https://doi.org/10.48009/1_iis_2016_107-118

Issues in Information Systems
Volume 17, Issue I, pp. 107-118, 2016

ATTRIBUTES OF DATA BREACH NOTIFICATION LAWS IN THE UNITED STATES

David T. Green, Governors State University dgreen@govst.edu
Nancy L. Martin, Southern Illinois University Carbondale nlmartin@siu.edu

ABSTRACT

The United States currently does not have a federal law covering data breach notifications for most areas of commercial activity involving consumer data. In place of a common federal law, many US states have enacted laws that address data breaches to varying degrees. This paper identifies the common attributes of state laws in the US to determine common requirements that may be useful for inclusion in federal breach notification legislation.

Keywords: Data Breach, Privacy, Notification, Law, Information Security

INTRODUCTION

President Obama has called on the United States Congress to pass a national data breach law to provide "one clear national standard" because at present there is a "patchwork of state laws that dictate how companies should respond to data breaches" (Perlroth, 2014). A data breach is a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed" (ISO/IEC 27040).

Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have passed laws requiring government and private organizations to notify individuals when a security breach has occurred involving the individual's personal information (NCSL, 2015).

Although there are many common attributes among data breach notification laws that have been enacted, there are variations in some areas.

DATA BREACHES

Hacks of consumer personal information have become a regular occurrence with security breaches impacting a wide variety of industries including banking, retail, and healthcare. There is a significant cost and time associated with individuals affected by data breaches (Gatzlaff & McCullough, 2012), and few cases of identity theft are solved (Owens, 2014). Data breaches are "expensive and time-consuming" for organizations and individuals impacted by a breach (Gatzlaff & McCullough, 2012).

Legislation is necessary for defining entities, organizations or individuals, who must comply; definitions of personal information; information regarding what constitutes a breach; requirements for notification; exemptions to notification; and penalties/consequences of failure to comply.

METHODOLOGY

Using a policy analysis technique, the common attributes of state security breach notification legislation were examined. The starting point was the National Conference of State Legislatures list of state security breach notification laws (NCSL, 2015). Based on an initial review of laws a set of attributes were defined that appear in

most laws. Twenty-two laws focus on both electronic data and paper records, while twenty-four focus on electronic data records.

ATTRIBUTES OF STATE DATA BREACH NOTIFICATION LAWS

Scope of the Statue - Who Must Comply?

State legislation typically determines the categories of entities for which the law applies. Most categorize the entities as businesses, data and information brokers, and government entities, covering one or more of the categories. Forty-six laws cover business entities; thirty-five include government; and two laws specifically identify information brokers, an entity that might also be considered a business (see Table 1).

Table 1. Count of States with Privacy Laws Covering Each Entity Type

Entity Type	# Laws
Business	46
Government	35
Information Brokers	2

Definitions of Personal Information

Among the legislation, 'personal information' is defined as first name, last name or usernames plus an additional piece(s) of identifiable information including social security number, state ID or drivers' license; account/credit/debit card number; or username/email plus password or security question. Some laws clarify that even if certain data has been breached the organization may not be required to notify individuals if the data breached was encrypted, unless the encryption key was also lost. Only three state laws cover encrypted personal information.

What Constitutes a Breach?

Personal information as defined by the law must either be breached or likely misused or both, triggering a notification. A breach is defined as "unauthorized access" or "unauthorized acquisition" of covered personal information maintained by a covered entity. Some definitions of a breach go into greater detail regarding exemptions for encrypted, unreadable or unusable data that may be impacted. Some laws describe how illegal use or likelihood of illegal use of the personal information. State statutes typically define a breach similar to the following: *"Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity."*

Notification requirements range from vague "shall be made without unreasonable delay" while giving time for the covered entity to determine the scope of the breach. Some specify 30-45 days unless law enforcement approves due to reasons related to an ongoing criminal investigation.

The method of notification typically includes one or more of the following forms of communication: written, electronic, or telephonic. Exemptions to notification or timing of notification may include:

> *Data was likely misused but not breached*. In consultation with law enforcement, a determination may be made that the personal information misused will not result in identity theft or other harm to individuals.
>
> *Data was encrypted*. If the personal information was encrypted or only included elements of the data that are unusable an exemption may be allowed.
>
> *On-Going Law Enforcement Investigation*. If law enforcement determines notification would harm an on-going investigation an exemption may be consider but often requires a written request from the law enforcement agency.

Fifteen states do not require notification if there is a low risk of harm. The penalties of failure to notify individuals after a breach include a range from as little as no consequence at all to consequences including fines (with maximum fines ranging from $0-$500,000); civil action for recovering damages; and prison time. Alternatively, some laws refer to other laws covering consumer fraud. Figure 1 includes the text of all state data breach notification laws. The word cloud highlights the most frequently used words and phrases by increasing the size of the word for more frequent words.

