PROSKAUER ROSE LLP®

Client Alert

A report
for clients
and friends
of the Firm

January 2007

Updated January 2007: Michigan and Washington, D.C. Become the Latest To Pass Security Breach Notification Laws: Businesses Continue To Struggle with Various and Sometimes Conflicting Regulations

News of security breaches at global corporations and large universities continued to occupy headlines throughout 2006. Meanwhile, state legislatures throughout the country continued to enact data breach legislation.[1] In total, thirty-five states, the District of Columbia and New York City now have adapted California's first-in-the-nation security breach notification legislation to suit individual jurisdictional needs. Arizona, Hawaii, Maine, New Hampshire, Utah and Vermont each have laws taking effect at either the end of December 2006 or during January 2007.

Although the lack of a universal standard for the protection of private data complicates compliance efforts, it is important for any entity holding such data to understand the various state law requirements governing the handling of the information and notification requirements. This is fast becoming an urgent business imperative as the Federal Trade Commission ("FTC") and state regulators increasingly are demonstrating a willingness to bring enforcement actions against companies that do not adequately protect data. For example, in addition to the FTC's well-publicized enforcement actions against companies (such as BJ's Wholesale Club; DSW, Inc.; Cardsystems Solutions; and Guidance Software), based on failure to engage in reasonable security practices, states are becoming more active as well. Recently, the Massachusetts Attorney General (Massachusetts is not among the states with a data breach notification law) reached a settlement with Ameriprise over a lost laptop; the North Dakota Insurance Commissioner brought an action against Humana because of breach incidents and the Oregon Attorney General settled a case with Providence Health System because of the theft of unencrypted backup tapes and discs containing personal information.

Businesses also have to be concerned with the class action bar. Many courts have dismissed negligence and invasion of privacy cases because an increased risk of identity theft without actual harm presents an insufficient basis for a claim. A new California class action lawsuit arising from the theft of a company laptop, *Mannacio v. General Electric Co.*, Cal. Super. Ct., CV-065227 (Dec. 5, 2006), will be closely followed by businesses. Among other claims, *Mannacio* alleges that GE's notices, which conformed with California law, did not enable affected individuals to protect themselves from improper use of the stolen information.

This Client Alert provides a broad overview of existing security breach notification legislation, including new

[1] *See* Proskauer Rose LLP Client Alert dated August 2006, containing a summary of data breach notification laws that had been enacted as of its release. Updated August 2006: States Continue To Pass Security Breach Notification Laws: Businesses Must Comply with Various and Sometimes Conflicting Regulations

laws from the District of Columbia and Michigan, the most recent additions to what one lobbyist called "a state law game of whack-a-mole." Oklahoma's statute is not discussed in detail because it applies only to state agencies.

The California Framework

The Security Breach Information Act, CAL. CIV. CODE § 1798.82 *et seq.*, was the first law passed in the United States that required companies to notify customers regarding a breach of their personal information. The California law, and most state security breach notification schemes, require notification to individuals if their computerized personal information "was, or is reasonably believed to have been, acquired by an unauthorized person."[2]

Personal Information, in California and elsewhere, *is defined as the first name or initial and last name of an individual, with one or more of the following: 1) Social Security Number, 2) driver's license number, 3) credit card or debit card number, or 4) a financial account number with information such as PINs, passwords or authorization codes that could gain access to the account.*

Subsequent sections of the California Code provide for exemptions from the disclosure requirements. The first exemption is for personal information held in encrypted form. The second is for maintenance of a present interest in a criminal investigation by law enforcement. Other states have developed exemptions for unauthorized access to information made available to the public by government agencies or for entities that are already regulated under federal privacy laws (*e.g.*, FERPA, GLBA, or HIPAA).

California requires notification in the "most expedient time possible and without unreasonable delay," either in writing or by e-mail. If a company can show: 1) the cost of notification will exceed $250,000; 2) the number of people affected is greater than 500,000; or 3) the contact information is unknown for affected individuals, then notice may be effected through statewide media outlets.

Common Departures from California's Framework

Examples of provisions different from the basic framework:

- Personal information can include: biometric data; codes or numbers necessary to obtain state identification cards; digital signatures; DNA profiles; employee identification numbers; fingerprints; information likely to lead to identity theft including mother's maiden name; or medical records.

- Notification is necessary to consumer reporting agencies in the event of a security breach; the threshold number of people affected in other states ranges from 500 in Minnesota to 10,000 in Georgia and Texas.

