as or is derived from the social security number of that individual.

(ii) Financial account number, or credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual’s account.

(iii) State driver’s license identification number or State resident identification number.

This bill provides that:

[a] covered entity shall develop, implement, maintain, and enforce a written program for the security of sensitive personal information the entity collects, maintains, sells, transfers, or disposes of, containing administrative, technical, and physical safeguards—

(1) to ensure the security and confidentiality of such data;

(2) to protect against any anticipated threats or hazards to the security or integrity of such data; and

(3) to protect against unauthorized access to, or use of, such data that could result in substantial harm to any individual.

Furthermore, with regards to the requirements of being in compliance with the standards of the Federal Trade Commission [hereinafter FTC], it states that “[a] covered entity that is in full compliance with... [the FTC’s]

79. Id. at § 11(9).
80. Id. at § 2(a).
rules on Standards for Safeguarding Customer Information and Disposal of Consumer Report Information and Records is deemed to be in compliance with the requirements of subsection (a).”

With respect to notification of security breaches, Bill 1178 defines “Breach of Security” as an “unauthorized access to and acquisition of data in any form or format containing sensitive personal information that compromises the security or confidentiality of such information.” The bill requires notification to consumers when a “covered entity discovers a breach of security and determines that the breach of security creates a reasonable risk of identity theft.” Moreover, the bill defines “reasonable risk of identity theft” as meaning “that the preponderance of the evidence available to the covered entity that has experienced a breach of security establishes that identity theft for one or more individuals from the breach of security is foreseeable.” This standard of foreseeability echoes the standard for general negligence, and establishes a general bias in favor of notification in the event of a security breach. The bill also includes a list of separate requirements which would impose a duty on covered entities to give notice to both the FTC and consumers.

In a move that could anger consumer advocate groups, and would certainly affect how mass data compromise is dealt with in the court systems; there is no private right of action under the current version of the bill.

b) Senate Bills Competing With Bill 1178

Additional and potentially competing Senate Bills are also pending. For example, Senate Bills 239, 495 and 1202 have been submitted to the Senate Judiciary Committee for consideration. While there are stark differences in each piece of proposed legislation, the highlighted features of Senate Bill 1178 are instructive of the general direction being taken by Senate lawmakers with regard to potential mass data loss and breach legislation.

81. Id. at § 2(b).
82. Id. at § 11(1).
83. Id. at § 3(c)(1).
84. Id. at § 11(7).
85. Id. at § 3.
86. See generally Identity Theft Protection Act, S. 1178 (noting that Senate Bill 1178 does not currently provide consumers with a private right of action).
87. See generally Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007) (simply illustrating that, while there are additional and emerging schools of thought in this field of law, Senate Bill 1178 reflects the most popular school with regards to Senate lawmakers’ stance on this type of legislation).
 Proposed House Legislation

In addition to the Senate Bill 1178, Bills 1685 and 836 have been proposed in the House of Representatives, and like their upper-house counterparts, these potential pieces of legislation vary sharply with one another, yet they incorporate many of the features found in different state laws already in place across the country. However, until one or more of these proposed pieces of legislation becomes law, federal law will remain largely silent on regulation and private action with respect to mass data loss or mass security breach. It follows that, pending their enactment, the patchwork of inconsistent state laws will continue to fill the void.

B. Common Law Sources of Liability

In addition to the myriad of statutory sources of liability, businesses in possession of sensitive consumer information face the prospect of liability arising from familiar common law causes of action. A small but growing body of cases have addressed common law claims brought against businesses that have suffered security breaches resulting in the loss of confidential personal information.

1. Negligence Actions

Although not always successful, negligence claims are often asserted in mass data loss lawsuits. For example, in Stollenwerk v. Tri-West Healthcare Alliance, the federal district court for the District of Arizona addressed claims brought by current and former members of the U.S. military, and their dependents, seeking to hold Tri-West liable for the loss of their sensitive personal information. Tri-West, a “contractor and agent of the federal government [that] manage[d] a local region of the United States Department of Defense’s health insurance program,” suffered a security breach at its Phoenix, Arizona facility during which unauthorized personnel entered the facility and removed computer hard drives containing the plaintiffs’ “names, addresses, birth dates, and social security numbers.” Some of the individuals whose information was compromised filed suit against Tri-West, alleging “negligence, gross negligence, negligence per se, res ipsa loquitur, breach of


90. Id.
implied contract, and violations of the Privacy Act, the Ninth Amendment, and the Arizona Consumer Fraud Act."91 Two of the plaintiffs, Michael Stollenwerk and Andrea DeGatica, alleged that they suffered losses in the form of payments made to purchase credit monitoring services in an effort to protect themselves from identity theft.92 A third plaintiff, Mark Brandt, suffered actual identity theft when his "personal information was used on six occasions to open or attempt to open unauthorized credit accounts," and "more than $7,000" was charged to these accounts.93 On Tri-West's motion to dismiss pursuant to the Federal Rule Civil Procedure Section 12(b)(6),94 the court dismissed all of the plaintiffs' claims "with leave to amend the complaint as to the negligence, Arizona Consumer Fraud Act and Privacy Act claims."95 Subsequently, the plaintiffs filed their Second Amended Complaint alleging "two counts of Privacy Act violations, one count of negligence, one count of consumer fraud under the Arizona Consumer Fraud Act, and one count of breach of contract."96 Nevertheless, the court granted Tri-West's second motion to dismiss "as to all counts but the negligence claim."97

