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

Dana J. Lesemann
Howard Law School, dlesemann@law.howard.edu

Once More Unto the Breach:[1] An Analysis of Legal, Technological, and Policy Issues Involving Data Breach Notification Statutes

Dana J. Lesemann[2]

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, to name a few generalized steps. 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 rise in the incidences of these breaches is well documented. Reports of data breaches increased dramatically in 2008. The Identity Theft Resource Center reported 656 breaches in 2008, reflecting an increase of 47% over the previous year's total of 446.[3] A single vendor, Verizon, recently issued a report that analyzed 90 confirmed data breaches within its 2008 caseload, which encompassed 285 million compromised records.[4]

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 industries have their own privacy laws. For example, financial firms must contend with the reporting

---

1 William Shakespeare, Henry V, Act III.

2 Managing Director and Deputy General Counsel, Stroz Friedberg and 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.

3 Identity Theft Resource Center, Report on Data Breaches 2008, http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml

4 Verizon 2009 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, at 32.

requirements associated with the federal Gramm-Leach-Bliley Act,[5] and health care companies face broad reporting requirements under the new HITECH Act.[6] Across the broader economy, however, attorneys and companies worry most about a thicket of data breach notification statutes enacted by 45 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 46 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*.[7] 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 enforcement of the statutes by states. Finally, Part V presents specific recommendations for the state legislatures and enforcement agencies and for Congress, as well as for companies facing data breaches.

---

5 15 U.S.C. § 6801 *et seq*.

6 HITECH Act at §13402, codified at 42 U.S.C. §17932.

7 *See infra* at Part I.

I. Background[8]

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.[9] 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.[10] 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.[11] The company later said the breach had actually occurred and 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, since 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 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.[12] 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.[13] The

---

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

9 *See, e.g.,* Anthony D. Milewski Jr., 2 Shidler J. L. Com. & Tech. 19 (Apr. 14, 2006), *at* http://www.lctjournal.washington.edu/Vol2/a019Milewski.html and sources cited within.

10 Cal. Civ. Code §§ 1798.80 *et seq. See also* Milewski, *supra*.

11 *See* http://www.ftc.gov/opa/2006/01/choicepoint.shtm

12 http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf

13 http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf, http://www.ftc.gov/opa/2006/01/choicepoint.shtm

following year the company settled with 44 state attorneys general to resolve allegations that ChoicePoint had failed to adequately maintain the privacy and security of consumers' personal information.[14]

A flood of disclosures similar to ChoicePoint's soon followed[15] and in 2005 ten states enacted data breach notification statues.[16] Seventeen states followed suit in 2006,[17] another nine in 2007,[18] five in 2008,[19] and three thus far in 2009,[20] bringing the total number of states enacting data breach notification laws to 46.

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 "[i]t is the intent of the legislature to ensure that personal information about California residents is protected."[21] Similarly, the statute's disclosure requirements are focused on California residents:

(a) 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.[22]

The other 45 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.[23]

---

14 See http://www.naag.org/44_attorneys_general_reach_settlement_with_choicepoint.php The 44 states that participated in the settlement are Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin and the District of Columbia.

15 *See* "A Chronology of Data Breaches," http://www.privacyrights.org/ar/ChronDataBreaches.htm

16 The 10 states to enact data breach notification statutes in 2005 were Arkansas, Georgia, North Dakota, Delaware, Florida, Tennessee, Washington, Texas, North Carolina, and New York.

17 The 17 states that enacted statutes in 2006 are Connecticut, Louisiana, Minnesota, Nevada, new jersey, Maine, Ohio, Montana, Rhode Island, Wisconsin, Pennsylvania, Illinois, Idaho, Indiana, Nebraska, Colorado, Arizona.

18 In 2007 Hawaii, Kansas, New Hampshire, Utah, Vermont, Michigan, District of Columbia, Wyoming, Oregon enacted data breach notification statutes.

19 Maryland, Massachusetts, West Virginia, Iowa, and Virginia enacted new data breach notification statutes and Oklahoma passed a substantial revision to its statute.

