March 2016

Once More Unto the Breach: An Analysis of Legal, Technological, and Policy Issues Involving Data Breach Notification Statutes

Dana J. Lesemann

Please take a moment to share how this work helps you through this survey. Your feedback will be important as we plan further development of our repository.

Follow this and additional works at: http://ideaexchange.uakron.edu/akronintellectualproperty

Part of the Intellectual Property Law Commons

Recommended Citation

ONCE MORE UNTO THE BREACH: AN ANALYSIS OF LEGAL, TECHNOLOGICAL, AND POLICY ISSUES INVOLVING DATA BREACH NOTIFICATION STATUTES

Dana J. Lesemann

I. Introduction ................................................................. 204
II. Background .................................................................... 206
III. Personal Information Defined ........................................ 209
    A. The California Model ............................................. 209
    B. Other State Variations ............................................. 212
IV. Defining a Data Breach .................................................. 212
    A. The Strict Liability Model ....................................... 213
    B. The Risk Assessment Model .................................... 215
    C. Blending Definitions: Risk Assessment and Strict Liability ...................................................... 217
    D. Conducting the Investigation .................................... 218
    E. Safe Harbor under Federal Banking Statutes and Other Laws ...................................................... 220
    F. Recommendation: States Should Adopt the Risk Assessment Model which Presents Greater Benefits for the Consumer over the Strict Liability Approach ...................................................... 221
V. When Time Limits Are Not Really Time Limits ................. 222
    A. Penalties ..................................................................... 224
    B. Enforcement and Litigation under the Data Breach Statutes ...................................................... 225

1. WILLIAM SHAKESPEARE, KING HENRY THE FIFTH, act 3, sc. 1.
2. Managing Director and Deputy General Counsel, Stroz Friedberg; Adjunct Professor of Law, Howard University School of Law. Stroz Friedberg is a consulting and technical services firm specializing in digital forensics, network intrusion, data breach response, and cyber-security investigations. I am grateful to my colleagues at Stroz Friedberg for their assistance in developing this article, particularly the research of Steven Mecca and the expert editorial review of Miriam Birnbaum, Thomas Harris-Warrick, and Paul Luehr. Thanks also to Ahmed Baset, Howard University School of Law, Class of 2010. All errors, of course, remain my own.
I. INTRODUCTION

Companies facing the loss of a laptop or a compromised server have long waged battles on several fronts: investigating the source of the breach, identifying potentially criminal behavior, retrieving or replicating lost or manipulated data, and putting better security in place. As recently as seven years ago, the broader consequences of a data breach were largely deflected from the party on whose resource the data resided and instead rested essentially on those whose data was compromised. Today, however, with the patchwork quilt of domestic data breach statutes and penalties, most companies forging “unto the breach” would consider paying a ransom worthy of King Henry to avoid the loss of its consumers’ identities through theft or manipulation.

The cost to businesses of responding to data breaches continues to rise. According to the Ponemon Institute, the average cost of data breaches to the businesses it surveyed increased from $6.65 million in 2008 to $6.75 million in 2009. The per-record cost of the data breaches experienced by the companies it surveyed was $202 in 2009, only $2 more per record more than the average in 2008 but a $66, or 38% overall increase since 2005. The most expensive data breach in the 2009 Ponemon survey was nearly $31 million; the least expensive was $750,000. In confronting a data breach, a company has to contend with a multitude of issues: the costs of replacing lost equipment, repairing the breach, and thwarting a potentially criminal act. Some specific

4. Id. at 12.
5. Id. at 14.
industries have their own privacy laws. For example, financial firms must contend with the reporting requirements associated with the federal Gramm-Leach-Bliley Act, and health care companies face broad reporting requirements under the new HITECH Act. Across the broader economy, however, attorneys and companies worry most about a thicket of data breach notification statutes enacted by forty-five states and the District of Columbia. These statutes expose law firms and their clients to conflicting time limits, reporting requirements, fines, and potentially millions of dollars in penalties and civil liability—not to mention reputational risk. The forty-six data breach notification statutes vary widely from state to state and, most critically, focus not on the location of the breach or where the company is incorporated, but on the residence of the victim. Therefore, a company facing a data breach must comply with the state laws of each of its affected consumers. A company’s multi-state or Internet presence only extends the potential web of specific time limits and other often conflicting requirements for notifying consumers.

This Article addresses the legal, technological, and policy issues surrounding U.S. data breach notification statutes and recommends steps that state and federal regulatory agencies should take to improve and harmonize those statutes. Part I of this Article provides background on the data breaches that gave rise to the enactment of notification statutes. Part II addresses the varying definitions of “personal information” in the state statutes—the data that is protected by the statute and whose breach must be revealed to consumers. Part III analyzes how states define the data breach itself, particularly whether states rely on a strict liability standard, on a risk assessment approach, or on a model that blends elements of both in determining how and when companies have to notify consumers of a breach. Part IV discusses the time limits companies face, penalties for non-compliance, litigation under the statutes, and state enforcement of the statutes. Finally, Part V presents specific recommendations for the state legislatures and enforcement agencies and for Congress, as well as for companies facing data breaches.

8. See infra Part I.
Data breach statute fever began in 2002 after a California state database, which contained the social security numbers and other personal information of more than 250,000 state employees, was compromised. The breach was not discovered for a month and affected employees were not notified for several weeks after that. This breach—and the way it was handled—led the California legislature to enact the country’s first data breach notification statute later that year. In February 2005, ChoicePoint, a commercial data broker, announced that it had unwittingly sold personal information regarding 145,000 individuals to a group of people engaged in identity theft. The company later stated that the breach had actually occurred and had been uncovered in September 2004, five months before ChoicePoint had alerted the victims in California pursuant to the California statute. Then, significantly, victims in other states were not notified, because no legal mandate required notification. This strict compliance with the letter of the law became a public relations nightmare for ChoicePoint when non-California victims found out they had been omitted from the notice. The Federal Trade Commission (FTC) subsequently sued ChoicePoint for not having reasonable procedures to screen prospective subscribers, for turning over consumers’ sensitive personal information to subscribers whose applications raised obvious “red flags,” and for making false or misleading statements about its privacy practices. In 2006, ChoicePoint agreed to pay the FTC $10 million in civil penalties—a record amount—and agreed to make $5 million available to consumers in restitution. The following year the company settled with
forty-four state attorneys general to resolve allegations that ChoicePoint had failed to adequately maintain the privacy and security of consumers' personal information. 16

A flood of disclosures similar to ChoicePoint’s soon followed and in 2005, ten states enacted data breach notification statutes. 17 Seventeen states followed suit in 2006, 18 another nine in 2007, 19 five in


18. The ten states to enact data breach notification statutes in 2005 were Arkansas, 2010 Ark. Leg. Serv. § 4-86-107 (West); Delaware, DEL. CODE ANN. tit. 6, § 12B-103 (2010); Florida, FLA. STAT. ANN. § 817.5681 (West 2010); Georgia, GA. CODE ANN. § 10-1-912 (West 2010); New York, N.Y. GEN. BUS. LAW § 899-aa (McKinney 2010); North Carolina, N.C. GEN. STAT. ANN. § 75-65 (West 2010); North Dakota, N.D. CENT. CODE § 51-30-02 (2010); Tennessee, TENN. CODE ANN. § 47-18-2107 (West 2010); Texas, TEX. BUS. & COM. CODE ANN. § 521.053 (Vernon 2010); and Washington, WASH. REV. CODE ANN. § 19.255.010 (West 2010).