Following this dismissal, Tri-West moved "for summary judgment on the remaining negligence claim."98 In supporting their motion, Tri-West first argued that plaintiffs Stollenwerk and DeGatica had failed to raise a fact issue with respect to damages.99 Specifically, defendants maintained that Stollenwerk and DeGatica had failed to prove that the cost of credit monitoring was an injury sufficient to establish the tort of negligence and that Brandt had failed to prove causation.100 The court began its analysis of Stollenwerk's and DeGatica's claims by noting the similarities and differences between cases involving exposure to toxic substances or unsafe products in which medical monitoring constitutes an actionable injury, and the "exposure of confidential personal information."101 Moreover, the court noted that "[i]n both circumstances the individual may manifest more obvious injury, such as identity fraud or disease, after some period of time, and in neither instance is

91. Id.
92. Id. at *2.
93. Id. at *1, 5.
96. Tri-West, 2005 WL 2465906 at *2.
97. Id.
98. Id.
99. Id.
100. Id. at *2-3.
101. Id.
the later manifestation of patent injury guaranteed.”102 However, the court found the claims to be dissimilar, in that toxic tort cases “necessarily and directly involve human health and safety,” while “credit monitoring cases . . . do not.”103 Ultimately, the court held that this public health interest, in large part, formed the justification for the “departure from the general rule that enhanced future risk of injury cannot form the sole basis for a negligence action.”104

The court then concluded that “even if credit monitoring costs were sufficient injury to state a cause of action for negligence in some circumstances,” Stollenwerk and DeGatica had not presented sufficient evidence to survive summary judgment.105 The court found that Stollenwerk and DeGatica failed to raise a fact issue as to whether: (1) “the personal information on the stolen computers was ever exposed to the thieves involved;” (2) their own risk of suffering identity fraud had “significantly increased;” and (3) credit monitoring would substantially reduce the risk of identity fraud.106 Accordingly, the court granted TriWest’s motion for summary judgment with respect to Stollenwerk and DeGatica’s claims.107

The court then turned to TriWest’s assertion that Brandt had failed to raise a fact issue as to whether the security breach caused the subsequent theft of his identity.108 The court established that to avoid summary judgment, a “plaintiff must show that causation by the defendant’s act or omission is reasonably likely, not merely possible,” and that circumstantial evidence “must permit a jury to draw reasonable inferences, not merely speculate or conjecture.”109 Examining evidence produced by Brandt, the court noted six occasions after the burglary on which unknown persons attempted to open accounts in Brandt’s name.110 After not admitting evidence that one account was opened using Brandt’s former Delaware address, the court held that the evidence was insufficient to survive summary judgment—specifically, that “[s]tanding alone . . . Brandt’s evidence that the burglary preceded the incidents of identity fraud does not allow a reasonable jury to infer that the burglary caused the incidents of identity fraud.”111

102. Id. at *3.
103. Id. at *4.
104. Id.
105. Id. at *5.
106. Id.
107. Id.
108. Id.
109. Id. at *5-6.
110. Id. at *6.
111. Id. at *7.
Stollenwerk is significant for two reasons. First, it effectively bars negligence claims by individuals whose personal information has been compromised, but who have not yet suffered identity theft or other tangible loss at the hands of a third party. Because prudence demands that individuals whose information is compromised take affirmative steps to prevent identity theft, the Stollenwerk rule prevents a large portion of the costs generated by information loss from being shifted onto businesses victimized by information thieves. Moreover, this rule could extend to unintentional information loss in which criminal conduct plays no part.

Second, Stollenwerk is significant in that it raises a substantial, although not insurmountable, hurdle for plaintiffs who seek to establish causation by requiring some evidence of causation. Mere evidence of a security breach and exposure of personal information followed by identity theft or other loss is insufficient because such reasoning invokes the logical fallacy of post hoc ergo propter hoc.\(^\text{112}\) In practice, this evidentiary requirement may prove fatal to numerous claims given that many individuals have given identical personal information to more than one business.

However, a completely different outcome was the result in a case involving common law claims brought against an entity that experienced a security breach. In *Bell v. Michigan Council 25 of the American Federation of State, County, and Municipal Employees, ALF-CIO, Local 1023*, a group of 911 emergency service operators that suffered identity theft brought suit against their union alleging that the union’s treasurer had compromised their personal information.\(^\text{113}\) The treasurer, Yvonne Berry, had frequently taken work records containing personal information of union members home with her.\(^\text{114}\) Her daughter, Dentry Berry, was later arrested for participating in the appropriation of the service operators’ identities.\(^\text{115}\) Dentry admitted her involvement in the crime and was convicted on criminal charges, but denied taking any of the information from her mother.\(^\text{116}\) In a civil suit brought by the service operators against the union, the investigating officer testified that she could not conclusively establish how Dentry acquired the lists.\(^\text{117}\) The jury awarded the plaintiffs a collective sum of $275,000 based on a negligence theory of liability, whereupon the union appealed.\(^\text{118}\)

The Michigan Court of Appeals addressed the union’s claims that the trial court erred in denying its motions for directed verdict and judgment.

\(^{112}\) *Id.*


\(^{114}\) *Id.* at *4.

\(^{115}\) *Id.* at *1.

\(^{116}\) *Id.*

\(^{117}\) *Id.*

\(^{118}\) *Id.*
notwithstanding the verdict on the theory that the union did not owe the service operators a duty to protect them from “the unforeseeable criminal acts of a third party.” Additionally, the union argued that no special relationship existed between itself and its members such that the union had a duty to protect its members from unforeseeable risks. In determining this issue, the court first began by noting that “[t]he scope and extent of the duty to protect against third parties is essentially a question of public policy.” In its analysis, the court utilized the following factors to consider when determining whether a special relationship exists:

(1) the societal interests involved, (2) the severity of the risk, (3) the burden on the defendant, (4) the likelihood of occurrence of the risk, and (5) the relationship between the parties. Other factors to consider are the foreseeability of the harm, the defendant’s ability to comply with the duty, the victim’s inability to protect himself, the cost of providing protection, and whether the victim bestowed any economic benefit on the defendant.

