

# Complying with Data Breach Notification Laws



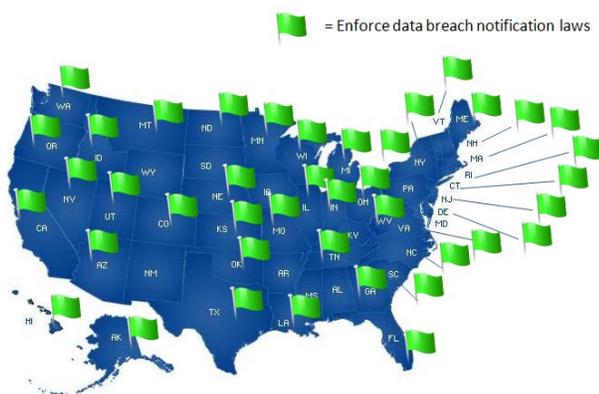
July 2011

## Introduction to data breach notification laws

Data breach notification laws, sometimes referred to as “information security laws,” are a growing number of regulations designed to ensure that companies protect personal identifiable information from theft or unauthorized access. Data breach notification laws typically require organizations to inform customers if their personal information was or had the possibility of being accessed without authorization<sup>1</sup>.

The first of such regulations enforced in the United States was the California data breach notification law Cal. Civ. Code 1798.82 and 1798.29. This law states “[...] a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. [...]”

As of 2010, almost all States enforce data breach notification requirements, as highlighted from the picture below.



<sup>1</sup> *Federal Information Security and Data Breach Notification Laws*, Congressional Research Service, 2010.

## How do you know if your company is subject to data breach notification laws?

There are two factors that may help you determine whether you must comply with notification laws:

- Your organization is active in a State or Country that enforces notification laws (see Appendix 1)<sup>2</sup>
- Customers’ personal identifiable information are stored unencrypted on a PC, laptop or desktop, that could be lost or stolen

Similar regulations apply in Europe, where the first of such laws was enforced in Sweden as early as 1973. Many other countries have implemented or have data breach notification laws on their political agendas<sup>3</sup>.

## Effects of potential breaches

The implications of a security breach that includes customers’ personal identifiable information may differ depending on State or Country-specific regulations.

In the U.S., most data breach notification laws require:

- Communication to the affected individuals in the “most expedient time possible, without unreasonable delay”
- Civil and criminal charges often apply in the case of a breach.

<sup>2</sup> *National Conference of State Legislature*, as of April 12, 2010. <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>

<sup>3</sup> *Data Breach Notification Laws in Europe*, Privacy Laws & Business, 2009. [http://www.privacylaws.com/Documents/data\\_breach\\_conference.pdf](http://www.privacylaws.com/Documents/data_breach_conference.pdf)

- Depending on the specific regulation, if customers cannot be reached directly organizations may be required to notify the public through the use of media<sup>4</sup>

Such notification requirements, however, do not apply if the organization can provide evidence that sensitive information was protected with encryption and/or other security solutions.

### Costs of losing laptops with sensitive information

Losing a laptop is one of the most common types of security breaches requiring prompt communication to customers under data breach notification laws.

According to Aberdeen Group, companies lose on average 4.7% of their endpoints (such as laptops) every year. This figure is a conservative estimate as it does not include the additional 10% of “missing inventory,” such as computers that cannot be found but are not confirmed to be lost or stolen<sup>5</sup>.

The Ponemon Institute reports that organizations experiencing missing or stolen equipment may incur significant costs, as high as \$50,000 per lost machine, especially if they are subject to data breach notification laws<sup>6</sup>. Data breach costs account for almost 80% of the total expenses associated with a lost computer. Legal and forensic costs account for an extra 4%.

Seven cost component	Average cost
Laptop replacement cost	1,582
Detection & escalation cost	262
Forensics & investigation cost	814
Data breach cost	39,297
Intellectual property loss	5,871
Lost productivity cost	243
Other legal or regulatory costs	1,177
<b>Total</b>	<b>\$49,246</b>

Exposure to security breaches may bring even higher costs. Aberdeen Group reports the average costs of incidents may add up to as much as \$640,000 when taking into account lost revenues, bad press, etc<sup>7</sup>.

### Reducing liability through full disk encryption and strong authentication

Best-in-class organizations have effectively managed to decrease their exposure to potential security breaches by deploying security software solutions aimed at protecting data stored on the computer and securing how users access the data or other business resources.

Organizations that have deployed data protection solutions, such as full disk encryption, have been able to reduce the number of breach exposure incidents experienced in the last twelve months by 84%<sup>8</sup>. Similarly, 52% of the companies surveyed with strong authentication not only reduced the number of

<sup>4</sup> An example of regulation including such requirement is the HITECH Act.