19. The seventeen states that enacted statutes in 2006 are Arizona, ARIZ. REV. STAT. ANN. § 44-7501 (2010); Colorado, COLO. REV. STAT. ANN. § 6-1-716 (West 2010); Connecticut, CONN. GEN. STAT. ANN. § 36a-701b (West 2010); Idaho, IDAHO CODE ANN. § 28-51-105 (2010), amended by Act of Apr. 6, 2010, 2010 Idaho Sess. Laws 170 (amending existing law relating to disclosure of personal information to provide for application to city, county, and state agencies; to provide that certain entities and individuals shall notify the office of the Attorney General in the event of certain breaches of security; to clarify that certain reporting requirements shall continue to apply to state agencies; and to provide for violations and penalties); Illinois, 810 ILL. COMP. STAT. ANN. 530/10 (West 2010); Indiana, IND. CODE ANN. § 24-4.9-3-1 (West 2010); Louisiana, LA. REV. STAT. ANN. § 51:3074 (2010); Maine, ME. REV. STAT. ANN. tit. 10, § 1348 (2010); Minnesota, MINN. STAT. ANN. § 325E.61 (West 2010); Montana, MONT. CODE ANN. § 30-14-1704 (2010); Nebraska, NEB. REV. STAT. ANN. § 87-803 (LexisNexis 2010); Nevada, NEV. REV. STAT. ANN. § 603A.220 (West 2010); New Jersey, N.J. STAT. ANN. § 56:8-163 (West 2010); Ohio, OHIO REV. CODE ANN. § 1349.19 (West 2010); Pennsylvania, 73 PA. STAT. ANN. § 2303 (West 2010); Rhode Island, R.I. GEN. LAWS § 11-49.2-3, -4 (2010); and Wisconsin, WIS. STAT. ANN. § 134.98 (West 2010).

2008, and three in 2009, bringing the total number of states enacting data breach notification laws to forty-six.

After ChoicePoint, each data breach notification statute passed by a state was designed to provide specific protection to that state’s residents. California’s statute, for example, provides that “[t]he intent of the legislature to ensure that personal information about California residents is protected.” Similarly, the statute’s disclosure requirements are focused on California residents:

Any person or business that conducts business in California, and that owns or licenses computerized data that includes 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 other forty-five statutes also have focused on their own residents in enacting statutes that have varied requirements for investigating and disclosing data breaches, some with significant monetary penalties. Thus, under these statutes, it is the resident of the

21. The jurisdictions were: Iowa, IOWA CODE ANN. § 715C.2 (West 2010); Maryland, MD. CODE ANN., COM. LAW § 14-3504 (West 2010); Massachusetts, MASS. GEN. LAWS ANN. ch. 93H, § 3 (West 2010); Virginia, VA. CODE ANN. § 18.2-186.6 (West 2010); and West Virginia, W. VA. CODE ANN. § 46A-2A-102 (West 2010). Oklahoma also passed a substantial revision to its statute. OKLA. STAT. ANN. tit. 24, § 163-64 (West 2010).

22. The jurisdictions were: Alaska, ALASKA STAT. § 45.48.010 (2010), Missouri, MO. ANN. STAT. § 407.1500 (West 2010), and South Carolina, S.C. CODE ANN. § 39-1-90 (2010).

23. CAL. CIV. CODE § 1798.81.5.

24. CAL. CIV. CODE § 1798.82(a).

25. See ALASKA STAT. § 45.48.010 (2009); ARIZ. REV. STAT. ANN. § 44-7501(L)(4) (2009); ARK. CODE ANN. § 4-110-105(a)(1) (West 2009); COLO. REV. STAT. ANN. § 6-1-716 (d)(1) (West 2009); CONN. GEN. STAT. ANN. § 36a-701b(b) (West 2008); DEL. CODE ANN. tit. 6, § 12B-102(a) (2009); D.C. CODE § 28-3852(a) (2009); FLA. STAT. ANN. § 817.5681(1)(a) (West 2009); GA. CODE ANN. § 10-1-912 (West 2009); HAW. REV. STAT. § 487N-2(a) (2009); IDAHO CODE ANN. §§ 28-51-104(5) (2009), § 28-51-105; 815 ILL. COMP. STAT. ANN. 530/10 (2009); IND. CODE ANN. § 24-4.9-3-1 (West 2009); IOWA CODE ANN. § 715C.1-2 (West 2008); KAN. STAT. ANN. § 50-7a02(a) (2008); LA. REV. STAT. ANN. § 51:3074(a) (2009); MD. CODE ANN., COM. LAW § 14-3504 (West 2009); MASS. GEN. LAWS ANN. ch. 93H, § 3 (West 2009); MICH. COMP. LAWS ANN. § 445.72 (West 2009); MINN. STAT. ANN. § 325E.61 (West 2009); MO. REV. STAT. § 407.1500.2 (West 2009); MONT. CODE ANN. § 30-14-1704(1) (2009); NEB. REV. STAT. § 87-803 (2009); NEV. REV. STAT. ANN. § 603A.220 (West 2009); NEW HAMPSHIRE, N.H. REV. STAT. ANN. § 359-C:19(V) (2009); N.J. STAT. ANN. § 56:8-163(12)(a) (West 2009); N.Y. GEN. BUS. LAW § 899-aa.2 (McKinney 2009); N.C. GEN. STAT. ANN. §§75-65 (West 2009); N.D. CENT. CODE § 51-30-02 (2009); OHIO REV. CODE ANN. § 1349.19(A)(1)(a) (West 2009); OKLA. STAT. ANN. tit. 24, § 163-64 (West 2009); OR. REV. STAT. ANN. § 646.602; 73 PA. STAT. ANN. § 2302 (West 2009); R.I. GEN. LAWS § 11-49.2-3 (2009); S.C. CODE ANN. § 39-1-90 (2008); TENN. CODE ANN. § 47-18-
victim—and not the location of the company or the breach—that controls the notification requirements. As a result, a company facing a data breach in which the victims are spread across the country—a near certainty today, especially with the Internet providing virtual locations across the globe—could face multiple, inconsistent requirements and harsh penalties for failing to comply.

III. PERSONAL INFORMATION DEFINED

A. The California Model

Most states have modeled their data breach statutes after California's 2002 groundbreaking statute. California’s statute requires notification to individuals if, as the result of a breach in a company’s computer security, an individual’s “personal information” is compromised. California’s initial statute defined “personal information” as a person’s first name or first initial and his or her last name in combination with any one or more of the following pieces of data, when either the name or the data elements are not encrypted or redacted: social security number; driver’s license number or state identification card number; account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

In 2007, California added two additional elements to the definition of personal information: medical information and health insurance information. These amendments became effective January 1, 2008. In California, as in all except three states with data breach notification statutes, “personal information” is defined to exclude information that is publicly available.

2107(b) (West 2009); TEX. BUS. & COM. CODE ANN. § 48.103 (Vernon 2009); UTAH CODE ANN. § 13-44-202(1)(a) (West 2009); VT. STAT. ANN. tit. 9, § 2430(2) (2009); VA. Code Ann. § 18.2-186.6 (West 2009); WASH. REV. CODE ANN. § 19.255.010(1) (West 2009); W. VA. CODE ANN. § 46A-2A-101(6) (2009); WIS. STAT. ANN. § 134.98 (2009); WYO. STAT. ANN. 40-12-501(a) (2009).