- A private right of action for affected individuals against the entity which suffered the personal data security breach, with fines ranging from $10,000 per breach in Arizona to potential damages of $500,000 in Florida, for failing to notify those affected by a breach (some states even allow for treble damages).

- A requirement of preventative security measures, including reasonable security policies for maintenance and disposal of personally identifying information in Arkansas, Montana, and Nevada.

- North Carolina requires the entity to provide contact information (for further assistance) to the party being notified, if available, along with a detailed description of the events allowing the breach to occur.

Notable Provisions from the Remaining Thirty-four State Laws and D.C.

Below is a review of the key provisions that impact security breach notification procedures in each of the jurisdictions that passed legislation regulating this area. These summaries discuss each jurisdiction's defining, but not exhaustive, differences with the basic California framework.

Arizona Revised Statutes Annotated § 44-7501 (effective December 31, 2006)

Arizona allows for civil damages of up to $10,000 per breach for willful and knowing violations. Statute applies to any person conducting business in the state.[3]

Arkansas Code Annotated § 4-110-101 *et seq.* (effective March 31, 2005)

Arkansas includes individually identifiable medical records in its definition of personal information.[4] The Arkansas law requires businesses to "implement and maintain reasonable security procedures and practices . . . to protect the personal information from unauthorized access, destruction, use, modification or disclosure."[5]

---

[2] CAL. CIV. CODE § 1798.82 *et seq.*

[3] ARIZ. REV. STAT. § 44-7501(H).

[4] ARK. CODE ANN. § 4-110-103(5).

[5] ARK. CODE ANN. § 4-110-104(b).

Colorado Revised Statutes § 6-1-716 (effective September 1, 2006)

Colorado requires standard notice unless more than 250,000 residents are affected, or costs exceed $250,000.[6] If more than 1,000 residents are affected, and the entity is subject to regulation under Title V of the GLBA, then notification to consumer reporting agencies is per GLBA requirements.[7]

Connecticut General Statutes Annotated § 36a-701b (effective January 1, 2006)

A business may forego notice to Connecticut residents if law enforcement determines that there is no reasonable likelihood of harm to consumers.[8] Notification by telephone is permissible, and substitute notice is allowed if costs of notification exceed $250,000 or affected individuals exceed 500,000 residents.[9]

Delaware Code Annotated title 12B, § 101 *et seq.* (effective June 28, 2005)

Delaware includes individually identifiable medical information in its definition of personal information.[10] The statute contains a private right of action allowing a harmed individual to recover treble damages and attorney's fees.[11]

District of Columbia B16-810 (effective July 1, 2007, subject to approval by Congress)

The District of Columbia legislation generally parallels the California framework with two noteworthy differences. First, a breach means merely "a **likelihood** that there has been unauthorized acquisition of computerized data" that compromises personal information.[12] And second, the definition of "personal information" includes an individual's first name or initial and last name in combination with, among other items, "account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords."[13]

Florida Statutes Annotated § 817.5681 (effective July 1, 2005)

In Florida, notification generally must be performed within forty-five days of determining a breach.[14] If an entity fails to inform the victims of a security breach, they can be subject to fines of up to $1,000 per day for the first thirty days, and $50,000 fines for each subsequent thirty-day period.[15] If notification is not made within 180 days, the entity is subject to an administrative fine of up to $500,000.[16] If more than 1,000 residents are affected, the entity suffering the breach must notify credit reporting agencies.[17] Notice by e-mail is appropriate if the affected party has consented to such notice, and the notice is done in accordance with 15 U.S.C. § 7001.[18]

Georgia Code Annotated § 10-1-911 (effective May 5, 2005)

Georgia's law applies only to computerized data held by consumer "information brokers," who store and transmit personal information to third parties for monetary fees.[19] Georgia's definition of personal information is standard; however, if personal information is obtained without a person's name and would be sufficient to perform identity theft, then notice is necessary.[20]