<sup>5</sup> *Laptop Lost or Stolen? Five Questions to Ask and Answer.* Aberdeen Group, 2010.

<sup>6</sup> *The Cost of a Lost Laptop.* The Ponemon Institute, 2009.

<sup>7</sup> *Full Disk Encryption on the Rise.* Aberdeen Group, 2009.

<sup>8</sup> *Id.* at 7.

security breaches, but also reduced the number of human errors related to security by 80%<sup>9</sup>.

DigitalPersona® Pro's Full Disk Encryption feature can help meet the requirements imposed by data breach notification laws by providing several security methods to protect all data stored on a computer. For example, IT Managers can enforce encryption of the entire hard drive on managed computers.

Once the hard drive is encrypted, users will be required to provide proper authentication credentials (password, fingerprint, or smart card), according to policies specified by the IT manager, before the Windows operating system starts (i.e. pre-boot authentication).



For convenience, the software provides the option to automatically unlock the drive and securely log on to Windows without further authentication (i.e. Single Sign-On, also called One-Step Logon).

DigitalPersona Pro's Full Disk Encryption meets the technical requirements mandated by NIST for both data at rest and data in motion, which include AES algorithm and/or FIPS 140-2.

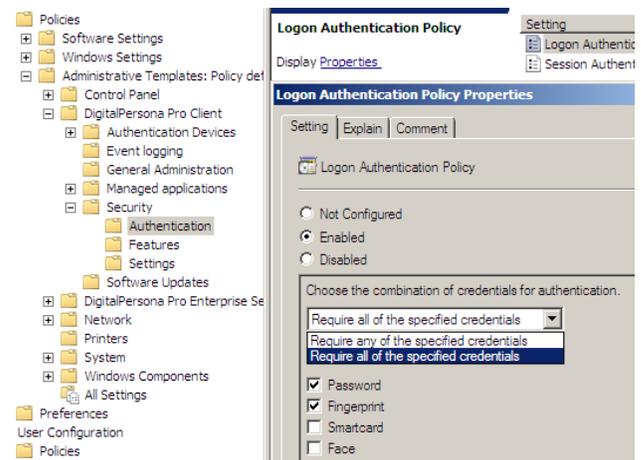
In addition, DigitalPersona Pro supports strong authentication which helps IT Managers further improve the security of the systems and reduce the

<sup>9</sup> *Strong User Authentication: Best-in-Class Performance at Assuring Identities*. Aberdeen Group, 2008.

risks related to insider threats. Two-factor authentication, including biometrics, makes it more difficult for users to share credentials, thus reducing the risk of unauthorized access.

With DigitalPersona Pro, IT Managers can select and enforce authentication policies for computers and application logon in just a few steps. For example, to mandate a two-factor PC logon policy requiring a password and a fingerprint, IT Managers can use DigitalPersona Pro Enterprise to:

1. Go to the Active Directory **Group Policy Management Editor**
2. Browse to **Computer Configuration > Policies > Administrative Templates > DigitalPersona Pro client > Security > Authentication**
3. Double-click the **Logon policy** policy object
4. Select **Enabled**
5. Select **Require all of the specified credentials**
6. Select **Password and Fingerprint**



### DigitalPersona Pro: security and compliance with a high ROI

DigitalPersona Pro provides small businesses and enterprises with a powerful, flexible solution for integrated data protection and strong authentication.

DigitalPersona Pro's efficient management of multiple security and authentication applications, combined with a low Total Cost of Ownership, helps organizations increase security and compliance while achieving a high Return on Investment. Based on industry data, an organization with 1,000 seats may be able to achieve cost savings of \$340,000 by using DigitalPersona Pro.

Cost saving item	Potential savings
Savings in value of lost Intellectual Property	\$ 275,937
Savings in password-related Help Desk calls	\$ 54,275
Savings in IT costs by adopting efficient management of authentication	\$ 10,745
<b>Total potential cost savings</b>	<b>\$ 340,957</b>

These estimates do not take into account any reduction to potential liability exposure of a security breach, which could easily add up to millions of dollars.

Key benefits of DigitalPersona Pro include:

- Full disk encryption with pre-boot authentication and BIOS-level integration<sup>10</sup>
- Strong authentication with a variety of credentials, including fingerprints, face recognition, smart cards, one-time (OTP) tokens, and smartphones. Support extends to fingerprint readers built into notebooks, peripherals and a wide range of smart cards and OTP devices
- Two-Factor VPN authentication for secure remote access that supports all RADIUS-based Virtual Private Networks, such as Cisco
- Powerful access recovery to "rescue" users who are locked out of their PCs, even when no network connection is available

<sup>10</sup> Available on select computers.