26. CAL. CIV. CODE § 1798.82(a) (West 2009).


28. ALASKA STAT. § 45.48.590(5) (West 2010) ("[Records of personal information] do[ not include publicly available information containing names, addresses, telephone numbers, or other information an individual has voluntarily consented to have publicly disseminated or listed."); ARIZ. REV. STAT. ANN. § 44-1373.01(3) (2010). Alaska’s Confidentiality of Personal Identifying Information Statute does not apply to "[d]ocuments or records that are recorded or required to be open to the public pursuant to the constitution or laws of this state or by court rule or order, and this.
article does not limit access to these documents or records." *Id.* ARK. CODE ANN. § 4-110-103(8)(B) (West 2010) ("[Records of personal information] do[not include any publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number . . ."); COLO. REV. STAT. ANN. § 6-1-716(1)(d)(II) (West 2010) ("[P]ersonal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media."); CONN. GEN. STAT. ANN. § 36a-701b(a) (West 2010) ("[P]ersonal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); D.C. CODE § 28-3851(3)(B) (2010) ("[T]he term ‘personal information’ shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); HAW. REV. STAT. § 487N-1 (2010) ("‘Personal information’ does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); 815 ILL. COMP. STAT. ANN. 530/5 (West 2010) ("‘Personal information’ does not include publicly available information that is lawfully made available to the general public, State, or local government records."); IND. CODE ANN. § 24-4.9-2-10 (West 2010) ("[T]he term ‘personal information’ does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public."); IOWA CODE ANN. § 715C.1 (West 2010) ("‘Personal information’ does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public."); KAN. STAT. ANN. § 50-7a01(g)(3) (2010) ("The term ‘personal information’ does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); LA. REV. STAT. ANN. § 51:3073(4)(b) (2010) ("‘Personal information’ shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); ME. REV. STAT. ANN. tit. 10, § 1347(6) (2010) ("‘Personal information’ does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public."); MD. CODE ANN., COM. LAW § 14-3501(d)(2) (West 2010) ("‘Personal information’ does not include: (i) Publicly available information that is lawfully made available to the general public from federal, state, or local government records; (ii) Information that an individual has consented to have publicly disseminated or listed; or (iii) Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act."); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2010) ("‘Personal information’ shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."); MINN. STAT. ANN. § 325E.61(f) (West 2010) ("‘P]ersonal information’ does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); MO. ANN. STAT. § 407.1500(9) (West 2010) ("‘Personal information’ does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public . . ."); NEB. REV. STAT. § 87-802(5) (2010) ("Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); NEV. REV. STAT. ANN. § 603A.040 (West 2010) ("The term [personal information] does not include the last four digits of a social security number or publicly available information that is lawfully made available to the general public."); N.H. REV. STAT. ANN. § 359-C:19(IV)(b) (2010) ("‘Personal information’ shall not include information that is lawfully made available to the general public from federal, state, or local government records."); N.J. STAT. ANN. § 56:8-161 (West 2010) ("[R]ecords [of personal information do] not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed."); N.Y. GEN. BUS. LAW § 899-aa(b) (McKinney 2010) ("‘Private
information' does not include publicly available information which is lawfully made available to the
general public from federal, state, or local government records.

N.C. GEN. STAT. ANN. § 75-65 (West 2010) ("[P]ersonal information shall not include electronic identification numbers, electronic
mail names or addresses, Internet account numbers, Internet identification names, parent's legal
surname prior to marriage, or a password unless this information would permit access to a person's
financial account or resources."); OHIO REV. CODE ANN. § 1349.19(A)(7)(b) (West 2010):
"Personal information" does not include publicly available information that is
lawfully made available to the general public from federal, state, or local
government records or any of the following media that are widely distributed:
(i) Any news, editorial, or advertising statement published in any bona
fide newspaper, journal, or magazine, or broadcast over radio or television;
(ii) Any gathering or furnishing of information or news by any bona
fide reporter, correspondent, or news bureau to news media described in
division (A)(7)(b)(i) of this section;
(iii) Any publication designed for and distributed to members of any
bona fide association or charitable or fraternal nonprofit corporation;
(iv) Any type of media similar in nature to any item, entity, or
activity...

Id.; OKLA. STAT. ANN. tit. 24, § 162(6) (West 2010) ("The term [personal information] does not
include information that is lawfully obtained from publicly available information, or from federal,
state or local government records lawfully made available to the general public . . . ."); OR. REV.
STAT. ANN. § 646A.602(11)(c) (West 2010) ("[P]ersonal Information' [d]oes not include
information, other than a Social Security number, in a federal, state or local government record that is
lawfully made available to the public."); 73 PA. STAT. ANN. § 2302 (West 2010) ("The term
'Personal Information' does not include publicly available information that is lawfully made
available to the general public from Federal, State or local government records."); S.C. CODE ANN.
§ 16-13-510(D) (2010) ("The term [personal information] does not include information that is
lawfully obtained from publicly available information, or from federal, state, or local government
records lawfully made available to the general public."); TENN. CODE ANN. § 47-18-2107 (West
2010) ("[P]ersonal information' does not include publicly available information that is lawfully
made available to the general public from federal, state, or local government records."); UTAH CODE
ANN. § 13-44-102(3)(b) (West 2010) ("[P]ersonal information' does not include information
regardless of its source, contained in federal, state, or local government records or in widely
distributed media that are lawfully made available to the general public."); VT. STAT. ANN. tit. 9, §
2430(5)(B) (2010) ("[P]ersonal information' does not mean publicly available information that is
lawfully made available to the general public from federal, state, or local government records.");
VA. CODE ANN. § 18.2-186.6 (West 2010) ("The term [personal information] does not include
information that is lawfully obtained from publicly available information, or from federal, state, or
local government records lawfully made available to the general public."); WASH. REV. CODE ANN.
§ 19.255.010(6) (West 2010) ("[P]ersonal information' does not include publicly available
information that is lawfully made available to the general public from federal, state, or local
information] does not include information that is lawfully obtained from publicly available
information, or from federal, state or local government records lawfully made available to the
general public."); WIS. STAT. ANN. § 134.97(e)(1) (West 2010) ("[P]ersonal information' means ...
data . . . not generally considered to be public knowledge."); WIS. STAT. ANN. § 134.98(1)(c):
"Publicly available information" means any information that an entity reasonably
believes is one of the following: 1. Lawfully made widely available through any
media. 2. Lawfully made available to the general public from federal, state, or
local government records or disclosures to the general public that are required to
be made by federal, state, or local law.
B. Other State Variations

Some states include additional elements in the definition of "personal information" beyond the California model. For example, the Iowa, Nebraska, and Wisconsin data breach notification statutes include unique biometric data, such as fingerprint, retina, or iris images in the definition. North Carolina and North Dakota expand on the California model to include an employee's digital signatures.

New York takes a different approach. The statute simply—and sweepingly—defines personal information as "any information concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person," plus the individual's social security number, driver's license number (or non-driver identification card number), account number, credit or debit card number, PIN, or other necessary code.

It is also worth noting that the data breach statutes in Alaska, Hawaii, Indiana, North Carolina, Massachusetts, and Wisconsin include a breach of written as well as electronic data within the scope of their laws.

IV. DEFINING A DATA BREACH

The forty-six statutes define a "data breach" on a continuum from a strict liability standard to a risk-based approach. Some states define a
data breach simply as the “compromise” of a system, whereas other states incorporate the extent to which the data is likely to be misused and, in some cases, the likelihood that the misuse will lead to injury of the consumers into the definition of data breach. In some cases, the definitions incorporate a requirement that the companies investigate where the risk of harm is unknown.

Some statutes require that companies notify consumers based solely on “unauthorized access” to consumers’ personal information or “compromise” of personal information, whether or not the access to or compromise of that information results in fraud, crime, or any injury to the consumer. Because of the lack of demonstrated risk, injury, or possibility of injury, this can be referred to as a form of “strict liability” notification. At the other end of the scale is the risk assessment model, in which notice is required if the unauthorized acquisition creates a risk of harm to the consumer.

A. The Strict Liability Model

Under the strict liability model, companies are not required to perform a risk assessment and must provide notice whether or not there has been an actual injury to consumers. Typically, the language found in this type of data breach notification statute is a requirement that companies must notify consumers on the basis of unauthorized access to or the compromise of personal information. North Dakota defines a security breach in the broadest possible terms, as the “unauthorized access to” or “acquisition of” computerized data. Notification is required whether or not the unauthorized access or acquisition of computerized data results in the compromise of personal information. California’s data breach notification statute defines a breach of the security system as an “unauthorized acquisition” of data that “compromises the security, confidentiality, or integrity of personal information.” This type of statute requires notification in nearly all cases where unencrypted sensitive personal data is reasonably believed to have been acquired, whether or not there is any injury to the

42. See discussion infra Section III.A.
43. See discussion infra Section III.B.
45. CAL. CIV. CODE § 1798.82(d) (West 2009). A standard provision found in the California Code and in the other data breach notification statutes is an exemption for the good faith acquisition of personal information by an employee or agent of the person, which is considered not to be a breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use. See, e.g., id.

Four states—Arizona, Florida, Nevada, and Tennessee—incorporate an element of "materiality" into the definition of a "breach of the security system." Florida, for example, defines a data breach as an "unauthorized acquisition" of data that "materially compromises the security, confidentiality, or integrity of personal information." However, none of these states defines a "material breach" or otherwise provides clarity as to what constitutes a breach that "materially compromises" personal information. Moreover, the relative gravity or "materiality" of a breach is not a function of the number of records or individuals whose personal information is compromised, or whether any actual injury has occurred, but rather whether any compromised record contains personally identifiable information (PII). Thus, a breach of a system that contains "personal information" appears to be a prima facie occurrence of a "material" breach. For example, if an ex-boyfriend who hacks into a computer system and targets the personal information of only his former girlfriend, he has effected a "material breach" of that system. As a result, although these statutes might initially appear to constitute a more relaxed standard, they too create a form of strict liability for companies facing a data breach.