20 Alaska, Missouri, and South Carolina have passed data breach notification statutes thus far in 2009.

21 Cal. Civ. Code § 1798.81.5.

22 Cal. Civ. Code § 1798.82(a).

23 See Alaska, Alaska Stat. § 45.48.010; Arizona, Ariz. Rev. Stat. § 44-7501(L)(4); Arkansas, § 4-110-105(a)(1); Colorado, Colo. Rev. Stat. Ann. § 6-1-716 (d)(I); Connecticut, Conn. Gen. Stat. § Sec. 36a-701b(b); Delaware, Del. Code Ann. Tit. 6, 12B-102 (a); District of Columbia, D.C. Code § 28-3852(a); Florida, Fla. Stat. §

Thus, under these statutes, it is the resident of the 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.

II. Personal Information Defined

A. The California Model

Most states have modeled their data breach statutes after California's 2002 groundbreaking law. 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.[24] 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. [25]

In 2007 California added two additional elements to the definition of personal information:

817.5681(1)(a); Georgia, Ga. Code. Ann. § 10-1-912; Hawaii, H.R.S. § 487N-2(a); Idaho, Idaho Code § 28-51-104(5), 28-51-105; Illinois, 815 Ill. Comp. Stat. § 530/10; Indiana, Ind. Code § 24-4.9-3-1; Iowa, § 715C.1-2; Kansas, Kan. Stat. Ann. § 50-7a02(a); La. Rev. Stat. Ann. § 51: 3074(a); Maryland, Md. Code Ann. §14-3502(A); Massachusetts, Mass. Gen. Laws 93H § 3; Michigan, Mich. Comp. Laws. § 445.72; Minnesota, Minn. Stat. § 325E.61, Subdiv. 1; Missouri, 407.1500. 2; Montana, Mont. Code Ann. § 30-14-1704 (1); Nebraska, Neb. Rev. Stat. § 87-803; Nevada, Nev. Rev. Stat. § 603A.220; New Hampshire, N.H. Rev. Stat. Ann. § 359-C:19 (V); New Jersey, N.J. Stat. Ann. 56:8-163(12)(a); New York, N.Y. Gen. Bus. Law § 899-aa.2; North Carolina, N.C. Gen. Stat. §75-65; North Dakota, N.D. Cent. Code § 51-30-02; Ohio, Ohio Rev. Code Ann. § 1349.19(A)(1)(a); Oklahoma, 2008 H.B. 2245(a); Oregon, Or. Rev. Stat. Section 2(2); Pennsylvania, 73 Pa. Stat. Ann. Section 2; Rhode Island, R.I. Gen. Laws, § 11-49.2-3; South Carolina, S.C. Code Ann. § 39-1-90; Tennessee, Tenn. Code Ann. 47-18-2107(b); Texas, Tex. Bus & Com. Code Ann. § 48.103(b); Utah, Utah Code Ann. § 13-44-202(1)(a); Vermont, 9 V.S.A. § 2430(2); Virginia, S.B. 307; Wash. Rev. Code § 19.255.010(1); West Virginia, W. Va. Code §46A-2A-101(6); Wisconsin, Wis. Stat. § 895.507; Wyoming, Wyo. Stat. Ann. 40-12-501 (a)(1).

[24] Cal. Civ. Code § 1798.82(e),

[25] Cal. Civ. Code § 1798.82(e).

- Medical information
- Health insurance information.[26]

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.[27]

B. Other State Variations

Some states include additional elements in the definition of "personal information" beyond the California model. For example, the Iowa,[28] Nebraska, [29] and Wisconsin[30] data breach notification statutes include unique biometric data, such as fingerprint, retina, or iris images in the definition. North Carolina[31] and North Dakota[32] 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.[33] (emphasis added)

It is also worth noting that the data breach statutes in Alaska,[34] Hawaii,[35] Indiana,[36] North Carolina,[37] Massachusetts,[38] and Wisconsin[39] include a breach of written as well as electronic data within the scope of their laws.

---

26 California Confidentiality of Medical Information Act, A.B. 1298.

27 The three states that do not exclude publicly available information from the definition of personal information are Michigan, Montana and Rhode Island.