Applying these factors, the court noted that the relationship between the union and its members was one of trust in which the union was obligated “to act on behalf of, and in the best interests of . . .” its members, and “that part and parcel of that relationship is a responsibility to safeguard its members’ private information.” The court also observed that “society has a right to expect that personal information divulged in confidence . . . will be guarded with the utmost care,” and that the union was “in the best position to protect [its members] because it controls who has access to its membership lists.” Moreover, the court noted that the risk of harm resulting from misuse of the service operators’ personal information was foreseeable based upon evidence that the union’s board members were aware that Berry frequently took lists containing members’ personal information home with her and discussed the risks of this activity on several occasions. The court found that this activity created a high severity of risk, given the increasing prevalence of identity theft and the costs associated with remedying it, and that the “commonplace” nature of identity theft made the risk of loss from criminal acts foreseeable. Additionally, the court observed that the union’s burden in securing its mem-

119. Id.
120. Id.
121. Id. at *2 (quoting Williams v. Cunningham Drug Stores, Inc, 379 N.W. 2d 458 (1985)).
122. Id. (quoting Murdock v. Higgins, 217 N.W. 2d 1 (1994)).
123. Id. at *3.
124. Id.
125. Id. at *4-5.
126. Id.
bers information was not great, but despite this fact, "the union had absolutely no procedures or safeguards in place to ensure that confidential information was not accessed by unauthorized persons."127

Based on its consideration of these factors, the court concluded that a special relationship existed between the union and its members such that the union owed the plaintiffs "a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information."128 The court was careful to limit its holding, however, noting that it did not intend its holding "to be construed as imposing a duty in every case where a third party has obtained identifying information and subsequently uses that information to commit the crime of identity theft."129 Instead, the court limited its holding "to the facts of this case where defendant knew confidential information was leaving its premises and no procedures were in place to ensure the security of the information."130

In Daly v. Metropolitan Life Insurance Co.,131 the Supreme Court of New York County, New York denied Metropolitan Life Insurance Company’s motion for summary judgment on Daly’s claim that it had negligently allowed custodial workers at its office facility access to her personal information and thereby enabled the workers to steal her identity. Daly completed a life insurance application and sent it to Met-Life. The application required Daly to provide personal information, including her full name, date of birth, driver’s license number, and her social security number. Upon receipt of Daly’s application, Met-Life forwarded to Daly a copy of its privacy policy outlining Met-Life’s efforts to safeguard customers’ personal information. After Daly’s application was made, Met-Life unintentionally allowed custodial staff access to Daly’s personal information. The staff members used Daly’s information to commit identity theft by establishing and using numerous credit card accounts in her name. Following discovery of the identity theft, Daly filed suit against Met-Life alleging two causes of action for negligence. Met-Life moved for summary judgment on Daly’s claims, arguing that Daly could not establish negligence, damages, or foreseeability.

The court rejected Met-Life’s arguments and held that summary judgment was not warranted.132 The court found that Daly had provided sensitive personal information to Met-Life relying on Met-Life’s promise that it would safeguard her information.133 In light of these facts, the court observed that Daly’s claim was "similar to those seen in causes of action for breach of

127. Id. at *5.
128. Id. at *5.
129. Id.
130. Id.
132. Id. at 537.
133. Id. at 535.
fiduciary duty of confidentiality.”134 The court found this duty of confidentiality arises from an implied covenant of trust and confidence, and that such a covenant could be inferred in business dealings where one party placed trust and confidence in another to exercise discretionary functions for the other party’s benefit.135 The court noted that “[w]hile this concept has never before been applied to issues surrounding the protection of confidential personal information, perhaps in the absence of appropriate legislative action, it should.”136 The court then concluded that:

[o]n the papers presented by the parties in this case, this court is convinced that Met Life had a duty to protect the confidential personal information provided by the plaintiffs. When Ms. Daly wished to purchase a life insurance policy from Met Life, she was required to, and agreed to supply Met Life with highly sensitive personal information including her full name, her social security number, and her date of birth. Implicit in this agreement was a covenant to safeguard this information.137

The court reserved judgment on the questions of whether Daly had adequately established damages, and whether negligence liability could be predicated on the criminal acts of third parties.138

Both Bell and Daly should give pause to businesses engaged in the practice of collecting the personal information of their customers. Although ostensibly limited to its facts, Bell provides that a business with knowledge that confidential information in its possession is being exposed to potential loss or theft must take remedial actions to prevent such loss or theft, or else risk tort liability if the information is compromised and some harm ensues. This reasoning assumes that the risk of identity theft is pervasive, and that the risk is common knowledge such that businesses in possession of sensitive personal information have a duty to take precautions to mitigate known risks to the security of the information. Daly reaches beyond the limited holding in Bell and assigns to businesses in possession of sensitive personal information a quasi-fiduciary duty to safeguard such information against loss. Notably, the court in Daly did not engage in an extensive discussion of facts giving rise to awareness on the part of Met-Life of a significant risk to Daly’s information, nor did it opine about the lack of security measures in place. Rather, the court’s finding of negligence seems to have been predicated solely on the fact that the information was compromised.

134. Id. at 534.
135. Id. at 535.
136. Id.
137. Id.
138. Id. at 536.
In *Guin v. Brazos Higher Education Service*, the plaintiff, Guin, asserted claims against Brazos based on the theft of a Brazos laptop during the course of the burglary of a Brazos' employee's home office. Guin's claims were based on Brazos' failure to comply with the duty of care established by the Gramm-Leach-Bliley Act regarding the protection and security of customer's non-public personal information. Guin also asserted a second negligence claim based on Brazos' purported failure to comply with its own privacy policy. The court granted Brazos' motion for summary judgment, holding that (1) Guin failed to provide any evidence that Brazos had failed to comply with Gramm-Leach Bliley, and (2) Guin failed to provide any evidence that Brazos could reasonably foresee that its laptop would be stolen from the home office of its employee during the course of a burglary. The *Guin* court further noted that even if Guin had been able to show a breach of duty, the court still would have dismissed his claims because he had not alleged or shown that he had actually been the victim of identity theft or suffered economic loss as a result of Brazos' data compromise. *Guin* teaches the important lesson that a mass security breach does not inherently result in a viable negligence claim. Courts will continue to insist that the elements of duty, breach of duty, causation, and appropriate accrued economic damages are satisfied.