- Flexible deployment options that include a cloud-based Software-as-a-Service solution, as well as Active Directory-based management
- High security with FIPS 140-2 compliant encryption for sensitive user data
- High Return on Investment and low Total Cost of Ownership compared to other solutions

DigitalPersona's award-winning technology has been used worldwide by thousands of companies and more than 100 million users for security and compliance. Customers range from small businesses to the U.S. Department of Defense.

DigitalPersona powers HP ProtectTools, the security suite preloaded by Hewlett-Packard on millions of business notebooks and desktops every year. Now you can use DigitalPersona Pro to centrally manage HP ProtectTools-enabled computers or any mixed environment of HP ProtectTools and DigitalPersona Pro client software.

### To Learn More

For more information about DigitalPersona Pro, visit [www.digitalpersona.com](http://www.digitalpersona.com) or contact us at:

- Email: [sales@digitalpersona.com](mailto:sales@digitalpersona.com)
- In North America, call: +1-650-474-4000
- In EMEA, call: +44-203-286-4004

Free trials are available.

### About DigitalPersona

DigitalPersona, Inc. is a global provider of authentication and endpoint protection solutions that make security simple, practical and affordable for businesses of all sizes. The company helps enterprises, government agencies, custom application developers

and independent software vendors to efficiently address growing security, compliance and fraud-prevention demands. DigitalPersona's award-winning technology is offered by market-leading computer manufacturers and solution providers around the world.

#### **Disclaimer**

**THE INFORMATION IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED TO BE ANYTHING OTHER THAN THE EDUCATED OPINION OF THE AUTHOR. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT DIGITALPERSONA MAKES NO CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS, OR ADEQUACY OF THE INFORMATION. THIS INFORMATION SHOULD NOT BE RELIED UPON AS LEGAL ADVICE. DIGITALPERSONA SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS OR COMPLIANCE WITH ANY LEGAL REQUIREMENTS.**

© 2011 DigitalPersona, Inc. All rights reserved. DigitalPersona, is a trademark of DigitalPersona, Inc. registered in the U.S. and other countries. All other brand and product names are trademarks or registered trademarks of their respective owners.

Appendix 1 – Data breach notification laws in the US, by State<sup>11</sup>

State	Data breach notification law(s)
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 §§ 56.06, 1785.11.2, 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. 36a-701(b)
Delaware	Del. Code tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. § 817.5681
Georgia	Ga. Code §§ 10-1-910, -911
Hawaii	Haw. Rev. Stat. § 487N-2
Idaho	Idaho Code §§ 28-51-104 to 28-51-107, 2010 H.B. 566
Illinois	815 ILCS 530/1 et seq.
Indiana	Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq., 2009 H.B. 1121
Iowa	Iowa Code § 715C.1 (2008 S.F. 2308)
Kansas	Kan. Stat. 50-7a01, 50-7a02
Louisiana	La. Rev. Stat. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq., 2009 Public Law 161
Maryland	Md. Code, Com. Law § 14-3501 et seq.
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Mich. Comp. Laws § 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	2010 H.B. 583 (effective July 1, 2011)
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code § 30-14-1701 et seq., 2009 H.B. 155, Chapter 163
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat. 603A.010 et seq.
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21
New Jersey	N.J. Stat. 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 et seq.
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. § 74-3113.1 and 2008 H.B. 2245
Oregon	Oregon Rev. Stat. § 646A.600 et seq.
Pennsylvania	73 Pa. Stat. § 2303
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.
South Carolina	S.C. Code § 39-1-90
Tennessee	Tenn. Code § 47-18-2107, 2010 S.B. 2793
Texas	Tex. Bus. & Com. Code § 521.03
Utah	Utah Code §§ 13-44-101, -102, -201, -202, -310
Vermont	Vt. Stat. tit. 9 § 2430 et seq.
Virginia	Va. Code § 18.2-186.6, 2010 H.B. 1039 (effective January 1, 2011)
Washington	Wash. Rev. Code § 19.255.010, 2010 H.B. 1149 (effective July 1, 2010)
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98 et seq.
Wyoming	Wyo. Stat. § 40-12-501 to -502
District of Columbia	D.C. Code § 28-3851 et seq.
Puerto Rico	10 Laws of Puerto Rico § 4051 et. seq.
Virgin Islands	V.I. Code § 2208

<sup>11</sup> Id. at 2.