28 Iowa Code § 715C.1(11).

29 Neb. Rev. Stat. § 87-802(5).

30 Wis. Stat. § 895.507(5).

31 N.C. Gen. Stat. § 75-65.

32 N.D. Cent. Code § 51-30-01(2)(a).

33 N.Y. Gen. Bus. Law. §899-aa(1)(a)-(b).

34 Alaska Stat § 45.48.090(1).

35 H.R.S. § 487N-1.

III. Defining a Data Breach

The 46 statutes define a "data breach" on a continuum from a strict liability standard to a risk-based approach. Some states define a breach simply as the "compromise" of a system,[40] whereas others incorporate into the definition 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.[41] 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

---

36 Ind. Code § 24-4.9-2-2 (2)(a).

37 N.C. Gen. Stat. § 75-65(a).

38 Mass. Gen. Laws., § 93H 1(a).

39 *See* Wis. Stat. § 895.507(b). In fact, Wisconsin's data breach statute never mention electronic data or computer systems, but requires an organization to notify all consumers – not merely Wisconsin residents – if it becomes aware that that someone has acquired personal information without authorization to do so. *See* Wis. Stat. § 895 507(2).

40 *See* discussion *infra* at Section III.A

41 *See* discussion *infra* at Section III.B.

"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.[42]

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."[43] 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 consumer.[44] Eight states—Delaware,[45] Georgia,[46] Illinois,[47] Minnesota,[48] North Dakota,[49] Texas,[50] Utah,[51] and Washington,[52] -- as well as the District of Columbia[53] follow this strict liability model.

Six of these states—Arizona,[54] Florida,[55] Idaho,[56] Nevada,[57] Oregon,[58] and Tennessee[59]—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

42 N.D. Cent. Code § 51-30-01 (1).

43 Cal. Civ. Code § 1798.82(d). 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.,* Cal. Civ. Code. § 1798.82(d).

44 *See* GAO Report to Congressional Requestors, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, GAO-07-737 (June 2007), at 37.

45 Del. Code Ann. Tit 6, § 12B-101(a).

46 *See* Ga. Code Ann. § 10-1-911(1).

47 *See* 815 Ill. Comp. Stat. 530/5.

48 *See* Minn. Stat. § 325E.61, Subdiv. 1(d).

49 S*ee* N.D. Cent. Code § 51-30-02.

50 *See* Tex. Bus. & Com. Code Ann. § 48.103.

51 *See* Utah Code Ann. § 13-44-102(1)(a).

52 *See* Wash. Rev. Code § 19.255.010(4).

53 *See* D.C. Code § 28-3851(1).

54 Ariz. Rev. Stat. § 44-7501

55 Fla. Stat. § 817.5681(4).

56 Idaho Code § 28-51-104(2).

57 Nev. Rev. Stat. § 603A.020.

58 Or. Rev. Stat. § 646A. 602(1)(a).

59 Tenn. Code. Ann. 47-18-2107(b).

security, confidentiality, or integrity of personal information."[60] (emphasis added) None of these states, however, 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.[61] For example, if an ex-boyfriend who hacks into a computer system and targets the personal information of only one person -- 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.

Two of these states -- Arizona[62] and Idaho[63] -- also require companies to undertake a reasonable investigation to determine whether there has been a security breach. However, neither statute provides detail 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, ___ 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,[64] Maine,[65] Nebraska,[66] New Hampshire,[67] Utah,[68] and Wyoming[69] --

60 Fla. Stat. § 817.5681(4) (emphasis added).

61 *See* Eric Friedberg and Michael McGowan, "Lost Back-Up Tapes, Stolen Laptops and Other Tales of Data Breach Woe," The Computer & Internet Lawyer (Oct. 2006).

62 Ariz. Rev. Stat. § 44-7501.

63 Idaho Code §§ 28-51-105.

64 Kan. Stat. Ann. §§ 70-7102.

65 10 Me. Rev. Stat. Ann. § 1348.

also require companies to determine whether there has been a misuse of individuals' information. As with Idaho and Arizona, these statues do not provide detail 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, it need not notify those individuals. These types of provisions are found in the data breach statutes of Alaska,[70] Arkansas,[71] Florida,[72] Iowa, [73] Rhode Island,[74] and Vermont.[75] 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.[76] 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

---

66 Neb. Rev. Stat. § 87-803(1).
67 N.H. Rev. Stat. Ann. § 359-C:20 I(a).
68 Utah Code Ann. §§13-44-102 b, 202.
69 Wyo. Stat. Ann. 40-12-501(a).
70 Alaska Stat. §45.48.010(c).
71 Ark. Code Ann. § 1167, § 4-110-105(d).
72 Fla. Stat. § 5681(10)(a)
73 Iowa Code § 715C.1(6).
74 R.I. Gen. Laws § 11-49.2-4.
75 V.S.A. § 435(d)(1).
76 Fla. Stat. § 817.5681(10)(a) – (b).

enforcement of the breach, providing 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.