2. Breach of Contract and Special Relationship Claims

Negligence is not the only common law claim arising from information security breaches. For instance, in *Kuhn v. Capital One Financial Corp.*, the Massachusetts Superior Court ruled on a motion for summary judgment against a complaint alleging breach of contract, breach of the implied covenant of good faith and fair dealing, negligence, misrepresentation, breach of

140. *Id.*
141. *Id.* at *3.
142. *Id.* at *4.
143. *Id.*
144. *Id.* at *6.
145. *Id.* at *5-6; see also Giordano v. Wachovia Secs., No. 06-476 (JBS), 2006 WL 2177036, at *4 (D. N.J. July 31, 2006) (plaintiff's claims based on data loss failed because data loss had not resulted in theft of identity — fear and threat of identity theft arising from data loss are insufficient); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1019-21 (D. Minn. 2006) (dismissing negligence and breach of contract claims arising from theft of computer containing sensitive consumer information because plaintiff failed to establish either accrued damages or a reasonable certainty of damages in the future).
fiduciary duty, and invasion of privacy. The plaintiff, Kuhn, brought these claims after an unidentified computer hacker broke into the website server of a merchant that accepted payment via Capital One Visa. The hacker gained access to Kuhn’s Capital One Visa card information. On the same day, Capital One contacted Kuhn to inform her that it had shut down her account. Kuhn later spoke with a Capital One representative who told her that no further action was necessary on her part. Capital One also sent her a letter to the same effect. Within days of the hacking incident, “approximately eighteen (18) fraudulent accounts were opened in plaintiff’s name, and $25,000 was wrongfully charged.”

Kuhn filed suit against Capital One, and Capital One subsequently filed a motion for summary judgment on all claims.

Turning first to Kuhn’s breach of contract claim, the court found that Capital One’s Privacy Notice and Customer Agreement, which provided that “we [Capital One] can protect you from identity theft, fraud, and unauthorized access to personal information about you[,]” governed Kuhn’s relationship with Capital One. Kuhn argued that this provision obligated Capital One to inform her that she needed to contact credit reporting agencies and place a fraud alert on her account in order to prevent identity theft. The court first noted that the provision applied only to Kuhn’s Capital One account. The court then found that the provision was located within a section of the Privacy Notice titled “Why we may collect and share information[,]” indicating that it was not a guarantee against illicit use so much as an invitation to share information. The court also observed that the Privacy Notice contained a link to Capital One’s website for persons who wanted to learn more about the policy. Noting that the link made Kuhn aware that the written Privacy Notice was not the only source of information about the policy, the court proceeded to find that the website contained the very information that Kuhn claimed Capital One had failed to provide. The court then observed that the Privacy Notice contained no guarantees against illicit use in the event of a lost or stolen card and limited Kuhn’s liability for wrongful charges to fifty dollars — a term that Capital One had honored by not holding Kuhn personally liable for the fraudulent charges to her account. Based on these findings, the court granted Capital One’s motion for summary judgment on Kuhn’s contract claim.

147. Id.
148. Id. at *3.
149. Id.
150. Id.
151. Id.
152. Id.
153. Id. at *4.
154. Id.
Capital One had fulfilled its contractual obligations by notifying her of the breach and deactivating her account.\textsuperscript{155}

The court next turned to Kuhn's negligence count. Finding that Kuhn produced no evidence that Capital One provided her personal information — such as her social security number, date of birth, pin number, or mother's maiden name — to retail establishments, the court concluded that the disclosure of Kuhn's credit card number could not have caused identity theft.\textsuperscript{156} The court rejected Kuhn's misrepresentation claim on a similar ground, finding no evidence that Capital One was aware of the disclosure of any information beyond Kuhn's credit card number.\textsuperscript{157} Given this lack of evidence, Kuhn could not establish that Capital One's statement that she need not "take any further action" was fraudulently or negligently made.\textsuperscript{158} Turning next to Kuhn's breach of fiduciary duty claim, the court held that Capital One's relationship to Kuhn was one of creditor-debtor and that no fiduciary duties arose from this relationship.\textsuperscript{159} Lastly, the court rejected Kuhn's invasion of privacy claim because she produced no evidence to show that Capital One bore any responsibility for the security breach.\textsuperscript{160}

On appeal, the Massachusetts Appeals Court reversed the judge's grant of summary judgment on all counts, citing Kuhn's affidavit, which stated "at least one Capital One representative had told her that 'the security breach had occurred at Capital One.'"\textsuperscript{161} In doing so, however, the court acknowledged that Kuhn's assertion "may only provide [her] a toehold, which may very well disappear through later discovery."\textsuperscript{162}

*Kuhn* is significant because it highlights the importance of conveying accurate information to consumers whose personal information is compromised. Given the notification requirements adopted in most states, businesses that experience breaches must not only concern themselves with notifying affected consumers, but also with accurately notifying consumers about appropriate steps to take. It would be a sad irony for a business to notify a customer in an effort to comply with a notification statute only to be held liable on a misrepresentation theory for negligently conveying incorrect information that causes the consumer additional loss.

\textsuperscript{155} Id.

\textsuperscript{156} Id. at *5.

\textsuperscript{157} Id.

\textsuperscript{158} Id.

\textsuperscript{159} Id. at *6.

\textsuperscript{160} Id. The court also disposed of one last claim based on the Massachusetts deceptive trade practices statute. Id. at *7.


