

# CAMPUS SECURITY BREACHES: COMPLIANCE WITH STATE NOTIFICATION STATUTES

(This article was previously published by a National Higher Education Association)

## Authors:

[Kenneth D. Salomon](#)

[Peter C. Cassat](#)

[Briana E. Thibeau](#)

## INTRODUCTION:

Over the past few years, data security breaches at corporations, government agencies, colleges, and universities have become a pervasive and highly publicized problem. Since February 2005, over 50 million people have had their personal information potentially exposed by unauthorized access to the computer systems of companies and institutions that store such data [1]. While large companies such as ChoicePoint, Bank of America, and DSW Shoe Warehouse have found themselves the focus of the media spotlight after experiencing such breaches, one-half of all reported security breaches since February 2005 have occurred at colleges and universities [2].

This Note addresses the implications of security breach notification laws for colleges and universities. In particular, the Note discusses the applicability of these laws to both public and private institutions, the compliance obligations imposed in the event of a security breach, and whether the obligations vary for in-state versus out-of-state students and employees. The Note also provides practical guidance to counsel and administrators on how to comply with security breach notification laws should a breach occur, and how to coordinate their institution's compliance approach in light of the privacy requirements imposed under other laws and regulations.

## DISCUSSION:

### I. Overview of Existing State Laws

According to consumer privacy advocates, most, if not all, of the reported data breaches within the last year might have gone unreported if not for the California legislature's enactment of the first data security breach notification law in July 2003 [3]. That law "forces state agencies and organizations doing business in California, including institutions of higher education, to notify California residents when a security breach results in the release of personal information. Potential victims must be made aware that their personal information may have been obtained by others so they can take action to prevent or minimize the effects [4]." Since July 2003, nearly half the states have passed or introduced legislation requiring businesses and, in some cases, state agencies to notify consumers if their personal information may have been exposed by an unauthorized security breach [5].

These security breach notification laws generally require that state residents be notified if the security, confidentiality, or integrity of their electronically stored, unencrypted personal information is breached in any way. While some of these laws apply to a narrow range of entities, such as information or data brokers (e.g., ChoicePoint), government agencies, or private businesses [6], most apply more broadly to any person, business, or state agency that conducts business within the state and stores personal information electronically [7].

#### *Definition of Personal Information*

Most states have modeled their security breach notification laws on California's statute and, like California, generally define "personal information" to include a person's first name or initial and last name, in combination with one or more of the following data elements: social security number, driver's license or state identification

card number, or any account number or credit or debit card number that is accompanied by the required security code, access code, or password that would permit an unauthorized person to access the individual's financial account [8]. A few states, however, have adopted more expansive definitions of "personal information" that include data such as a person's date of birth, mother's maiden name, employee identification number, electronic signature, medical information, or even that person's "personal characteristics [9]."

### *Notification Requirements*

With few exceptions, existing state security breach notification laws require notification any time a resident's information is exposed – regardless of the location of the breach or the entity suffering the breach. For example, under California's law, any business or agency that conducts business in California must notify California residents if there was, or is reasonably believed to have been, an "unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information [10]." To comply with the law's notice requirements, covered entities must disclose the breach to California residents whose data has been exposed "in the most expedient time possible and without unreasonable delay [11]." The notice may be provided either in a written or an electronic form that satisfies the federal E-Sign Act's requirements relating to electronic records [12]. If a covered entity can demonstrate that the cost of providing this notice would exceed \$250,000, or that the affected number of persons to be notified exceeds 500,000, it can give a substitute notice by: (1) notifying affected persons by email (regardless of whether the email notice satisfies the E-Sign Act's electronic records requirements); (2) making a conspicuous posting of the notice on the entity's website; and (3) notifying major statewide media [13]. In addition, some states require covered entities to notify state and/or federal consumer protection agencies of security breaches, or to notify consumer-reporting agencies when the security breach affects a specified threshold number of consumers [14].

Significantly, the majority of these laws impose notification obligations only in cases where unencrypted personal information is hacked or exposed [15]. In other words, as long as all of a covered entity's personal information is maintained in encrypted form, these laws generally will not be triggered.