47. ARIZ. REV. STAT. ANN. § 44-7501 (2009).
48. CAL. CIV. CODE § 1798.82 (West 2009).
51. See GA. CODE ANN. § 10-1-911(1) (West 2009).
52. See 815 ILL. COMP. STAT. 530/5 (West 2009).
53. See MINN. STAT. ANN. § 325E.61(1)(d) (West 2009).
54. NEV. REV. STAT. ANN. § 603A.020 (West 2009).
55. See N.D. CENT. CODE § 51-30-02 (2009).
56. TENN. CODE. ANN. § 47-18-2107(b) (West 2009).
57. See TEX. BUS. & COM. CODE ANN. § 48.103 (Vernon 2009).
60. FLA. STAT. ANN. § 817.5681(4) (West 2009) (emphasis added).
Arizona also requires companies to undertake a reasonable investigation to determine whether there has been a security breach. However, the statute does not provide details on what steps satisfy the requirements for a "reasonable" investigation.

B. The Risk Assessment Model

In contrast to those states that require companies to notify consumers on the basis of unauthorized access or the compromise of personal information, twenty-four states require companies to provide notice only if the unauthorized acquisition creates a risk of harm to the consumer. The states that have adopted this risk assessment model have done so using different approaches.

Six of these states—Kansas, Maine, Nebraska, New Hampshire, Utah, and Wyoming—also require companies to determine whether there has been a misuse of individuals' information. As with Idaho and Arizona, these statutes do not provide details on what steps satisfy the requirements for a "reasonable" investigation. New Hampshire, for example, requires an entity to "immediately determine" whether or not misuse of individuals' personal information has occurred. These statutes do not indicate whether notice needs to be given if there is no indication that there has been financial injury. Nevertheless, companies should be ready to demonstrate their reasonableness by documenting the steps they take, the relevant expertise of the personnel performing the investigation, and adequately and thoroughly report the relevant findings to appropriate senior management and/or government agencies. In short, a company that investigates whether a data breach has or will lead to consumer injury needs to be ready to "show its work" and report what it did to make that assessment.

Another group of states provides that if a business undertakes an "appropriate" investigation or consults with relevant federal, state, and local law enforcement, and "reasonably" determines that the breach has not—and likely will not—result in harm to the individuals whose personal information has been acquired and accessed, then the business need not notify those individuals. These types of provisions are found in

the data breach statutes of Alaska,\textsuperscript{69} Arkansas,\textsuperscript{70} Florida,\textsuperscript{71} Iowa,\textsuperscript{72} and Rhode Island.\textsuperscript{73} These states require businesses to document their findings in writing and maintain the documentation for a stated number of years. In Florida, for example, companies face a fine of up to $50,000 for failure to create and maintain proper documentation should they choose not to provide notice following a breach.\textsuperscript{74} Although companies in these ten states are not required to conduct an investigation, the laws encourage them to do so. The statutes also provide incentives for companies to notify federal, state, and local law enforcement of the breach, and provide investigators and prosecutors with the opportunity to assess the nature and extent of the compromise, and focus their limited resources on the investigations that are the highest priority.

Sixteen states—Hawaii,\textsuperscript{75} Idaho, Iowa,\textsuperscript{76} Indiana,\textsuperscript{77} Kansas,\textsuperscript{78} Massachusetts,\textsuperscript{79} Montana,\textsuperscript{80} New York,\textsuperscript{81} North Carolina,\textsuperscript{82} Ohio,\textsuperscript{83} Oklahoma,\textsuperscript{84} Pennsylvania,\textsuperscript{85} South Carolina,\textsuperscript{86} Virginia,\textsuperscript{87} Wisconsin,\textsuperscript{88} and West Virginia\textsuperscript{89}—define a “security breach” in terms of whether it leads to a risk of injury to the consumer. Although these statutes do not explicitly require a company to conduct an investigation into a breach, such a determination probably requires such a review. Pennsylvania, for example, defines “breach of the security system” as the:

Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal

\textsuperscript{69} ALASKA STAT. § 45.48.010(c) (2009).
\textsuperscript{70} ARK. CODE ANN. § 4-110-105(d) (West 2009).
\textsuperscript{71} FLA. STAT. ANN. § 5681(10)(a) (West 2009).
\textsuperscript{72} IOWA CODE ANN. § 715C.1(6) (West 2009).
\textsuperscript{73} R.I. GEN. LAWS § 11-49.2-4 (2009).
\textsuperscript{74} FLA. STAT. ANN. § 817.5681(10)(a)-(b).
\textsuperscript{75} HAW. REV. STAT. § 487N-1 (2009).
\textsuperscript{76} IOWA CODE ANN. § 715C.1(6).
\textsuperscript{77} IND. CODE ANN. § 24-4-9-2-2 (West 2009).
\textsuperscript{78} KAN. STAT. ANN. §§ 50-7a01, -7a02 (2009).
\textsuperscript{79} MASS. GEN. LAWS ANN. ch. 93H, § 1(a) (West 2009).
\textsuperscript{80} MONT. CODE ANN. § 30-14-1704(4)(a) (2009).
\textsuperscript{81} N.Y. GEN. BUS. LAW § 899-aa(c) (McKinney 2009).
\textsuperscript{82} N.C. GEN. STAT. ANN. § 75-61(14) (West 2009).
\textsuperscript{83} OHIO REV. CODE ANN. § 1349.19(A) (West 2009).
\textsuperscript{84} OKLA. STAT. ANN. tit. 74, § 3113.1 (West 2009).
\textsuperscript{85} PA. STAT. ANN. § 2302 (West 2009).
\textsuperscript{87} VA. CODE ANN. § 18.2-186.6(A) (West 2009).
\textsuperscript{88} WIS. STAT. ANN. § 134.98 (West 2009).
information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.90

New York alone lists specific factors that an organization may consider in determining whether consumers' personal information has been acquired or is reasonably believed to have been acquired by an unauthorized individual, including indications (1) that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device; (2) that the information has been downloaded or copied; or (3) that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft.91

C. Blending Definitions: Risk Assessment and Strict Liability

Nine state data breach notification statutes incorporate both risk assessment and strict liability clauses. These statutes generally start with the premise that a company must disclose a breach. They then typically incorporate a claw-back provision stating that notification will not be required if the company undertakes an “appropriate investigation,” consults with federal, state, and local law enforcement agencies, and determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Connecticut’s statute is typical:

Any person . . . shall disclose any breach of security following the discovery of the breach to any resident of this state whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.92

There are similar provisions in the data breach notification statutes of Colorado,93 Maryland,94 Michigan,95 Missouri,96 New Jersey,97 Oregon,98 and Vermont.99

90. 73 PA. STAT. ANN. § 2302.
91. N.Y. GEN. BUS. LAW, § 899-aa(c) (McKinney 2009).
92. CONN. GEN. STAT. ANN. § 36a-701b(b) (West 2009).
93. COLO. REV. STAT. ANN. § 6-1-716 (West 2009).
94. MD. CODE ANN. § 12-701b(b) (West 2009).
95. MICH. STAT. ANN. § 691.777 (West 2009).
96. MISS. CODE ANN. § 49-21-4 (West 2009).
97. N.J. STAT. ANN. § 56:8-17 (West 2009).
98. ORE. REV. STAT. ANN. § 45.028 (West 2009).
In a few states, a blend of definitions has created internal contradictions. North Carolina defines a security breach both as “unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer.” The statute then adds: “[a]ny incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.” These two standards are in conflict. The first clause includes a risk-based analysis into whether there has been actual illegal use of data or some other “material risk of harm.” The second clause imposes strict liability for a mere “incident of unauthorized access” to personal information, regardless of whether there is a risk of injury to consumers.100

Similarly, Massachusetts’ data breach statute incorporates two different standards, the first of which is risk-based and the second of which creates a strict liability standard. First, the statute requires an organization to notify the Commonwealth’s residents if it knows or has reason to know of a breach of security. A breach is defined as “the unauthorized acquisition or unauthorized use of unencrypted data, or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth.”101 In addition, however, a company must also provide notice if it knows or has reason to know that the personal information of such a resident was acquired or used by an unauthorized person or used for an unauthorized purpose.102

D. Conducting the Investigation

California’s landmark statute, enacted in the wake of data breaches in 2002, requires companies to notify consumers “in the most expedient time possible and without unnecessary delay, consistent with the needs of the investigation.”