\textsuperscript{162} Id. at *3.
In Jones v. Commerce Bancorp, Inc., the plaintiff, Jones, claimed commercial bad faith, consumer fraud, intentional and negligent infliction of emotional distress, negligence, breach of fiduciary duty, and breach of contract. In May of 2005, several Commerce employees were arrested for the theft of large amounts of confidential information from the company’s databases. On May 22, 2005, Jones learned that funds were missing from her business checking account and that a separate, fraudulent account had been opened in her name. Commerce eventually credited the fraudulently withdrawn funds back to Jones’ account. The court granted Commerce’s motion to dismiss on the commercial bad faith, consumer fraud and infliction of emotional distress claims, but found that Jones had successfully stated claims for negligence, breach of fiduciary duty, and breach of contract.

In upholding the negligence claim, the court relied on Jones’ allegations that Commerce knew of the fraudulent activity within its branch network and failed to stop it. In refusing to dismiss Jones’ claim for breach of fiduciary duty, the court reasoned that, given that Jones was required to submit confidential data to Commerce, and that Commerce’s “Booklet with Deposit Rules, Regulations, Disclosures and Privacy Notice” represented that such data was protected by a variety of measures, “[u]nder these circumstances, plaintiff was entitled to rely on Commerce’s superior expertise to safeguard her personal confidential information.”

In her pleadings, Jones characterized Commerce’s “Booklet with Deposit Rules, Regulations, Disclosures and Privacy Notice” as a contract. Jones alleged that this “contract” was breached when Commerce allowed unauthorized withdrawals from Jones’ account. Commerce did not challenge Jones’ interpretation of the Booklet as a contract, but rather, claimed that since it replaced the fraudulently withdrawn funds, there could not have been damages from any breach. The court disagreed, reasoning that “[p]laintiff may be able to prove some (albeit minimal) damages stemming from her inability to access her funds for several weeks prior to their restoration by Commerce.”

164. Id. at *1.
165. Id.
166. Id.
167. Id. at *5.
168. Id. at *3.
169. Id.
170. Id. at *4.
171. Id.
172. Id.
Jones is noteworthy in that it suggests, first, that booklets and similar literature describing security policies could conceivably be construed as contracts between the institutions promulgating them and victims of identity theft.\footnote{Id.} Second, Jones proposes that the inability to access funds for a short period of time due to identity theft could itself be sufficient to show damages in a claim for breach of contract.\footnote{Id.}

3. Risk Of Future Injury Insufficient

In Hendricks v. DSW Shoe Warehouse, Inc.,\footnote{Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 776 (W.D. Mich. 2006).} the plaintiff, on behalf of herself and a class of similarly situated individuals, brought suit against DSW Shoe Warehouse after the breach of DSW’s consumer information database.\footnote{Id. at 777.} Although Hendricks’s information was not used for any fraudulent purposes, Hendricks purchased credit monitoring services to protect against future identity theft. Hendricks sought, as damages, the costs of the credit monitoring services she purchased.\footnote{Id. at 778.} DSW moved to dismiss the claims asserted against it.\footnote{Id.} The court granted DSW’s motion on the grounds that the plaintiff had not suffered a legally recognizable injury.\footnote{Id. at 783.}

Because the plaintiff had not been the victim of actual identity theft, she had no legally recognizable injury:

There is no existing Michigan statutory or case law authority to support plaintiff’s position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss. Indeed, there is reason to believe that Michigan’s highest court would reject a novel legal theory of damages which is based on a risk of injury at some indefinite time in the future.\footnote{Id. at 783. See also Bell v. Acxiom, No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (holding that the plaintiff did not have standing to sue under the case-or-controversy requirement since she did not have evidence to show that her personal information was included in a recent data loss and since she had not suffered any damages other than an increased risk of identity theft).}

Because identity theft is the concern most often associated with a mass data breach, many consumer-plaintiffs have advanced legal theories that allege damages arising from the fear or risk of future identity theft. Hendricks, and other decisions like it, demonstrate that damage claims based on a future risk of injury are founded on shaky ground. The emerging trend seems to be...
that actual theft of identity or unauthorized charges are a prerequisite for a successful claim based on a mass data breach.

4. Claims Brought by Parties other than Consumers after Mass Data Compromise

Three interrelated cases arising from the breach of a wholesaler's electronic records are worth examining in detail: Pennsylvania State Employees Credit Union v. Fifth Third Bank ("PSECU"),180 Sovereign Bank v. BJ's Wholesale Club, Inc., (Sovereign Bank)181, and Banknorth, N.A. v. BJ's Wholesale Club, Inc.182

In PSECU, the plaintiff brought claims for breach of contract, negligence, equitable indemnification, and unjust enrichment against BJ's Wholesale Club and Fifth Third Bank, who processed BJ's Visa card transactions.183 In PSECU, the court considered several claims brought by PSECU against BJ’s Wholesale Club, a Visa merchant that accepted Visa card transactions from its customers, and Fifth Third Bank, an acquiring bank that processed Visa card transactions on behalf of BJ’s. The lawsuit arose after unauthorized third parties obtained access to BJ’s electronic records and stole Visa card magnetic-strip information from over 20,000 Visa cards issued by PSECU. BJ’s software had improperly stored consumers’ information instead of deleting it upon completion of each transaction, thereby enabling the thieves to access and steal the magnetic-strip information from over 20,000 Visa cards issued by PSECU. As damages, PSECU sought the cost of replacing the cards that had been compromised by the breach of BJ’s system.184 Fifth Third and BJ’s filed separate motions to dismiss under Fed. R. Civ. P. 12(b)(6), arguing that none of PSECU’s claims stated a valid cause of action.185