### *Penalties*

The penalties imposed for violations of security breach notification laws vary widely from state to state. Some states allow a private right of action for those injured by a violation of the law [16]. Some states also allow state attorneys general to bring an action and recover penalties imposed under state fraud or consumer protection laws [17]. And a handful of states impose civil penalties that could subject covered entities to significant liability [18].

In addition, corporations, agencies, and institutions that are subject to security breach notification laws may face additional liability in actions brought under traditional negligence theories. Courts may interpret security breach notification laws as evidencing a general common law duty on all entities, whether covered by statute or not, to notify persons who have had their personally identifiable information exposed. Indeed, at least one court has awarded damages to victims of identity theft after the court found an organization negligent for failing to adequately safeguard personal information [19]. In that case, the court reasoned that the relationship between the organization - a labor union - and its members was such that the union had "a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information . . . [20]" Applying similar logic, it is possible that a court could conclude that a duty exists to notify persons who have had their personally identifiable information exposed, since failure to do so arguably could exacerbate the effects of a security breach and any subsequent identity theft.

Although the security breach notification laws already passed at the state level have created a patchwork of legal requirements with which companies, state agencies, and educational institutions must comply, legislative action in this field is far from complete. Security breach notification legislation was recently introduced in at least 12 other states [21], which has helped spur Congress to actively consider federal legislation that would preempt similar state laws and provide a uniform federal standard. In fact, during the 2005 Congressional session, at least nine bills contained a security breach notification component [22]. While none of these have yet passed into law, significant attention continues to be focused on this issue in both the

House [\[23\]](#) and the Senate [\[24\]](#), and it is possible that federal legislation will pass in 2006, although it remains unclear which approach to data security legislation will prevail.

## II. Implication for Colleges and Universities

As noted above, the majority of state security breach notification laws apply to both state agencies and businesses and, therefore, arguably encompass both public colleges and universities (as state agencies) and private colleges and universities (as businesses). Consequently, both public and private educational institutions that store personal information electronically should be aware of, and prepared to comply with, the requirements of applicable state security breach notification laws.

In determining which security breach notification laws may apply to an institution's activities, it is important to remember that these laws apply not just to entities that are operating within a state's borders, but also potentially to any out-of-state entities that store personal information about a state's residents. Although courts have not yet ruled on this question, the wording of some security breach notification laws suggests this to be the case. Some laws, such as California's security breach notification law, apply to entities simply "doing business" within the state. Some commentators have noted that courts have broadly construed similar language in other statutes as permitting enforcement against out-of-state entities [\[25\]](#). Nonetheless, the constitutionality of doing this remains unclear, and one could argue that the law impermissibly interferes with interstate commerce or conflicts with federal laws, such as the [Health Insurance Portability and Accountability Act \(HIPAA\)](#) or the [Gramm-Leach-Bliley Act \(GLBA\)](#) [\[26\]](#). To date, however, constitutional challenges to these laws have not yet been raised, and it is debatable whether any such challenge would prove successful in court.

Accordingly, counsel and administrators need to be cognizant of the laws of the states from which their students hail. If security breach notification legislation is enacted in a student's home state, arguably it will apply to any institution's storage of the student's personal information. Thus, institutions operating in states that have not yet passed security breach notification legislation may have an obligation to comply with such laws. However, depending on the nature of the security breach, an institution that is in the midst of a crisis may not be able to immediately evaluate its obligations to notify each individual student. As such, institutions would be well served to focus their efforts on developing a compliance plan that will satisfy all potentially applicable state laws in the event that a breach occurs. Specifically, college and university administrators should consider taking the following steps to ensure preparedness in the event of a security breach and avoid liability under security breach notification laws:

- **Appoint an employee to oversee compliance with applicable security breach notification laws.**

The employee overseeing security breaches should understand current security breach notification requirements and track all federal and state legislative developments. He or she also should communicate with and train employees about the requirements of applicable security breach notification laws. Inasmuch as 24 states – so far -- have enacted security breach notification laws, the most practical approach to comply with them may be to adhere to the strictest applicable state standard. This is particularly true for institutions that admit a high percentage of out-of-state students.