Fifteen states -- Hawaii,[77] Iowa,[78] Indiana,[79] Kansas,[80] Massachusetts,[81] Montana,[82] New York,[83] North Carolina,[84] Ohio,[85] Oklahoma,[86] Pennsylvania,[87] South Carolina,[88] Virginia,[89] West Virginia[90] and -- 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. Massachusetts, for example, defines "breach of the security system" as:

> the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.[91]

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.[92] Michigan notes simply that "[i]n determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft," a person or agency shall act with the care an ordinarily prudent person or agency in like

77 H.R.S. § 487N -1.
78 Iowa Code § 715C.1(6).
79 Ind. Code § 24-4.9-2-2.
80 Kan. Stat. Ann. §§ 50-7°01-02
81 Mass. Gen. Laws 93H§ 1(G).
82 Mont. Code. Ann. § 30-14-1704(4)(a).
83 N.Y. Gen. Bus. Law, § 899-aa(c).
84 N.C. Gen. Stat. § 75-61(14).
85 Ohio Rev. Code Ann. § 1349.19(A).
86 74 Okla. Stat. 3113.3.
87 73 Pa. Stat. Ann., § 2302(a).
88 S.C. Code Ann. § 37-20-110(15).
89 Va. Code 18.2.-186.6(A).
90 W. Va. Code § 46A-2A-101(1).
91 Mass. Gen. Laws 93H§ 1(G).
92 N.Y. Gen. Bus. Law, § 899-aa(c).

position would exercise under similar circumstances.[93]

C. Blending Definitions: Risk Assessment and Strict Liability

Some 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 clawback 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 likely will not 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. [94]

There are similar provisions in the data breach notification statutes of Colorado, [95] Maryland,[96] Michigan,[97] Missouri,[98] New Jersey,[99] Oregon,[100] and Vermont,[101]

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: "Any incident of unauthorized access to and acquisition of encrypted records or data containing personal

---

93 Mich. Comp. Laws. § 445.72(12).
94 Conn. Gen. Stat. § 36a-701(b).
95 Colo. Rev. Stat. § 6-1-716.
96 Md. Code Ann. § 14-3504(B)(3).
97 Mich. Comp. Laws. § 445.72(12)(1).
98 Mo. H.B. No. 62, § 407.1500.2(5).
99 N.J. Stat. Ann. § C.56:8-163.
100 Or. Rev. Stat. § 646A.602.
101 V.S.A. § 435(d)(1).

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.[102]

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".[103] 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 person.[104]

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 law enforcement . . . or any measures to determine the scope of the breach and restore the reasonable integrity of the data system."[105] 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, incorporating a provision that notification would not be required if the investigation resulted in a determination that consumers had not been injured.[106] Other state statutes included requirements that companies undertake their own investigations and report their findings to law

---

102 N. C. Gen. Stat. § 75-61(14).
103 Mass. Gen. Laws 93H § 3(a).
104 Mass. Gen. Laws 93H § 3(a).
105 Calif. Civ. Code. § 1798.82(a).
106 *See supra* III.C.

enforcement or a regulatory authority.[107]

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 consumer's personal information has simply been acquired and accessed.[108] In states that focus on substantial risk of injury like Massachusetts, [109] 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 was this information accessed, when, and by whom?
- 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?[110]

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

---

107 *See supra* III.B.

108 N.D. Cent. Code §§ 51-30-02.

109 Mass. Gen. Laws 93H § 1(G).

110 *See* Eoghan Casey, "Data Theft: An Ounce of Forensic Preparedness is Worth a Pound of Incident Response," ISSA Journal (Aug. 2007).