183. PSECU, 398 F. Supp. 2d at 319-20.
184. Id. at 323.
185. Id. at 320. In addition to these claims, BJ’s filed a third-party complaint against IBM seeking indemnity for any damages received by PSECU. BJ’s had contracted with IBM to provide credit card payment processing software, and had specifically requested that IBM disable the “Store and Forward” feature, which stored credit card data accepted after the software was taken off-line for processing when the system came back on-line. IBM failed to disable the “Store and Forward” feature, and BJ’s alleged that this failure contributed to the loss of consumer data. The U.S. District Court for the Middle District of Pennsylvania granted IBM’s motion to dismiss in part in Pennsylvania State
Looking first to PSECU’s claims against BJ’s, the court held that PSECU’s breach of contract claim failed because PSECU was not a third-party-beneficiary of the contract between BJ’s and Fifth Third Bank.\textsuperscript{186} BJ’s and Fifth Third had entered into credit and debit card processing agreements which prohibited BJ’s from disclosing Visa cardholder account information to unauthorized third parties, and from retaining or storing Visa magnetic strip data subsequent to transaction authorization. The agreements also contained explicit disclaimers stating that they were not made for the benefit of, and could not be enforced by, any third party. Based on these disclaimers, PSECU’s breach of contract argument was rejected.\textsuperscript{187}

The court next held that PSECU’s negligence claim was barred by the economic loss rule.\textsuperscript{188} Pennsylvania’s economic loss rule was described as barring “negligence claims seeking recovery for ‘economic damages’ or ‘losses’ unless there has also been physical injury either to a person or property.”\textsuperscript{189} Significantly, the court rejected PSECU’s argument that the economic loss doctrine did not apply because the data security breach caused a complete loss of all Visa cards rendered useless by the breach.\textsuperscript{190} The court held that “[a] plaintiff must show physical damage to property, not its tangible nature,” and that “costs of replacing the cards” were economic losses.\textsuperscript{191}

The court then addressed PSECU’s equitable indemnification and unjust enrichment claims. The court dismissed PSECU’s equitable indemnification claim on grounds that PSECU had paid no damages for which it was entitled to receive indemnification; rather, it had merely fulfilled a contractual obligation to its customers by replacing their Visa cards after the cards were compromised.\textsuperscript{192} Further, the court dismissed PSECU’s unjust enrichment claim on grounds that the replacement of the cards by PSECU did not confer a benefit on BJ’s because the replacement was done in fulfillment of PSECU’s contractual responsibility to its customers, and any benefit conferred on BJ’s was incidental.\textsuperscript{193}

\begin{flushright}
\end{flushright}

\textsuperscript{186} \textit{PSECU}, 398 F. Supp. 2d at 323-26.
\textsuperscript{187} \textit{Id}.
\textsuperscript{188} \textit{Id.} at 326-30.
\textsuperscript{189} \textit{Id.} at 327.
\textsuperscript{190} \textit{Id.} at 330.
\textsuperscript{191} \textit{Id.} Turning to Pennsylvania state law, the court also rejected PSECU’s contention that the economic loss doctrine applies only when the plaintiff and defendant are in privity of contract. \textit{Id.} at 329.
\textsuperscript{192} \textit{Id.} at 330.
\textsuperscript{193} \textit{Id.} at 331.
Turning to PSECU’s claims against Fifth Third Bank, the court dismissed PSECU’s negligence, equitable indemnification, and unjust enrichment claims on largely the same grounds it relied upon to reject PSECU’s claims against BJ’s. However, the court refused to dismiss PSECU’s breach of contract claim against Fifth Third. PSECU alleged that it was a third-party-beneficiary of a contract between Visa and Fifth Third requiring Fifth Third to provide assurances that its merchants (such as BJ’s) would comply with Visa’s operating regulations, which prohibited the disclosure and retention of account and magnetic-strip information, and required Fifth Third to take responsibility for losses caused by a merchant’s failure to abide by the regulations. The court found that this provision in the contract between Visa and Fifth Third was made for the purpose of securing the Visa card network in a way that directly benefited issuing banks such as PSECU, and that this purpose was within the contemplation of the parties at the time of contracting. The court concluded:

The purpose of the agreement was to make the Visa network safe for issuing banks, either those already in the network or those contemplating joining it, by assuring them that their customer information will only be in a merchant’s possession long enough to make a transaction. Thus, the third-party-beneficiary relationship for issuing banks was within the contemplation of Visa and Fifth Third at the time of contracting. Further, since Visa intended to give issuing banks like PSECU the benefit of Fifth Third’s performance, PSECU has third-party-beneficiary status under Fifth Third’s member agreement with Visa.

Demonstrating the unsettled nature of the law in this area, on Fifth Third’s second motion for reconsideration, the court then reversed itself, holding that PSECU was not an intended third-party-beneficiary of the contract. The court’s ruling hinged on a new determination that Visa did not intend for PSECU to benefit from its contract with Fifth Third. Therefore, whether Fifth Third intended PSECU to be a third-party beneficiary to its agreement with Visa was irrelevant because both parties to the agreement were required to have the intent to benefit PSECU for PSECU’s contract claim to survive.

The court reached a slightly different result in Sovereign Bank. There, Sovereign Bank asserted claims against BJ’s based on the fact that some of the stolen credit card information belonged to customers of Sovereign

194. Id. at 336.
195. Id.
196. Id.
197. Id.
198. Id.
Bank.199 Sovereign Bank’s damages were based on the new cards it issued to its customers, as well as the reimbursements it made to its customers for unauthorized charges arising from the BJ’s breach.200 The court dismissed Sovereign’s breach of contract claim, finding that Sovereign was not a third-party-beneficiary of BJ’s contract with Visa.201 However, the court determined that BJ’s owed Sovereign’s customers a duty of care, which was not excused by the criminal acts of the identity thieves.202 The court also determined that Sovereign had a valid third party breach of contract claim against Fifth Third.203 Thus, Sovereign was able to maintain its negligence claim against BJ’s and its contract claim against Fifth Third.204

In the Banknorth case, the Court took an entirely different approach, even though the facts and claims were almost identical to the Sovereign Bank case.205 There, the Court dismissed each of the plaintiff’s claims against BJ’s and Fifth Third, held that Banknorth was not a third-party beneficiary to the BJ’s-Visa-Fifth Third contracts, and found that Banknorth’s negligence claim against BJ’s failed under Maine’s economic-loss rule.206

The inconsistent holdings in these three cases demonstrate how unsettled the law of data loss and breach is, especially where the underlying claims are between parties other than the consumers affected by the data breach. On identical facts and claims, three plaintiffs obtained very different results. Despite their inconsistent results, these cases are indicators of the analysis a court will likely undertake when examining the liability of third parties who are indirectly damaged by a data breach.