---

6 Colo. Rev. Stat. § 6-1-716(1)(c).

7 Colo. Rev. Stat. § 6-1-716(2)(d).

8 Conn. Gen. Stat. Ann. § 36a-701(b)(b).

9 Conn. Gen. Stat. Ann. § 36a-701(b)(e).

10 Del. Code Ann. tit. 12B, § 101(2).

11 Del. Code Ann. tit. 12B, § 104(a).

12 District of Columbia B16-810 (to be codified at D.C. Code § 28-3851(1)).

13 District of Columbia B16-810 (to be codified at D.C. Code § 28-3851(3)(A)).

14 Fla. Stat. Ann. § 817.5681-1(a).

15 Fla. Stat. Ann. § 817.5681-1(b).

16 Fla. Stat. Ann. § 817.5681-1(b).

17 Fla. Stat. Ann. § 817.5681-12.

18 Fla. Stat. Ann. § 817.5681-6(b).

19 Ga. Code Ann. § 10-1-911(2).

20 Ga. Code Ann. § 10-1-911(5)(E).

Hawaii SB 2290, Act 135 (effective January 1, 2007)

In addition to the standard entities covered by the legislation, Hawaii specifically includes those in the business of records destruction.[21] Hawaii identification and driver's license numbers are considered personal information.[22] Risk of harm to a person must be material before notification is required.[23]

Idaho Code § 28-51-104 *et seq.* (effective July 1, 2006)

Idaho requires notification when misuse of personal information is likely.[24] Substitute notice is appropriate if costs exceed $25,000, more than 50,000 residents are affected, or insufficient contact information is available.[25] If an entity intentionally fails to notify those affected by a breach, they may be fined up to $25,000 per breach.[26]

815 Illinois Compiled Statutes Annotated 530/5 (effective January 1, 2006)

Entities responsible for protecting personal information are expanded to include "government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information."[27]

Indiana Code Annotated § 4-1-11-1 *et seq.* (effective July 1, 2006)

Under Indiana's law, if a laptop computer is stolen but password-protected, notice is not necessary.[28]

Kansas S.B. 196 (effective upon publication in state statute book)

Kansas allows substitute notice if more than 5,000 residents are affected, notification costs exceed $100,000, or the entity does not have sufficient information to contact those who had their personal information breached.[29] An entity must notify consumer reporting agencies of the timing, content, and distribution of the notices when more than 1,000 residents are affected.[30]

Louisiana Revised Statutes Annotated § 51:3071 *et seq.* (effective January 1, 2006)

Louisiana does not require notification to customers if after a reasonable investigation the entity suffering the breach determines there is no reasonable likelihood of harm to customers.[31] Louisiana states a private cause of action if actual damages result from the breach.[32]

Maine Revised Statute Annotated title 10, § 1346 et seq. (effective January 31, 2006)

Maine's security breach notification law applies to all persons (not just information brokers) as of January 31, 2007. Notification is not required unless misuse of the personal information has occurred or is reasonably possible.[33] If more than 1,000 persons are affected at one time, the details of the breach must be reported to consumer reporting agencies and state regulators.[34] The Maine statute provides for penalties of not more than $500 per violation, up to a maximum of $2,500 per day the person fails to provide notice as required.[35]

Michigan SB 309 (effective July 2, 2007)

Michigan's law differs from the California standard through its risk of harm threshold that limits when notification is required. In Michigan, notice to consumers is required only if substantial loss or identity theft is likely to result from a breach.[36] The Michigan law also incorporates a data disposal provision that requires covered entities to completely destroy records containing personal information when such records are no longer needed. Destroying records may include "shredding, erasing, or otherwise modifying the data so that

---

[21] Hawaii S.B. 2290, Act 135, § 2, subject to final verification.

[22] Hawaii S.B. 2290, Act 135, § 2, subject to final verification.

[23] Hawaii S.B. 2290, Act 135, § 2, subject to final verification.

[24] Idaho Code § 28-51-105(1).

[25] Idaho Code § 28-51-104(4).

[26] Idaho Code § 28-51-107.

[27] 815 Ill. Comp. Stat. Ann. 530/5.

[28] Ind. Code Ann. § 4-1-11-2(b)(2).

[29] Kansas S.B. 196, § 3(c)(3) (tentatively codified at Kan. Stat. Ann. § 50-7a01-02).

[30] Kansas S.B. 196, § 4(f) (tentatively codified at Kan. Stat. Ann. § 50-7a01-02).

[31] La. Rev. Stat. Ann. § 51:3074(G).

[32] La. Rev. Stat. Ann. § 51:3075.

[33] Me. Rev. Stat. Ann. tit. 10, § 1348(1)(B).

[34] Me. Rev. Stat. Ann. tit. 10, § 1348(4), (5).

[35] Me. Rev. Stat. Ann. tit. 10, § 1349(2).