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 "appropriate" investigation and prepare documentation that supports any resulting findings, a company would be wise to consider the services of digital forensic examiners, much 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.[111] These exemptions arise from the fact that these other

[111] *See* Alaska, Alaska Stat. § 45.48.040(c); Arizona, Ariz. Rev. Stat. § 44-7501(J)(1); Arkansas, Ark. Rev. Stat. § 4-110-106(a); California, Cal. Civ. Code § 4-110-106(5); Colorado, Colo. Rev. Stat. § 6-1-716(2); Connecticut, Conn. Gen. Stat. § 36a-701(f); Delaware, Del. Code. Ann. Tit. 6, § 12B-103(b); D.C., D.C. Code § 28-3852(g); Florida, Fla. Stat. § 817.5681(9)(b); Hawaii, H.R.S. § 487N-2(g); Idaho, Idaho Code § 28-51-106(2); Indiana, Indiana Code § 24-4.9-3-3.5; Iowa, Iowa Code § 715C.2(7)(C); Kansas, Kan. Stat. Ann. § 50-7a02(e); Maine, 10 Me. Rev. Stat. §1349(4); Maryland, Md. Code Ann. Code Ann. §14–3507(c); Mass. Gen. Laws 93H § 5; Michigan, Mich. Comp. Laws, §445.72(8)(b); Minnesota, Minn, Stat. § 325E.61, Subdiv. 4; Missouri, H.B 62 § 407.1500. 3; Montana, Mont. Code Ann. § 30-14-1702(8)(b); Nebraska, Neb. Rev Stat. §87-804; Nevada, Nev. Rev. Stat. § 603A.040(5)(a); New

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 Act, 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.[112]

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.[113] 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

---

Hampshire, N.H. Rev. Stat. Ann. § 359-C:19(V); North Carolina, N.C. Gen. Stat. § 75-65(h); North Dakota, N.D. Cent. Code § 51-30-06; Ohio, Ohio Rev. Code Ann. §1349.19(F)(1); Oklahoma, 74 Okla. Stat. § 3113.1; Oregon, Or. Rev. Stat. § 646A.602(8)(c); Pennsylvania, 73 Pa. Stat. Annot. § 7307(b); Rhode Island, R.I. Gen. Laws, § 11-49.2-7; South Carolina, S.C. Code Ann. § 39-1-90(J); Tennessee, Tenn. Code Ann. § 47-18-2107(i); Utah, Utah Code Ann. §13-44-202(5)(c); Vermont, 9 V.S.A. §2435(f); Virginia, Virginia Code Ann. § 18.2-186.6(A); West Virginia, W. Va. Code §46A-2A-102(f); Wisconsin, Wis. Stat. §134.98(3m); Wyoming, Wyo. Stat. Ann § 40-12-502(c).

[112] *See* 12 C.F.R. Pt. 30, App. B., Supp. A. III(A); 12 C.F.R. Pt. 208, App. D-2, Supp. A. § III(A); 12 C.F.R. Pt. 225, App. F, Supp. A § III(a); 12 C.F.R. Pt. 364, App. B, Supp. A, § III(A); 12 C.F.R. Pt. 570, App. B, Supp. § IIII(A); and 12 C.F.R. Pt. 748, App. B § III(A). *See also* "Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, GAO Report to Congressional Requesters," GAO-07-737 (June 2007).

[113] *See* Schwartz and Janger, Notification of Data Security Breaches, 913 Mich. L. Rev. 916 (2007) (arguing for determination of data security breaches and post-notification remediation by an independent third party).

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.

IV. 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[114] "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*."[115] (emphasis added)

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 45-days after there is a "determination of a breach."[116] In fact, the 45-day

114 Fla. Stat. § 817.5681(6).
115 Fla. Stat. § 817.5681(1)(a).
116 *Id.*

countdown to provide notice is subject to either tolling or nullification under several circumstances. First, the 45-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."[117] These measures may take a substantial period of time and no outside time limit is specified in the statute. Second, the 45-day countdown for notice is nullified and no notification is required under Florida law if, after a reasonable investigation, the company determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed.[118]

Only the data breach statutes in Ohio[119] and Wisconsin[120] replicate the 45-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."[121] (emphasis added) 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 45-day notification requirement is tolled. Wisconsin's statute, in contrast, posits that the only law enforcement exceptions to the 45-day rule must be related to the protection of an investigation or to homeland security.[122]

Another group of 30 states require a company to provide notice in the "most expedient time possible," "without unreasonable delay" or "as soon as possible."[123] In the seven states that require

---

117 *Id.*

118 *See* Fla. Stat. § 817.5681(10)(a).