94. MD. CODE ANN., COM. LAW § 14-3504(b) (West 2009).
95. MICH. COMP. LAWS. ANN. § 445.72(12)(1) (West 2009).
96. MO. ANN. STAT. § 407.1500 (West 2009).
98. OR. REV. STAT. ANN. § 646A.602 (West 2007).
100. N.C. GEN. STAT. ANN. § 75-61(14) (West 2009).
101. MASS. GEN. LAWS ch. 93H, § 3(a) (West 2009).
102. Id.
of law enforcement . . . or any measures to determine the scope of the breach and restore the reasonable integrity of the data system.\footnote{CAL. CIV. CODE. § 1798.82(a) (West 2009).} The states that followed California in enacting data breach notification statutes encouraged or required companies, in various ways, to investigate data breaches. As discussed above, some states encouraged companies to conduct an "appropriate investigation" and consult with law enforcement, and incorporated a provision that notification would not be required if the investigation resulted in a determination that consumers had not been injured.\footnote{See supra III.C.} Other state statutes included requirements that companies undertake their own investigations and report their findings to law enforcement or a regulatory authority.\footnote{See supra III.B.}

The focus of the investigation varies depending on whether there is a strict liability to report or a need to report based on a finding of substantial risk. In strict liability states, like North Dakota, the investigation focuses on whether a consumer's personal information has simply been acquired and accessed.\footnote{N.D. CENT. CODE § 51-30-02 (2009).} In states that focus on substantial risk of injury, like Massachusetts,\footnote{M A S S. G E N. L A W S ch. 93H, § 1(a) (West 2009).} the focus of the investigation is on whether the consumers had been injured by fraud or identity theft.

No statute actually defines the scope of an "adequate investigation," details what steps a company must take, or prescribes how a company should document the results of its investigation. However, there are a number of questions a company should be able to answer in order to determine what data was exposed and who was involved in the data breach:

- Where was the compromised stolen information stored?
- How, when, and by whom was this information accessed?
- What did the perpetrators do with the data? Did they extract it? If so, how and what did they do with it?
- With whom did the perpetrators communicate about the stolen data, both within and outside the organization?\footnote{See Eoghan Casey, Data Theft: An Ounce of Forensic Preparedness Is Worth a Pound of Incident Response, INFO. SYS. ASS'N J., Aug. 2007, at 6, available at https://www.issa.org/page/?p=183.}

A digital forensic examiner can take the necessary steps to preserve the evidence in a forensically sound manner to ensure that nothing crucial to the investigation is altered or obliterated. Something as simple as changing the "last accessed" dates on the compromised computer...
system may make it impossible to ascertain whether an intruder gained unauthorized access to the data at issue.

Even if evidence of illegal activity is found, failures to handle digital evidence in a forensically sound manner can prevent an organization from taking legal action against the culprit or making a successful criminal referral to law enforcement.

On a practical level, there could be a real or perceived threat to the jobs of the local IT staff, which creates a potential conflict of interest and an incentive not to disclose all of the circumstances surrounding the breach. Often an internal IT group may be hesitant to admit that a breach was caused by an internal security weakness because they fear that any blame for the vulnerability leading to the breach will be placed at their feet. In fact, IT personnel may even be concerned that they could be viewed as complicit suspects in the data compromise. For example, if a company discovers that customer sales data may have been copied illicitly from a shared file server, members of the IT department might be reluctant to conduct a thorough investigation if they fear being held responsible for failing to secure the file server, or if they fear that they will be viewed as suspects because they are among the few individuals who have administrative rights to the file server.

In short, independent digital forensic examiners can be an important part of the successful investigation of a data breach. When confronting the issue of how to conduct an "adequate investigation" and prepare documentation that supports any resulting findings, a company would be wise to consider the services of digital forensic examiners, just as they would consider the services of outside counsel well-versed in privacy and data breach law.

E. Safe Harbor under Federal Banking Statutes and Other Laws

Most of the state data breach statutes provide exemptions for firms already governed by the Gramm-Leach-Bliley Act (GLBA) of 1999 or, alternatively, for procedures that are enacted pursuant to other state or federal rules or regulations. These exemptions arise from the fact that

109. See ARiz. REV. STAT. ANN. § 44-7501(J)(1), § 45.48.040(c) (2009); ARK. CODE ANN. § 4-110-106(a), § 4-110-106(5) (West 2009); COL. REV. STAT. ANN. § 6-1-716(2) (West 2009); CONN. GEN. STAT. ANN. § 36a-701b(f) (West 2009); DEL. CODE ANN. tit. 6, § 12B-103(b) (2009); D.C. CODE § 28-3852(g) (2009); FLA. STAT. ANN. § 817.5681(9)(b) (West 2009); HAW. REV. STAT. § 487N-2(a) (2009); IDAHO CODE ANN. § 28-51-106(2) (2009); IND. CODE ANN. § 24-4.9-3-3.5 (West 2009); IOWA CODE ANN. § 715C.2(7)(C) (West 2009); KAN. STAT. ANN. § 50-7a02(e) (2009); ME. REV. STAT. ANN. tit. 10, § 1349(F) (2009); MD. CODE ANN., COM. LAW §14-3507(c) (West 2009); MASS. GEN. LAWS ANN. ch. 93H, § 5 (West 2009); MICH. COMP. LAWS ANN. §445.72(8)(b) (West
these other statutes have their own reporting requirements and privacy protections. For example, Congress enacted the GLBA to ensure that financial service providers would protect consumers’ personal financial information. Under the GLBA, financial institutions must develop and implement data security policies that “prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information.” Under the guidance issued pursuant to the GLBA, a financial institution that becomes aware of unauthorized access to personal information should conduct a reasonable investigation promptly to determine the likelihood that the information has been or will be misused. If the company determines that misuse of the information has occurred or is reasonably possible, it is supposed to notify affected consumers as soon as possible.110

F. Recommendation: States Should Adopt the Risk Assessment Model Which Presents Greater Benefits for the Consumer over the Strict Liability Approach

A strict liability regime sets a hair trigger for data breach notification. Companies send out letters to consumers even when there is no evidence of injury, risk of injury, or possibility of injury, but merely when there is evidence that “access to” consumers’ PII occurred. As a result, consumers receive so many data breach notification letters that they become numb to the effect.111 The form letters sent to consumers generally provide them with no information about actual


injury or risk, nor do they provide consumers with the ability to judge whether there is any likelihood of injury or risk.

Adopting a risk assessment model is a more efficient approach. States and the federal government should exempt companies from the obligation to notify individuals of a data breach if the companies (1) undertake an appropriate investigation and “reasonably” determine that the breach has not—and likely will not—result in harm to the individuals whose PII has been acquired and accessed, document those results, and maintain them for at least five years; and (2) consult with relevant federal, state, or local law enforcement regarding their determination that the breach has not—and likely will not—result in harm to the individuals whose PII has been acquired and accessed. Requiring companies to undertake a thorough investigation will protect consumers. Directing them to liaise with law enforcement regarding a breach would provide investigators with the information they need and allow for increased coordination of efforts. The proposal would require federal, state, and local law enforcement to share information they receive from companies that had suffered data breaches; the risk is that government agencies would find themselves so inundated with information they would be unable to separate the wheat from the chaff.

V. WHEN TIME LIMITS ARE NOT REALLY TIME LIMITS

Several states have enacted what appear to be stringent time limits on notification of data breaches to consumers. In reality, these purported time limits have several elements that toll or, in some cases nullify, the requirements written into these statutes. For example, Florida’s data breach notification statute states that, absent an investigation or the involvement of law enforcement and the reasonable determination of no harm, Florida organizations suffering a material breach must notify the affected individuals in writing, by email, or through substituted notice:

without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or subject to any measures necessary to determine the presence, nature and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.