- **Minimize the use of unnecessary personal information.**

Colleges and universities often collect and retain personal information from employees and students. They should instead collect such information only when necessary and destroy it when it no longer is needed. Although institutions have commonly used student social security numbers to identify students in the past, they should minimize their use of such information since a breach generally will trigger a duty to notify [\[27\]](#).

- **Encrypt personal information where possible.**

State security breach notification laws generally do not apply to security breaches involving encrypted personal information. Likewise, most of the federal bills being considered in Congress apply only to unencrypted information. Therefore, by encrypting electronically stored personal information, colleges and universities can significantly reduce their chances of triggering compliance obligations under these laws. Encrypting personal information also may help to reduce an institution's risks based on other possible claims, such as common law negligence.

- **Conduct a security audit of the personal information contained on an institution's computer system**

Data containing personal information often can be found in multiple locations and on multiple computers across campus. Institutions should identify all locations in which personal information resides and evaluate the security that is in place to protect that information from being exposed [\[28\]](#). Once these tasks are completed, the institution should conduct an assessment of security mechanism vulnerabilities and implement appropriate measures to minimize the risk of breach [\[29\]](#). In this way, an institution can take preventive steps to lower its risk and make the necessary arrangements to notify the affected individuals if a breach actually occurs. As discussed below, such steps should be coordinated with the institution's information security program required under the [Federal Trade Commission \(FTC\) Safeguards Rule](#) (promulgated under the GLBA).

- **Establish a plan to comply with security breach notification legislation in the event of a breach**

Even if an institution augments its security for protecting personal information, some risk of a security breach will always remain. Therefore, colleges and universities should have a plan in place to comply with applicable security breach notification requirements [\[30\]](#). Some thoughts to consider are:

- Prepare to act with reasonable speed in the event of a breach to provide notice to all covered individuals.
  - Be sure to follow the institutional security breach notification plan if a breach actually occurs.
  - Prepare a template for an email notification that would be sent to students or employees who have their personal information exposed by a breach.
  - Create a template website with an FAQ about the incident and how to protect against identity theft (among other items).
  - Staff a hotline for a week or two after the incident to answer questions.
  - Notify all individuals whose personal information has been exposed instead of only the individuals who are legally required to be notified, as the failure to notify all affected individuals could result in a public relations disaster.
- **Consider how obligations under security breach notification laws relate to obligations under other privacy laws and regulations.**

In addition to the obligations that may be imposed by security breach notification laws, the legal requirements stemming from [HIPAA](#), the [GLBA](#), the [FTC Safeguards Rule](#), and the [Family Educational Rights and Privacy Act \(FERPA\)](#) may impose similar or overlapping obligations. For example, the [Safeguards Rule](#) requires financial institutions to develop, implement, and maintain an information security program that protects customers' financial information, including certain types of

information also covered by state security breach notification laws. The FTC has interpreted the [Safeguards Rule](#) to also include educational institutions. Accordingly, those colleges and universities that must comply [\[31\]](#) should coordinate their compliance efforts under the security breach notification laws with requirements imposed under these additional laws and regulations. Significantly, of the 24 state security breach notification laws that have been enacted, at least five exempt from their purview institutions that are covered by and are in compliance with the [GLBA](#) or [HIPAA \[32\]](#).

## CONCLUSION:

The recent wave of security breach notification laws has created a new set of obligations for colleges and universities, and both current and future legislation present difficult challenges for them. Although the laws in many states are markedly similar to each other, they can contain important differences. While legislation currently being considered by Congress may impose some relief by creating a national security breach notification standard, the precise scope remains to be seen.

Security breach notification laws may contain burdensome obligations for colleges and universities, but covered institutions can take steps now to reduce their compliance burdens later. Moreover, administrators should pay careful attention to the developments at both state and federal levels in security breach notification legislation to ensure that their institutions are prepared to comply with all applicable requirements in this quickly changing field.

## [FOOTNOTES](#)

## AUTHORS:

[Kenneth D. Salomon](#)  
[Peter C. Cassat](#)  
[Briana E. Thibeau](#)

## RESOURCES FOR COUNSEL:

### Case Law:

- *Bell et al. v. Michigan Council 25 of the AFSCME*, No. 246624, 2005 WL 356306 (Mich. Ct. App. Feb. 15, 2005).