119 Ohio Rev. Code Ann. § 1349.9(B)(2) (emphasis added)

120 Wis. Stat. § 895. 507(3).

121 Ohio Rev. Code Ann. § 1349.9(B)(2).

122 Wis. Stat. § 895.507(3).

123 The 30 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, *see* Alaska Stat. § 45.48.010; Arkansas, *see* Ark. Code Ann. § 4-110-105(d); California, *see* Cal. Civ. Code § 1798,82(a); Colorado, *see* Colo. Rev. Stat. § 6176(2); Connecticut, *see* Conn. Gen. Stat. § 36a-701b(b); Delaware, *see* Del. Code Ann. Tit 6, 12B-102(a); District of Columbia, *see* D.C. Code § 28-3852(a); Georgia, *see* Ga. Code Ann. § 10-1-912(a); Hawaii, *see* H.R.S. § 487N-2; Illinois, *see* 815 Ill. Comp. Stat. 530/10(a); Indiana, *see* Ind. Code § 24-4.9-3-3; Louisiana, *see* La. Rev. Stat. §

companies to undertake investigations, companies generally must first conduct a "reasonable and prompt" investigation to determine the likelihood that personal information has been or will be misused; if so, they must then provide notice in the most expedient time possible.[124]

A. Penalties

Consumers in California,[125] Hawaii,[126] New Hampshire,[127] North Carolina,[128] Washington[129] and the District of Columbia[130] 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[131] to a maximum of $750,000 in Michigan,[132] and a range of penalties in between.[133] In 26 states the attorney general may institute suit for actual damages or injunctive relief against organizations or individuals that violate the data breach statute.[134]

51:3074; Massachusetts, Mass Gen. Laws 93H §3; Michigan; *see* Mich. Comp. Laws. § 445.72(12)(4); Minnesota, *see* Minn. Stat. § 325E.61, Subdiv. 1(a); Missouri, H.B. No. 62, 407.1500.2(3); Montana, *see* Mont. Code Ann. § 30-14-1704(1); Nevada, *see* Nev. Rev. Stat. § 603A.220(1); New Jersey, *see* N.J. Stat. Ann. § 56:8-163(12)(a); New York, *see* N.Y. Gen. Bus. Law, § 899-aa(2); North Carolina, *see* N.C. Gen. Stat. § 75-65; North Dakota, *see* N.D. Cent. Code § 51-30-02; Oklahoma, 74 Okla. Stat. § 3113(3); Oregon, Or. Rev. Stat.§ 646A.604; Pennsylvania, *see* 73 Pa. Stat. Ann. § 2303(a); Rhode Island, *see* R.I. Gen. Laws, § 11-49.2-3; Tennessee, *see* Tenn. Code Ann., § 47-18-2107(d); Texas, *see* Tex. Bus. & Com. Code Ann. § 48.103(b); Utah, *see* Utah Code Ann. 13-44-202(2); Vermont, *see* V.S.A.. Tit. 9 § 2435(b)(1); Washington, *see* Wash. Rev. Code § 19.255.010(1).

[124] The seven states in which states first must conduct a "reasonable and prompt" investigation are Arizon, Ariz. Rev. Stat. § 44-7501; Idaho, Idaho Code §§ 28-51-105; Kansas, Kan. Stat. Ann. §§ 70-7102; Maine, 10 Me. Rev. Stat. Ann. § 1348; Nebraska, Neb. Rev. Stat. § 87-803(1); New Hampshire, N.H. Rev. Stat. Ann. § 359-C:20 I(a); Wyoming, Wyo. Stat. Ann. 40-12-501(a).

[125] *See* Cal. Civ. Code § 1798.84.

[126] Cal. Civ. Code § 1798.84.

[127] N.H. Rev. Stat. Ann. § 359-C:21.

[128] N.C. Gen. Stat. § 75-65-(i).

[129] Wash. Rev. Code. § 19.255(10)(a).

[130] D.C. Code § 28-3853(a).

[131] 10 Me. Rev. Stat. Ann. § 1349.2.

[132] Mich. Comp. Laws. § 445.72(13)-(14).