---

The statute appears to require quick action based on two complementary guidelines regarding when notice must be issued. Specifically, the notice must be made "without unreasonable delay" but, in any event, not later than forty-five days after there is a "determination of a breach." In fact, the forty-five day countdown to provide notice is subject to either tolling or nullification under several circumstances. First, the forty-five day countdown is tolled when the victimized company begins taking "measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system." These measures may take a substantial period of time and no outside time limit is specified in the statute. Second, the forty-five day countdown for notice is nullified and no notification is required under Florida law if, after a reasonable investigation, the company determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed.

Only the data breach statutes in Ohio and Wisconsin replicate the forty-five day limits found in Florida's data breach statute. Ohio's statute makes the rigorous time constraints "subject to the legitimate needs of law enforcement, and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system." However, the conjunctive between these two clauses means that companies in Ohio need to coordinate with law enforcement from the onset of the investigation of a data breach to ensure that the forty-five day notification requirement is tolled. Wisconsin's statute, in contrast, posits that the only law enforcement exceptions to the forty-five day rule must be related to the protection of an investigation or to homeland security.

Another group of thirty states require a company to provide notice in the "most expedient time possible," "without unreasonable delay," or "as soon as possible." In the seven states that require companies to

---

114. Id.
115. Id.
116. See FLA. STAT. ANN. § 817.5681(10)(a).
118. WIS. STAT. ANN. § 134.98 (West 2009).
119. OHIO REV. CODE ANN. § 1349.19(B)(2).
120. WIS. STAT. ANN. § 134.98.
121. The thirty states that require a company to provide notice in the "most expedient time possible" and "without unreasonable delay" or "as soon as possible" are Alaska, ALASKA STAT. § 45.48.010 (2009); Arkansas, Ark. CODE ANN. § 4-110-105(d) (West 2009); California, CAL. CIV.
undertake investigations, companies generally must first conduct a "reasonable and prompt" investigation to determine the likelihood that personal information has been or will be misused; if so, they must then provide notice in the most expedient time possible.\textsuperscript{122}

A. Penalties

Consumers in California,\textsuperscript{123} Hawaii,\textsuperscript{124} New Hampshire,\textsuperscript{125} North Carolina,\textsuperscript{126} Washington,\textsuperscript{127} and the District of Columbia\textsuperscript{126} have an explicit private right of action under their state data breach statutes. Companies that do not comply with the statute face civil penalties ranging from $500 a violation in Maine\textsuperscript{129} to a maximum of $750,000 in Michigan,\textsuperscript{130} and a range of penalties in between.\textsuperscript{131} In twenty-six states, 

\textsuperscript{122} The seven states in which states first must conduct a "reasonable and prompt" investigation are Arizona, ARIZ. REV. STAT. ANN. § 44-7501 (2009); Idaho, IDAHO CODE ANN. § 28-51-105 (2009); Kansas, KAN. STAT. ANN. §§ 50-7a02 (2009); Maine, ME. REV. STAT. ANN. tit. 10, § 1348 (2009); Nebraska, NEB. REV. STAT. ANN. § 87-803(1) (West 2009); New Hampshire, N.H. REV. STAT. ANN. § 359-C:20(I)(a) (2009); and Wyoming, WYO. STAT. ANN. § 40-12-501(a) (2009).

\textsuperscript{123} See CAL. CIV. CODE § 1798.84 (West 2009).

\textsuperscript{124} Id.

\textsuperscript{125} N.H. REV. STAT. ANN. § 359-C:21 (2009).

\textsuperscript{126} N.C. GEN. STAT. ANN. § 75-65-(i) (West 2009).

\textsuperscript{127} WASH. REV. CODE ANN. § 19.255(10)(a) (West 2009).

\textsuperscript{128} D.C. CODE § 28-3853(a) (2009).

\textsuperscript{129} ME. REV. STAT. ANN. tit. 10, § 1349 (2009).

\textsuperscript{130} MICH. COMP. LAWS ANN. § 445.72(13)-(14) (West 2009).

\textsuperscript{131} In Arizona, companies face civil penalties up to $10,000, see ARIZ. REV. STAT. § 44-7501(H) (2009); in Hawaii, civil penalties up to $2500 for each violation, see HAW. REV. STAT. § 487N-3 (2009); Idaho, fines of up to $25,000 per breach, see IDAHO CODE ANN. § 28-51-107.
the attorney general may institute suit for actual damages or injunctive relief against organizations or individuals that violate the data breach statute.\textsuperscript{132}

B. Enforcement and Litigation under the Data Breach Statutes

In the first five years after the first data breach statute was passed in California in 2002, there were relatively few state or federal complaints filed under the data breach notification statutes, especially in light of the number of data breaches reported. The early suits arising out of the data breaches were focused on contract or tort rather than violation of the data breach notification statutes themselves. For example, the Office of the Massachusetts Attorney General led a multi-state investigation into the security breach reported by the TJX Companies (TJX), the parent company of TJ Maxx, Marshalls, HomeGoods, and A.J. Wright stores. The FTC filed suit as well, alleging that TJX failed to prevent unauthorized access to personal information on its computer networks and that these failures allowed a hacker to exploit vulnerabilities and obtain tens of millions of credit and debit payment cards used at the retailer’s stores, as well as personal information relating to approximately 455,000 consumers who returned merchandise without receipts.\textsuperscript{133} The TJX breach affected information regarding credit and debit card sales transactions in TJX’s stores in the United States.


Canada, and Puerto Rico during 2003, as well as such information for these stores from mid-May through December 2006.\(^{134}\) TJX also faced numerous individual and class action suits filed by consumers across the country.\(^{135}\) Both the private litigation and the public enforcement actions were focused on claims arising under TJX's failure to protect consumers' personally identifiable information; there were no claims that the company had failed to notify the victims upon the discovery of the breach.

In June 2009, TJX settled with the multi-state group of attorneys general and agreed to pay $9.75 million to the states, $5.5 million of which is to be dedicated to data protection and consumer protection efforts by the states and $1.75 million is for reimbursement of the states' costs and fees. The remaining $2.5 million of the settlement will fund a Data Security Trust that will be used by the state attorneys general for policy efforts in the field of data security and protecting consumers' personal information.\(^{136}\) The company's settlement with the FTC requires that it establish and maintain a comprehensive security program reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers.\(^{137}\) To settle


the class action suits, TJX offered vouchers, cash, credit monitoring, identity theft insurance, and reimbursement to eligible class members.\textsuperscript{138}

However, starting in 2008 a number of recent large breaches have spawned suits under data breach statutes in federal courts around the country as well as an increasing number of actions by state attorneys general. The data breach at Countrywide Financial, the holding company for Countrywide Home Loans, has thus far given rise to six class actions filed in federal district courts across the country. One of the six was filed in the Southern District of Florida and alleges a violation of the Florida data breach notification statute.\textsuperscript{139} The United States Judicial Panel on Multidistrict Litigation consolidated the six cases and transferred them to the Western District of Kentucky for pretrial proceedings.\textsuperscript{140} In addition, the Connecticut Attorney General announced in September 2008 that as part of its ongoing investigation it was seeking more details about the threat to Connecticut consumers, confirmation that the company would provide free credit monitoring and freezes, and a guarantee that consumers would be compensated for losses associated with the breach.\textsuperscript{141}

In 2007, the New York Attorney General’s Office announced a settlement with CS Stars LLC, a Chicago-based claims management company for failing to notify 540,000 New York consumers for seven weeks after a breach in 2006 in contravention of the statute’s requirement that notice be made “immediately following discovery.” The company agreed to comply with the law, ensure that proper notifications be made in the event of the future, implement more extensive practices relating to the security of private information, and pay the Attorney General’s office $60,000 for costs related to the investigation.\textsuperscript{142}


In the wake of the Heartland Payment Systems breach of 2009, plaintiffs seeking class action status have filed suit alleging contract violations as well as failure to promptly notify consumers of the data breach in violation of New Jersey law.\textsuperscript{143} The plaintiffs in the Express Scripts class action cited eleven data breach notification statutes, noting that Missouri, the home of the St. Louis-based pharmacy benefit management company that suffered the breach, did not then have such a requirement.\textsuperscript{144}

RBS WorldPay also has to contend with a federal district court action filed in the Northern District of Georgia seeking class action status and alleging a violation of Georgia's data breach notification statute.\textsuperscript{145} In addition, Wackenhut Corporation, the security company, is contending with a suit filed in 2008 in Tennessee Circuit Court alleging that it failed to notify consumers of a data breach as required by state law.\textsuperscript{146}

The Indiana Attorney General's Office recently resolved suits brought with the U.S. Department of Health and Human Services' Office of Civil Rights against two pharmacy chains, CVS and Walgreens, which involved data breach complaints alleging that customers' medical information was improperly discarded in trash bins outside of the stores.\textsuperscript{147} The actions, however, were brought under HIPAA, not the Indiana data breach notification statute.