5. Deceptive Trade Practices Liability

Private litigants have struggled to maintain deceptive trade practices claims against companies based on security breaches or compromises of personal information. However, in United States v. Choicepoint, Inc., the FTC asserted deceptive trade practices claims against Choicepoint.207 The FTC alleged that Choicepoint had allowed several imposters to access sensitive information contained in Choicepoint’s database.208 Although the claims re-

---

200. Id.
201. Id. at 191.
202. Id. at 193-96.
203. Id. at 203.
204. Id. at 206.
206. Id. at *216.
208. Id.
Receiving the most publicity were all based on impermissible access under the Fair Credit Reporting Act, the FTC also based their claims on Choicepoint's failure to protect the sensitive personal information contained in its database as advertised in its privacy policy statement. Based on those representations by Choicepoint, the FTC made deceptive trade practices claims against Choicepoint under Section 5 of the Federal Trade Commission Act ("FTC Act").

Ultimately, the FTC and Choicepoint entered into a stipulated final judgment and order for civil penalties. The stipulation included an agreement that the FTC's deceptive trade practices claims stated a claim on which relief could be granted. Choicepoint paid a $10,000,000 civil penalty, partly based on those claims.

The Choicepoint case may be distinguishable for two reasons. First, only the FTC can assert FTC Act deceptive trade practices claims. Second, a stipulated final judgment entered by the court may not be as indicative as a contested judgment of the direction the law is going. However, the Choicepoint case suggests that deceptive trade practices claims may be a viable cause of action where representations regarding privacy and security have been made by a company who subsequently suffers a mass security breach.

C. Key Case To Watch In 2006 and 2007

There are several cases pending across the country that have arisen from the front-page data loss and data breach stories discussed earlier in this article. Even in instances where the mass data loss and data breach have not resulted in identity theft, consumers have asserted claims against the entities they have deemed responsible for the potential compromise of their personal information. Because of the uncertainty of the law surrounding data loss and data breach, the outcome of those claims is uncertain. The case that may be most indicative of corporate exposure to data loss, and the subsequent potential recovery for consumers, is Parke v. Cardsystems Solutions, Inc.

Although the Parke case is currently subject to an automatic stay due to the bankruptcy of one of the defendants, the case could be the best possible indicator of where the law of data loss and breach is headed once the stay is lifted.

209. Id.
In *Parke*, Cardssystems acted as a third-party data processing vendor for both VISA and Mastercard.\(^{214}\) Computer hackers allegedly hacked into Cardssystems’ computer database, then compromised and stole consumer data relating to approximately forty million consumers.\(^{215}\) As a result, a class action was filed against Cardssystems, VISA, Mastercard, and other defendants in California Superior Court. The class action plaintiffs asserted claims under California’s data loss and breach statute, as well as claims for negligence and deceptive trade practices.

The *Parke* case is significant for two reasons. First, the class plaintiffs have asserted claims under the California statute that has served as a model for most of the other state legislation passed or pending regarding data loss or data breach. Second, the class plaintiffs have asserted that they suffered from unauthorized charges on their credit cards. Thus, *Parke* offers a case with alleged actual damages resulting from consumer identity theft, a representative statutory regulatory scheme, a private right of action, and additional causes of action that have not yet been fully tested.

**VI. Conclusion**

Consumers, corporations, and the lawyers representing them are on the cusp of a new legal frontier. Five years ago, a mass security breach or mass data loss was an afterthought as individual identity theft cases captured the attention of the media and filled court dockets. Three years ago, the first comprehensive statute dealing with mass data loss and breach was enacted in California. Today, mass compromises of consumer information are often front-page news. Laptops are stolen, computer disks and reports are lost in the mail, rogue employees are improperly accessing data from the inside, and skilled hackers and crime rings are stealing information from the outside.

Even as mass data loss and breach becomes predictable and commonplace, uncertainty remains regarding the law that relates to these incidents. Inconsistent statutory schemes remain relegated to some, but not all, states. Competing federal laws wait in the wings to preempt the field. In the meantime, corporate counsel struggles to determine what conduct complies with the law when a mass data compromise occurs, and both consumer lawyers and courts struggle to determine when a viable claim based on a mass data loss of breach can be brought.