### Statutes:

- [E-Sign Act, 17 U.S.C. § 7001\(c\) \(1\).](#)
- [Family Educational Rights and Privacy Act \(FERPA\), 20 U.S.C. § 1232g.](#)
- [Gramm-Leach-Bliley Act, Pub. L. No. 106-102 \(1999\).](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\), Pub. L. No. 104-191 \(1996\).](#)
- Security Breach Notification Laws by State:

<u>State</u>	<u>Citation</u>
Arkansas	<a href="#">Ark. Code Ann. § 4-110-101 et seq.</a>
California	<a href="#">Cal. Civ. Code §§ 1798.29, 1798.82.</a>
Connecticut	<a href="#">Conn. Gen. Stat. § 36a-701b.</a>
Delaware	<a href="#">Del. Code Ann. tit. 6, § 12B-101 et seq.</a>
Florida	<a href="#">Fla. Stat. § 817.5681.</a>
Georgia	<a href="#">Ga. Code § 10-1-910 et seq.</a>
Illinois	<a href="#">815 Ill. Comp. Stat. 530/1 et seq.</a>
Indiana	<a href="#">Ind. Code § 4-1-11-1 et seq;</a> <a href="#">Ind. Code § 24-4.9-1 et seq</a>
Louisiana	<a href="#">La. Rev. Stat. Ann. § 51:3071 et seq.</a>
Maine	<a href="#">Me. Rev. Stat. Ann. Tit. 10, § 1346 et seq.</a>
Minnesota	<a href="#">Minn. Stat. §§ 325E.61, 609.891.</a>
Montana	<a href="#">Mont. Code Ann. § 30-414-1701 et seq.</a>
Nevada	<a href="#">2005 Nev. Stat. 485.</a>
New Jersey	<a href="#">N.J. Stat. Ann § 56:8-161.</a>
New York	<a href="#">A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005).</a>
North Carolina	<a href="#">N.C. Gen. Stat. § 75-65.</a>
North Dakota	<a href="#">N.D. Cent. Code § 51-30-01 et seq.</a>
Ohio	<a href="#">Ohio Rev. Code Ann. § 1349.19.</a>
Pennsylvania	<a href="#">S.B. 712.</a>
Rhode Island	<a href="#">R.I. Gen. Laws § 11-49.2-1 et seq.</a>
Tennessee	<a href="#">2005 Tenn. Pub. Acts 473.</a>
Texas	<a href="#">Tex. Bus. &amp; Com Code Ann. § 48.001 et seq.</a>
Utah	<a href="#">S.B. 69, 2006 General Session (Utah 2006).</a>
Washington	<a href="#">Wash. Rev. Code § 19.255.010.</a>

### Regulations:

- [FTC Safeguards Rule, 16 CFR Part 314 \(2002\).](#)
- Gramm-Leach-Bliley
  - [Privacy of Consumer Financial Information, 16 CFR Part 313 \(2000\).](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\) – Privacy Rule, 45 CFR Parts 160 and 164 \(2002\).](#)

### Additional Resources:

- [Alston & Bird, Information Security Advisory \(June 2003\).](#)
- [Educause Data Incident Notification Toolkit](#)
- [Educause/Internet2 Security Task Force, Risk Assessment Framework.](#)
- [Electronic Privacy Information Center Bill Track](#)
- [Daniel L. Langin, Coming Clean in California: California Civil Code Section 1798 Requires Companies to](#)

[Notify Hacking Victims or Face Damages](#) (June 2004)

- [National Conference of State Legislatures, 2006 Breach of Information Legislation](#)
- Rodney Petersen, "[Security Breaches: Notification, Prevention and Treatment](#)," Educause Review July/August 2005
- Rodney Petersen, "[Data Incident Notification Templates](#)"
- University of Florida, Office of Information Technology, [UF Guidelines to Develop Applications for Secure Deployment \(2005\)](#).
- [University of Georgia Summary of State Security Breach Notification Laws](#).

### **Sample Institutional Policies:**

- [Georgetown University](#)
- [Miami University Incident Response Policy and Procedures \(2005\)](#)
- [Tufts University](#)
- [University of California, Berkeley](#)
- [University of Southern California](#)