[133] In Arizona, companies face civil penalties up to $10,000, *see* Ariz. Rev. Stat. § 44-7501(H); in Hawaii, civil penalties up to $2,500 for each violation, *see* H.R.S.§ 487N -3; Idaho, fines of up to $25,000 per breach, *see* Idaho Code § 28-51-107; Indiana, civil penalties up to $150,000 per deceptive act; *see* Ind. Code § 24-4.9-4-2.

[134] The 26 jurisdictions in which state Attorneys General have authority to bring suits for damages or injunctive relief are Alaska, Alaska Code §45.48.080(a), Arkansas, Ark. Code Ann. § 4-109-108; Colorado, Colo. Rev. Stat. Stat. § 6176(4); Connecticut, Conn. Gen. Stat. 36a-701b(g); Delaware, Del. Code Ann. Tit. 6, § 12B-106; Illinois, 815 ILCS 530/20; Kansas, Kan. Stat. Ann. § 50-7a02(g); Louisiana, La. Rev. Stat. Ann. § 3075; Maine, Me. Rev. Stat. Ann., Tit. 10 § 1349.2; Iowa, Iowa Code § 715C.2(8); Maryland, Md. Code; Ann. § 14-3508; Massachusetts, Mass. Gen. Laws. Ch. 93H, § 6; Minnesota, Minn. Stat. § Subdiv. 6; Missouri, Mo. H.B. No. 62, § 407.1500.4; Nebraska, Neb. Rev. Stat. § 87-806; Nevada, Nev. Rev. Stat. § 603A.920; New Jersey, C.56:8-166; North Carolina, N.C. Gen. Stat. § 75-65(i); North Dakota, N.D. Cent. Code § 51-03-07; Ohio, Ohio Rev. Code Ann. § 1349.19(I); Oklahoma, 74 Okla. Stat. § 3113.3 Pennsylvania, 73 Pa. Stat. Annot. 2309; Tennessee, Tenn. Code An., 47-18-2106; Texas, Tex. Bus. & Com. Code Ann. § 48.201; Utah, Utah Code Ann. § 14-44-301(4); Vermont, V.S.A § 2435(g), Virginia, 18.2-186.6; West Virginia, W. Va. Code § 46A-2A-104; Wyoming, Wyo. Stat. Ann. § 40-12-502(f).

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, 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.[135] 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.[136] TJX also faced numerous individual and class action suits filed by consumers across the country.[137] 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

---

135 http://www.ftc.gov/os/caselist/0723055/080801tjxcomplaint.pdf

136 http://www.mass.gov/?pageID=pressreleases&agId=Cago&prModName=cagopressrelease&prFile=2007_02_07_tjx_investigation.xml

137 The actions filed against TJX, the parent company of TJ Maxx, include Robinson v. TJX Companies, Inc., et al., 07-cv-02139 (N.D. Ill.); Arians, et al. v. TJX Companies, Inc., et al., 07-cv-10769 (D. Mass.); Massachusetts Bankers Ass'n, et al. v. TJX Companies, Inc., et al., 07-cv-10791 (D. Mass.); Wardrop v. TJX Companies, Inc., et al., 07-cv-00430 (W.D. Mich); Taliaferro, et al. v. TJX Companies, Inc., et al., 07-cv-00388 (S.D. Ohio); Lack, et al. v. TJX Companies, Inc., et al., 07-cv-00233 (E.D. Tex.); Lamb, et al. v. TJX Companies, Inc., et al., 07-cv-00379 (W.D. Mo.); Roberts, et al. v. TJX Companies, Inc., et al., 07-cv-02887 (N.D. Ill.); and Mace v. TJX Companies, Inc., et al., (D. Mass.), which has been administratively designated as the lead case with respect to all actions pending in the District of Massachusetts, which have been consolidated.

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.[138] 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.[139] To settle the class action suits, TJX offered vouchers, cash, credit monitoring, identity theft insurance, and reimbursement to eligible class members.[140]

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.[141] The United States Judicial Panel on Multidistrict Litigation consolidated the six cases and transferred them to the Western District of Kentucky for pretrial proceedings.[142] 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.[143]

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

138 http://www.nmag.gov/Articles/newsArticle.aspx?ArticleID=718#FullArticle

139 http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf

140 http://www.tjxsettlement.com/

141 Goldman v. Countrywide Financial Corp., et al., 2008 WL 4236995, (S.D.Fla. Aug 22, 2008), Class Action Complaint with Injunctive Relief Sought and Demand for Jury Trial (NO. 08-61349).