Until more common law precedent is developed and a comprehensive statutory scheme is in place that governs all consumer information regardless

the action back to State Court on equitable grounds, noting specifically that plaintiff’s claims are all based on state law and implicate issues on which California courts have yet to rule. *Parke*, 2006 WL 2917604, at *4.


of the consumer’s residence, representatives of consumers and corporations would do well to look to the California statutory scheme for compliance, and assume common law claims will be limited to incidents where a consumer suffers actual damages as a result of identity theft arising from a mass data breach or loss.
## VII. STATE STATUTES GOVERNING SECURITY BREACHES

<table>
<thead>
<tr>
<th>State</th>
<th>Citation</th>
<th>Effective Date</th>
<th>Private Right of Action?</th>
<th>Reasonable Likelihood of Harm Required for Notice?</th>
<th>Unique Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arizona</td>
<td>ARIZ. REV. STAT. ANN. § 44-7501 amended by 2007 Ariz. Legis. Serv. 1042 (West)</td>
<td>12/31/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Arkansas</td>
<td>ARK. CODE ANN. §§ 4-110-101 to -108</td>
<td>8/12/2005</td>
<td>No</td>
<td>Yes</td>
<td>Covers information in physical or non-electronic form</td>
</tr>
<tr>
<td>California</td>
<td>CAL. CIVIL CODE §§ 1798.80 to .84</td>
<td>7/1/2003</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Colorado</td>
<td>COLO. REV. STAT. § 6-1-716</td>
<td>9/1/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Connecticut</td>
<td>CONN. GEN. STAT. § 36A-701b</td>
<td>1/1/2006</td>
<td>No</td>
<td>Yes</td>
<td>Government entities not required to provide notice.</td>
</tr>
<tr>
<td>Delaware</td>
<td>DEL. CODE ANN. tit. 6, §§ 12B-101 to -104</td>
<td>6/28/2005</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>District of Columbia</td>
<td>D.C. CODE §§ 28-3851 to -3853</td>
<td>1/1/2007</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Florida</td>
<td>FLA. STAT. § 817.5681</td>
<td>7/1/2005</td>
<td>No</td>
<td>Yes</td>
<td>45-day deadline for notification.</td>
</tr>
<tr>
<td>Georgia</td>
<td>GA. CODE ANN. §§ 10-1-910 to -912</td>
<td>5/5/2005</td>
<td>No</td>
<td>No</td>
<td>Covers information brokers only.</td>
</tr>
<tr>
<td>Hawaii</td>
<td>HAW. REV. STAT. §§ 487N-1 to -4</td>
<td>1/1/2007</td>
<td>Yes</td>
<td>Yes</td>
<td>Precludes actions against government agencies.</td>
</tr>
<tr>
<td>Idaho</td>
<td>IDAHO CODE ANN. §§ 28-51-104 to -107</td>
<td>7/1/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Illinois</td>
<td>815 ILL. COMP. STAT. 530/1 to /20</td>
<td>1/1/2006</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Code/Statute Description</td>
<td>Date</td>
<td>Private Access</td>
<td>Public Access</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indiana</td>
<td>IND. CODE § 24-4.9 (private) IND. CODE § 4-1-11 (government)</td>
<td>6/30/2006</td>
<td>No</td>
<td>Private: Yes Gov.: No</td>
<td></td>
</tr>
<tr>
<td>Kansas</td>
<td>KAN. STAT. ANN. § 50-7a01</td>
<td>1/1/2007</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Louisiana</td>
<td>L.A. REV. STAT. ANN. §§ 51:3071 to :3076</td>
<td>1/1/2006</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Maine</td>
<td>ME. REV. STAT. ANN. tit. 10, §§ 1346 to 1350-A</td>
<td>1/31/2006</td>
<td>No</td>
<td>No</td>
<td>Covers Information Brokers only.</td>
</tr>
<tr>
<td>Michigan</td>
<td>MICH. COMP. LAWS ANN. § 445.72</td>
<td>7/2/2007</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Minnesota</td>
<td>MINN. STAT. § 325E.61</td>
<td>1/1/2006</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Montana</td>
<td>MONT. CODE ANN. §§ 30-14-1701 to -1705</td>
<td>3/1/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Nebraska</td>
<td>NEB. REV. STAT. §§ 87-801 to -807</td>
<td>7/14/2006</td>
<td>No</td>
<td>Yes</td>
<td>Protects &quot;unique biometric data&quot; in addition to other personal information.</td>
</tr>
<tr>
<td>Nevada</td>
<td>NEV. REV. STAT. §§ 603A.010 to .920</td>
<td>1/1/2006</td>
<td>No</td>
<td>No</td>
<td>Data collector can sue one who misappropriates information for cost of notice.</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>N.H. REV. STAT. ANN. §§ 359-C:19 to :21</td>
<td>1/1/2007</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>New Jersey</td>
<td>N.J. STAT. ANN. § 56:8-163</td>
<td>1/1/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>N.Y. GEN. BUS. LAW § 899-aa</td>
<td>12/7/2005</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>North Carolina</td>
<td>N.C. GEN. STAT. §§ 75-60 to -65</td>
<td>12/1/2005</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>North Dakota</td>
<td>N.D. CENT. CODE §§ 51-30-01 to -07</td>
<td>6/1/2005</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Code Reference</td>
<td>Date</td>
<td>Private</td>
<td>Government</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------</td>
<td>------------</td>
<td>---------</td>
<td>------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Ohio</td>
<td>OHIO REV. CODE ANN. § 1349.19 (private) OHIO REV. CODE ANN. § 1347.12 (government)</td>
<td>2/17/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Oklahoma</td>
<td>OKLA. STAT. tit. 74, § 3113.1</td>
<td>6/8/2006</td>
<td>No</td>
<td>No</td>
<td>Applies to government agencies only.</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>73 PA. CONS. STAT. §§ 2301 to 2329</td>
<td>6/20/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Rhode Island</td>
<td>R.I. GEN. LAWS §§ 11-49.2-1 to -7</td>
<td>3/1/2006</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Tennessee</td>
<td>TENN. CODE ANN. § 47-18-2107</td>
<td>7/1/2005</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Texas</td>
<td>TEX. BUS. &amp; COM. CODE ANN. §§ 48.001 to .201</td>
<td>9/1/2005</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Utah</td>
<td>UTAH CODE ANN. § 13-44-101 to -301</td>
<td>1/1/2007</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Vermont</td>
<td>VT. STAT. ANN. tit. 9, § 2430</td>
<td>1/1/2007</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Washington</td>
<td>WASH. REV. CODE § 19.255.010</td>
<td>7/24/2005</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>