The rise of complaints alleging violations of data breach notification statutes—both by state attorneys general and by private litigants in federal court—should be a wake up call for lawyers and their clients. As the incidence of reported data breaches increases, along with the number of complaints that companies have failed to comply with the requirements under the statute, liability—in terms of penalties and judgments—will rise as well. Statutes in twenty-four states incorporate provisions that allow companies to take "any measures necessary to determine the presence, nature, and scope of the breach and restore the

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{143} Sansom v. Heartland Payment Sys., Inc., 2009 WL 217497 (D.N.J. filed Jan. 23, 2009).
  \item \textsuperscript{144} Amburger, v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1049 (E.D. Mo. 2009) (granting defendant's motion to dismiss because plaintiff lacked standing to bring a claim, and plaintiff failed to state a claim upon which relief could be granted).
  \item \textsuperscript{145} Irwin v. RBS WorldPay, Inc., 2009 WL 412516, 412516 (N.D. Ga. filed Feb 05, 2009).
  \item \textsuperscript{146} Throckmorton v. Metro. Gov't of Nashville, 2008 WL 227312 (Tenn. Cir. Ct. filed Jan 04, 2008).
\end{itemize}
\end{footnotesize}
reasonable integrity of the system”, any time limits are tolled while the company is undertaking such an investigation. Seven states also require companies to undertake a “reasonable” investigation to undertake the scope of the breach. Accordingly, when companies face a data breach—and the prospect of litigation—it would be in their best interest to consider the stakes at risk and how they will approach such an investigation.

VI. RECOMMENDATIONS: TOWARD A FEDERAL DATA BREACH NOTIFICATION STANDARD

A. Overview: Breach Notification under the HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, includes provisions designed to advance the use of health information technology while strengthening privacy and security protections for that information. The HITECH Act required the Department of Health and Human Services (“HHS” or “Department”) to issue interim final regulations for breach notification by entities subject to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and their business associates. The statute also directed the Federal Trade Commission (“FTC” or “Commission”) to adopt within 180 days of enactment of the statute a rule implementing the breach notification requirements for vendors and third-party service providers of personal health records (PHRs), such as online repositories of health information that individuals can create to track their medical visits and prescription information.

148. See supra Section III.B.
149. See supra Section III.B.
151. § 13407(g)(1), id. at 270-71 (codified at 42 U.S.C.A. § 17937(g)(1)). The statute addresses only breach notification with respect to PHRs voluntarily created by individuals; it does not address electronic health records more generally, such as those created for patients by hospitals or doctors.
152. The statute defines PHRs as electronic records “on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.” § 13400(11), id. at 259 (codified at 42 U.S.C.A. § 17921(11)).
On August 24, 2009, HHS issued an Interim Final Rule with Request for Comments\(^{153}\) entitled “Breach Notification for Unsecured Protected Health Information” to require notification of breaches of unsecured PHI.\(^{154}\) The next day the FTC issued its Final Breach Notification Rule, which required PHRs and related entities to notify consumers when the security of their individually identifiable health information has been breached.\(^{155}\) In general, the HHS regulations apply to HIPAA-covered entities—health plans, health care providers, and their business associates—and the FTC regulations apply to vendors of PHRs and their third-party service providers.\(^{156}\)

B. Protected Health Information and Personal Health Records

The HITECH Act requires covered entities and business associates to provide notification following the breach of unsecured protected health information (PHI). PHI, in turn, is defined by HIPAA’s Privacy Rule as “individually identifiable health information held or transmitted in any form or medium by these HIPAA-covered entities and business associates, whether electronic, paper or oral.”\(^{157}\) The Privacy Rule defines “individually identifiable health information” as information, including demographic data that relates to:

- The individual’s past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,

\(^{153}\) Congress required HHS to issue regulations as “interim final regulations” within 180 days after the enactment of the Recovery Act on February 23, 2009. § 13402(j), id. at 263 (codified at 42 U.S.C.A. § 179320)). Based on the statutory directive and the time frame, the Department decided to waive the notice-and-comment requirements of the Administrative Procedure Act and to proceed with the interim final rule along with Request for Comments. HHS Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740-41 (Aug. 24, 2009) (to be codified at 45 C.F.R. pt. 160, 164).

\(^{154}\) Id. at 42740.


\(^{156}\) The FTC adopted a provision specifying that its rule “does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity.” Id. at § 318.1(a).

\(^{157}\) HHS Definitions, 45 C.F.R. § 160.103 (2010). The general principle underlying the Privacy Rule is that a covered entity may not use or disclose PHI except either (1) as the Privacy Rule permits or requires or (2) as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing. Id.
And that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.\textsuperscript{158}

Individually identifiable health information also includes many common identifiers, e.g., name, address, birth date, and social security number.\textsuperscript{159}

As required by the HITECH Act, HHS promulgated the Interim Final Rule, which requires organizations to provide notice following a breach of unsecured PHI.\textsuperscript{160} Under the regulation, disclosure of individually identifiable health information that is not PHI would not qualify as a "breach" for purposes of this rule, although the Department noted that a company should consider whether it has notification requirements under other laws.\textsuperscript{161} In the Interim Final Rule, the Department clarified that the term "unauthorized" meant an impermissible use or disclosure of protected health information under the HIPAA Privacy Rule.\textsuperscript{162}

C. Definition of "Breach"

Section 13400(1)(A) of the HITECH Act defines "breach" as unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the protected health information except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.\textsuperscript{163}

The Act also provides exceptions to the definition of "breach" for certain circumstances involving inadvertent acquisition, access, or use of PHI by employees and agents of covered entities or business associates where the information is not further acquired, accessed, used, or disclosed.\textsuperscript{164}

\textsuperscript{158} Id.
\textsuperscript{159} Id.
\textsuperscript{161} Id.
\textsuperscript{162} Id.
\textsuperscript{164} § 13402(a) & (b), id. at 260 (codified at 42 U.S.C.A. § 17932(a) & (b)); § 13400(1)(B), id. at 258 (codified at 42 U.S.C.A. § 17921(1)(B)).
The HHS Regulations noted that the agency had “consulted closely with the FTC in the development of these regulations” and were cognizant of worries that organizations that could fall under “different and inconsistent regulatory schemes.” The two agencies charged with promulgating regulations under this Act, however, have come up with separate—and conflicting—definitions of “breach.” HHS relies on a risk assessment standard while the FTC uses a blended approach that incorporates both elements of strict liability and risk assessment. HHS defines a “breach” as the “acquisition, access, use or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.” For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. For example, the Interim Final Rule notes that uses or disclosures that impermissibly involve more than the minimum necessary information in violation of the HIPAA Privacy Rule may qualify as breaches.