142 In Re Countrywide Financial Corp. Customer Data Security Breach Litigation, MDL No. 1998 (Dec. 2, 2008).

143 http://www.ct.gov/ag/cwp/view.asp?A=2795&Q=422688

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.[144]

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.[145] The plaintiffs in the Express Scripts class action cited 11 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.[146]

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.[147] 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.[148]

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[149] and Walgreens,[150] that involved data breach complaints alleging that customers' medical information was improperly discarded in trash bins outside of the stores. The actions, however, were brought under HIPAA, not the Indiana data breach notification statute.

---

144 http://www.oag.state.ny.us/media_center/2007/apr/apr26a_07.html

145 Sansom v. Heartland Payment Systems, Inc., 2009 WL 217497, *217497+ (Trial Pleading) (D.N.J. Jan 23, 2009) Class Action Complaint (No. 33AV00001).

146 Amburgy, v. Express Scripts, Inc., 2009 WL 1344547, *1344547 (E.D.Mo. May 08, 2009) Class Action Complaint (No. 09705).

147 Irwin, v. RBS WorldPay, Inc., 2009 WL 412516, *412516 (Trial Pleading) (N.D.Ga. Feb 05, 2009) First Amended Class Action Complaint (No. 109-CV-0033).

148 Throckmorton v. Metropolitan Gov't of Nashville, *et al.* 2008 WL 227312, *227312+ (Tenn. Cir. Ct. Jan 04, 2008) Verified Complaint (No. 08C43).

149 http://www.in.gov/attorneygeneral/press/CVSSettlement20090710.pdf

150 http://www.in.gov/attorneygeneral/press/WalgreensSettlement20090710.pdf

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 24 states incorporate provisions that allow companies to take "any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system;"[151] any time limits are tolled while the company is under taking such an investigation. Seven states also require companies to undertake a "reasonable" investigation to undertake the scope of the breach. [152] 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.

V. Recommendations: Toward a Federal Data Breach Notification Standard

A. Data Breach Notification Statute for HIPAA-Covered Entities

The 2009 economic stimulus legislation includes requirements that "covered entities" as defined under the Health Insurance Portability and Accountability Act (HIPAA) provide notices to consumers of any breaches in the security of their protected health information (PHI). "Business associates" of HIPAA-covered entities will also be required to report such breaches to covered entities.[153]

Congress uses a hybrid approach in its notification requirement, defining "breach" as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." §13400(1)(A). There is an another exception for certain circumstances involving inadvertent acquisition, access, or use

151 *See supra* Section III.B.

152 *See supra* Section III.B.

153 H.R. 1 (111th Cong., 1st Sess., Feb. 17, 2009) at §13402(a) & (b).

of PHI by employees and agents of covered entities or business associates where the information is not further acquired, accessed, used, or disclosed. [154]

The notification of breach provisions apply to PHI that is "unsecured." The legislation leaves the definition of "unsecured" to the Secretary of Health and Human Services to address within 180 days of the statute's passage in February 2009, that is by August 2009. The provisional standard included by the statute, however, defines "unsecured" information as:

> [p]rotected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.[155]

Congress' enactment of a federal data breach notification requirement for PHI is an important first step toward a rationalization of data security standards. Congress should now take the next step and enact a statute that applies to *consumers'* PII, as defined by California's statute, and incorporating 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.[156] The form letters generally provide consumers with no 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.

Instead, Congress should enact a statute that provides that notification is not required if, after an appropriate investigation, 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

---

154 H.R. 1 (111th Cong., 1st Sess., Feb. 17, 2009) at §13402(a) & (b).§13400(1)(B)

155 H.R. 1 (111th Cong., 1st Sess., Feb. 17, 2009) at §13402(h)(1)(B).

156 *See* Schwartz and Janger, Notification of Data Security Breaches, *913* Mich. L. Rev. 916 (2007) (arguing for determination of data security breaches and post-notification remediation by an independent third party).

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.

B. Waiting for Godot:[157] 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

157 Samuel Beckett (1956).

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[158] and the rule regulating the "pay-per-call" industry[159], which provide such authority to both 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 law.

158 16 C.F.R. § 310.7.

159 16 C.F.R § 308.7.