Figure 1. Word Cloud Including Data Breach Definitions from All State Privacy Laws

FEDERAL

A company operating across the nation must follow state law among 47 states and the District of Columbia. When enacted, US federal law supersedes state legislation. In the US, federal law does exist for data privacy and breach notification in a few contexts, including financial information (Gramm Leach Bliley Act; Sarbanes-Oxley Act), health information (Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act of 2009), and student educational records (Family Educational Rights and Privacy Act). Other consumer information used by retailers or other organizations outside healthcare and financial services is not protected by federal law in the US.

Beyond requirements of law, there may be competitive market pressures for companies to notify consumers about data breaches, but given the inconsistencies among state legislation, and the inclusion of data privacy and breach notification requirements in specific settings, including general individual data in any context is an important step to provide uniform responses and penalties within the United States.

CONCLUSION

Based on the policy analysis of forty-seven state data breach notification laws it is clear there are differences across laws, but the general structure of each law is very similar with each including language that defines the covered entity, defines personal information, determines what constitutes a breach, requirements for notification, and penalties or consequence of failure to comply). A federal law will be next logical step because data breaches are on the rise (Williamson, 2015) and litigation occurring as a result of data breaches is increasing (Grossenbacher, 2015). A federal law would increase protections for consumers and decrease the complexity and expense for businesses attempting to comply with a patch work of laws across states. Statutes citations and summary data are included in Appendix 1 and 2.

REFERENCES

Gatzlaff, K. M., & McCullough, K. A. (2012). Implications of Privacy Breaches for Insurers. *Journal of Insurance Regulation*, *31*.

Grossenbacher, K. (2015). Businesses Need a Preemptive Federal Law on Data Breach Notification. *The Hill.* http://thehill.com/blogs/congress-blog/judicial/248978-businesses-need-a-preemptive-federal-law-on-data-breach

ISO/IEC 27040. (2015). ISO Standards Catalogue.

National Conference of State Legislatures. (2015) Security Breach Notification Laws. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Owens, M. (2004). Policing Privacy: Michigan Law Enforcement Officers on the Challenges of Tackling Identity Theft. http://pirgim.org/reports/policingprivacy04.pdf

Perlroth, N. (December 4, 2014). Hacked vs. Hackers: Game On. New York Times Bits Blog. http://bits.blogs.nytimes.com/2014/12/02/hacked-vs-hackers-game-on/?_r=0

Federal Trade Commission. (2000). Fair Information Practices. https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

Williamson, W. (2015). Data Breaches by the Numbers. Security Week, August 31, 2015. http://www.securityweek.com/data-breaches-numbers

Appendix 1: United States Data Breach Notification Law Citations by Statute Entity

State	Statute (By Entity)	
	Business/ Information Broker	Government
Alabama	NONE	
Alaska	Alaska Stat. § 45.48.010 et seq.	
Arizona	Ariz. Rev. Stat. § 44-7501	
Arkansas	Ark. Code § 4-110-101 et seq.	
California	Cal. Civ. Code §§ 1798.29, 1798.80 et seq.	Cal. Civ. Code §§1798.29,
Colorado	Colo. Rev. Stat. § 6-1-716	
Connecticut	Conn. Gen Stat. § 36a-701b	
Delaware	Del. Code tit. 6, § 12B-101 et seq.	
Florida	Fla. Stat. § 817.5681	
Georgia	Ga. Code §§ 10-1-910, -911, -912;	
Hawaii	Haw. Rev. Stat. § 487N-1 et seq.	
Idaho	Idaho Stat. §§ 28-51-104 to -107	
Illinois	815 ILCS §§ 530/1 to 530/25	
Indiana	Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.	
Iowa	Iowa Code §§ 715C.1, 715C.2	
Kansas	Kan. Stat. § 50-7a01 et seq.	
Kentucky	Ky. Rev. Stat. Ann. §§ 365.720 – .734	KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. § 51:3071 et seq.	
Maine	Me. Rev. Stat. tit. 10 § 1347 et seq.	
Maryland	Md. Code Com. Law §§ 14-3501 et seq.,	Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.	
Michigan	Mich. Comp. Laws §§ 445.63, 445.72	
Minnesota	Minn. Stat. §§ 325E.61, 325E.64	
Mississippi	Miss. Code § 75-24-29	
Missouri	Mo. Rev. Stat. § 407.1500	
Montana	Mont. Code § 30-14-1701 et seq.	Mont. Code§ 2-6-504

Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807	
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183	
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21	
New Jersey	N.J. Stat. § 56:8-163	
New Mexico	NONE	
New York	N.Y. Gen. Bus. Law § 899-aa,	N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65	
North Dakota	N.D. Cent. Code § 51-30-01 et seq.	
Ohio	Ohio Rev. Code §§ , 1349.19, 1349.191, 1349.192	Ohio Rev. Code §§1347.12
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166	
Oregon	Oregon Rev. Stat. § 646A.600 et seq.	
Pennsylvania	73 Pa. Stat. § 2301 et seq.	
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.	
South Carolina	S.C. Code § 39-1-90, 2013 H.B. 3248	
South Dakota	NONE	
Tennessee	Tenn. Code § 47-18-2107	
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053, Tex. Ed. Code § 37.007(b)(5)	
Utah	Utah Code §§ 13-44-101 et seq.	
Vermont	Vt. Stat. tit. 9 § 2430, 2435	
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05	
Washington	Wash. Rev. Code § 19.255.010, 42.56.590	
West Virginia	W.V. Code §§ 46A-2A-101 et seq.	
Wisconsin	Wis. Stat. § 134.98	
Wyoming	Wyo. Stat. § 40-12-501 et seq.	

Appendix 2: United States Data Breach Notification Law Attributes Summary

State Abbrev.	Entities	Personal Information				Notification			Max. Fine	Other Contents
		Personal Information Includes（First/Last Name+following）	Does Health information include?	Encrypted？	Does Statute Cover Electronic Data, Paper Records, or Both?	Notice shall be made without unreasonable delay	Notification required if there is a Low Risk of Harm?	Exemptions（Maintains its own notification procedures could be deemed to be compliance with the notification req.）		Req. for protection of personal information when discards
AK	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	--	50,000	--
AL										
AR	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	Yes	No	Electronic Data	Yes	No	Yes	$10,000	Yes
AZ	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	Yes	$10,000	--
CA	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	Yes	No	Both	Yes	Yes	--	$3,000	--
CO	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	Yes	--	Yes
CT	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	Yes	$5,000	--
DE	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	Yes	$10,000	--
FL	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card	Yes	No	Both	Yes	Yes	Yes	500,000	--

		number +Personal Code								
GA	Business, Information Brokers, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	Yes	--	--	--
HI	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	--	2,500	--
IA	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	--	$40,000	--
ID	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	Yes	25,000	--
IL	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	Yes	Yes	$50,000 (plus an additional $10,000 if victim is 65 years of age or older)	Yes
IN	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No (Yes, state agency)	Yes	150,000	Yes
KS	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	Yes	--	--
KY	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	Yes	No	Both	Yes	No	Yes	--	Yes
LA	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	Yes	No	Electronic Data	Yes	No	Yes	--	--
MA	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card	No	No	Both	Yes	No	Yes	$5,000, or $10,000 for violating	--

		number +Personal Code							an injunction entered pursuant to an enforcement action	
MD	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	Yes	$1,000 for first violation,$5,000 for any subsequent violation by a covered merchant	Yes
ME	Business, Information Brokers, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	--	2,500	--
MI	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	--	750,000	--
MN	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	Yes	--	$25,000	--
MO	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	Yes	No	Electronic Data	Yes	No	Yes	--	--
MS	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	--	$10,000	--
MT	Business, Government Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	--	Both	Yes	No	--	$10,000	--
NC	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	--	$5,000	--
ND	Business	SSN, State ID/Drivers'License,	No	No	Electronic Data	Yes	Yes	Yes	$1,000	--

		Credit/Debit Card number +Personal Code								
NE	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	--	Electronic Data	Yes	Yes	Yes	--	--
NH	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	--	$10,000, and no less than double and no more than treble damages in private actions upon finding of willful violation	--
NJ	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	--	Both	Yes	No	--	--	Yes
NM										
NV	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	Yes	Yes	--	Yes
NY	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	--	Electronic Data	Yes	Yes	--	$150,000	--
OH	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	--	penalties can be as high as $10,000 per day of noncompli ance	--
OK	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No (Yes, state agency)	--	150,000	--
OR	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	--	$500,000	Yes

PA	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	Yes	--	$5,000	--
RI	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	Yes	--	$25,000	--
SC	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	--	$1,000 per resident whose informatio n was accessible if violation was knowing and willful	--
SD										
TN	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	Yes	Electronic Data	Yes	Yes	--	The greater of $10,000; $5,000 per day of an assumed identity theft; or 10 times the amount obtained using the identity theft	--
TX	Business, Student	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	Yes	Yes	$50,000, plus $250,000 for failure to take reasonable action to comply with notice requireme nts	Yes
UT	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	Yes	$100,000	Yes
VA	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	Yes	Yes	Electronic Data	Yes	No	Yes	$150,000	--

VT	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	Yes	Both	Yes	No	--	$10,000	--
WA	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	Yes	--	--
WI	Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Both	Yes	No	--	$1,000	Yes
WV	Business, Governme nt Entities	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	Yes	Yes	$150,000	--
WY	Business	SSN, State ID/Drivers'License, Credit/Debit Card number +Personal Code	No	No	Electronic Data	Yes	No	--	--	--