As noted above, the HITECH Act defines a security breach in terms of an “acquisition which... compromises the security or privacy of the protected health information.” In the Interim Final Rule, the Department agreed with comments that noted that this language “contemplates that covered entities will perform some type of risk assessment to determine if there is a risk of harm to the individual, and therefore, if a breach has occurred.” Thus, the Department decided that the statute “encompassed a harm threshold” and “clarified” that a breach that “compromises the security or privacy of the protected health information” means that it “poses a significant risk of financial, reputational, or other harm to the individual.” The Interim Final Rule—as opposed to the statute—therefore contains an explicit requirement that organizations facing a data breach conduct an investigation to determine where there is a significant risk of harm to the individual(s) as a result of the impermissible use or disclosure:

166. Id.
167. HHS Uses and Disclosures of Protected Health Information: General Rules, 45 C.F.R. § 164.502(b) (2010); HHS Other Requirements Relating to Uses and Disclosures of Protected Health Information, 45 C.F.R. § 164.514(d) (2010).
171. Id.
Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.\footnote{172}

The FTC, on the other hand, took a different approach. Where HHS has read a requirement of a “risk assessment” into the definition of breach, the FTC has adopted a rebuttable presumption that acquisition of information includes access to identifiable information. The Commission defined “breach of security” to mean, with respect to unsecured PHR identifiable health information as:

acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence that there has not been, or could not reasonably have been, unauthorized acquisition of such information.\footnote{173}

The first part of the FTC’s definition defines a security breach in the broadest sense—as an acquisition of PHI “without authorization.” The second clause, however, includes a claw-back in which the organization will not have to notify individuals if it provides “reliable” evidence that the unauthorized acquisition has not included unauthorized access to identifiable information. Although the regulation does not explicitly require organizations to undertake an investigation, the definitions adopted by both the FTC and HHS encourage them to do so.\footnote{174}

D. Encryption

The HITECH Act requires organizations to provide notice only if a breach involves PHI that is “unsecured.”\footnote{175} Under the HHS regulation, “unsecured protected health information” means protected health information that is not rendered unusable, unreadable, or indecipherable

\footnotesize{\begin{itemize}
  \item \footnote{172}{HHS Definitions, 45 C.F.R. § 164.402 (2010).}
  \item \footnote{173}{FTC Health Breach Notification Rule, 16 C.F.R. § 318.2(a) (2010) (emphasis added).}
  \item \footnote{174}{See Section III.B and cites therein.}
\end{itemize}}
to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS Web site. The definition of “unsecured” in the FTC’s Rule similarly relies on the protection of information through technologies identified by the Secretary of HHS. This approach allows the Department to update its guidance to companies quickly as encryption technologies improve.

E. Time Line for Notification

Under both the HHS Interim Final Rule and the FTC’s Final Rule, a company must send the required notification “without unreasonable delay” and in no case later than sixty calendar days after the date the breach was discovered. The only exception to this time frame is when law enforcement requests a delay. A breach is treated as “discovered” on the first day the breach is known to the company or third party vendor or would have been known to the company had it exercised reasonable diligence. Thus, “the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in this rule.

F. Notification of Breach

In addition to the requirement that a covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed to have been breached, if a breach involves more than 500 residents of a state or jurisdiction, the organization must notify “prominent media outlets serving the state or jurisdiction” without unreasonable delay and in no case later than sixty calendar days after discovery of a breach.

Regardless of the location of the victims, if the breach affects fewer than

177. 16 C.F.R. § 318.2(c)(2)(i).
178. 45 C.F.R. § 164.404(b); 16 C.F.R. § 318.4(a).
179. See 45 C.F.R. § 164.412; 16 CFR § 318.4(c).
180. 45 C.F.R. § 164.404(a)(2); 16 C.F.R. § 318.3(c). In addition, the HHS regulation specifies that the knowledge of a breach by a workforce member or other agent—other than the person committing the breach—is imputed to the covered entity itself. 45 C.F.R. § 164.404(a)(2).
181. 45 C.F.R. § 164.404(a)(2).
183. HHS Notification to Media, 45 CFR § 164.406 (2010); FTC Methods of Notice, 16 C.F.R. § 318.5(b) (2010).
500 individuals, then the covered entity must provide notice to either the FTC or HHS, as applicable.\textsuperscript{184} If the breach affects fewer than 500 individuals, the organization must maintain a log or other similar documentation and provide that information to the Department or the Commission no later than sixty days after the end of the calendar year.\textsuperscript{185}

Congress' enactment of a federal data breach notification requirement for PHI is an important first step toward a rationalization of data security standards. However, HHS and the FTC have taken the same statutory language and promulgated separate and conflicting definitions of a security breach, with the former based on a risk assessment while the latter incorporates elements of both strict liability and risk assessment. Maintaining both definitions could set up the very "different and inconsistent regulatory schemes" the agencies vowed they would avoid through consultation and coordination.\textsuperscript{186}

Congress should now take the next step and enact a statute that applies to consumers' PII, as defined by California's statute, and incorporates a risk assessment approach to data breach notifications, rather than strict liability. The hair trigger set in the strict liability models has caused so many disclosure letters to be sent to so many consumers—with consumers often receiving letters from multiple companies regarding the same breach—that people have become numb to the effect.\textsuperscript{187} The form letters generally do not provide consumers with information about any genuine injury or risk, nor do they provide the consumers with the ability to judge whether there is any likelihood of injury or risk.

Congress should enact a statute that provides that notification is not required if, after an appropriate investigation within a reasonable timeframe—not to exceed sixty calendar days—and after consultation with relevant federal, state, or local agencies responsible for law enforcement, the company determines that there is no reasonable likelihood of financial harm to the consumers whose personal information has been acquired as a result of the breach. The company should be required to document the results of its investigation and retain those records for at least five years, with a fine of $50,000 for failure to maintain those records.

---

\textsuperscript{184} HHS Notification to Secretary, 45 C.F.R. § 164.408(a) (2010); 16 CFR § 318.5(c).

\textsuperscript{185} 45 C.F.R. § 164.408(c); 16 C.F.R. § 318.5(c).


\textsuperscript{187} See Schwartz & Janger, supra note 111 (arguing for determination of data security breaches and post-notification remediation by an independent third party).
G. Waiting for Godot.\textsuperscript{188} Steps for State Legislatures, Enforcement Agencies, and Companies

An overarching federal data breach notification standard may not happen soon. In the meantime, there are a number of steps that state and local legislatures and enforcement agencies can take. First, the five states that do not have data breach notification statutes—Alabama, Kentucky, Mississippi, New Mexico, and South Dakota—should enact them immediately. As laid out above, the most efficient, consumer-oriented approach is a statute that encompasses a risk-assessment definition of "data breach."

Second, law enforcement agencies and prosecutors should determine if the statutes in their jurisdictions have "reasonable investigation" and cooperation provisions that toll notification to consumers. If so, these agencies should ensure that companies are aware of these provisions and work toward taking full advantage of the ability to find out about breaches as early as possible.

Third, data breach statutes throughout the country present a web of conflicting obligations for companies and their lawyers that may potentially expose organizations to millions of dollars in fines and civil liability if obligations under the laws are ignored or misunderstood. A unified data breach notification statute—either a model state law or a federal statute—will minimize the burden on the private sector. Companies with a multi-state or Internet presence currently must adhere to the most restrictive law or wrestle with conflict between the jurisdictions where it does business. Many, if not most, of the state statutes allow companies to forego notifying individuals whose personal information may have been compromised if the company "reasonably" determines that the breach did not and likely will not result in harm to those individuals. Although the statutes do not provide detail on what steps satisfy the requirements for a "reasonable" investigation, most do require the companies to document what steps they have taken and to maintain the records for a set period of time. Companies that undertake a "reasonable investigation" face extraordinarily high stakes in terms of potential fines and risk to reputation and should consider whether to rely on untrained personnel or individuals with potential conflicts of interest to investigate the origin, nature, and extent of the breach, and to provide a determination as to whether the breach resulted in harm to individuals whose personal information has been compromised.

Enactment of a federal data breach notification statute can provide enforcement authority to state attorneys general and a federal law enforcement authority, such as the U.S. Department of Justice or the Federal Trade Commission. This model has worked well with the Telemarketing Sales Rule\textsuperscript{189} and the rule regulating the “pay-per-call” industry.\textsuperscript{190} Both rules provide authority to the federal government and the states, which typically have the most experience combating such problems. Ultimately, the private sector and consumers will benefit from a unified data breach notification law as well as multiple enforcers of that statute.

\textsuperscript{189} FTC Actions by States and Private Persons, 16 C.F.R. § 310.7 (2010).
\textsuperscript{190} FTC Billing and Collection for Pay-Per-Call Services, 16 C.F.R. § 308.7 (2010).