[36] Michigan S.B. 309 (to be codified at Mich. Comp. Laws § 445.72(1)).

they cannot be read, deciphered, or reconstructed through generally available means."[37] Entities that fail to properly destroy records may be fined up to $250.00 per violation and be subject to other civil penalties.

Minnesota Statutes Annotated § 325E.61 (effective January 1, 2006)

Minnesota mandates notification to consumer reporting agencies within 48 hours if notice is required under the statute to more than 500 consumers.[38]

Montana Code Annotated § 30-14-1701 (effective March 1, 2006)

Montana's legislation closely follows California's, with substitute notice appropriate if the cost of providing notice exceeds $250,000 or if more than 500,000 residents are affected.[39]

Nebraska Revised Statutes § 87-801 *et seq.* (effective July 14, 2006)

Nebraska law allows the Attorney General to issue subpoenas and seek to recover damages for Nebraska residents injured by violations.[40] Substitute notice is allowed if: 1) costs of notification exceed $75,000; 2) more than 100,000 Nebraska residents are affected; or 3) entity required to provide notice has fewer than ten employees and cost will exceed $10,000.[41] Personal information includes unique biometric data such as a fingerprint, voiceprint, or retina or iris image.[42] Entities following procedures of its own security plan, if timing requirements are consistent with the act, are considered in compliance.[43]

Nevada Revised Statutes Annotated § 603A.010 *et seq.* (Effective January 1, 2006; Mandatory encryption by October 1, 2008).

Nevada was the first state to require encryption for all transmissions of personal information outside secure networks; however, this provision does not become effective until October 1, 2008.[44] Nevada's law provides for punitive damages, where applicable, under the private rights of action.[45]

New Hampshire Revised Statutes Annotated § 359-C:1 *et seq.* (effective January 1, 2007)

New Hampshire allows for substitute notification if the cost is greater than $5,000 or more than 1,000 residents are affected.[46] Damages are at least doubled, and may be tripled, for willful or knowing breaches. And damages can include reasonable attorney's fees.[47] Notification to consumer reporting agencies is required if more than 1,000 people are affected.[48]

New Jersey Statutes Annotated § 56:8-163 (effective January 1, 2006)

New Jersey expands the definition of personal information to include "dissociated data that, if linked, would constitute personal information . . . if the means to link the dissociated data were accessed in connection with access to the dissociated data."[49] All security breaches must be reported to the State Police before notifying those residents affected by the breach.[50]

New York General Business Law § 899-aa (effective December 7, 2005)

New York law mandates notification of security breaches to the Attorney General and relevant state regulatory offices, in addition to individual consumer notification.[51] While the

---

[37] Michigan S.B. 309 (to be codified at MICH. COMP. LAWS § 445.72a(4)).

[38] MINN. STAT. § 325E.61 subd. 2.

[39] MONT. CODE ANN. § 30-14-1704(5)(a)(iv).

[40] NEB. REV. STAT. § 87-806.

[41] NEB. REV. STAT. § 87-802(4).

[42] NEB. REV. STAT. § 87-802(5).

[43] NEB. REV. STAT. § 87-804(1).

[44] NEV. REV. STAT. ANN. § 597.970.

[45] NEV. REV. STAT. ANN. § 603A.900.

[46] N.H. REV. STAT. ANN. § 359-C:20(III).

[47] N.H. REV. STAT. ANN. § 359-C:21.

[48] N.H. REV. STAT. ANN. § 359-C:20(VI).

[49] N.J. STAT. ANN. § 56:8-161.

[50] N.J. STAT. ANN. § 56:8-163(c)(1).

[51] N.Y. GEN. BUS. LAW § 899-aa(6)(a).

legislation does not provide a private right of action, the Attorney General may sue on behalf of the affected parties for actual and consequential damages. For knowing or reckless violations, an entity may be fined the greater of $5,000 or $10 per failed notification, with a maximum fine of $150,000 per occurrence.[52]

The legislation allows for notice by telephone, if logged. Consumers may consent to electronic notification. But consent cannot be a condition of establishing a business relationship or engaging in a transaction. The notification to individuals must include contact information for more information regarding the data security breach, full disclosure of the extent of the data security breach, and categories of compromised personal information.

The law explicitly preempts local and city government laws that are inconsistent with, or more restrictive than, the state law. So significant portions of the New York City ordinances, signed by Mayor Bloomberg in September 2005, which required businesses licensed by the Department of Consumer Affairs to notify consumers in the event of the breach, and required destruction of records containing personal information, may be preempted.[53]

North Carolina General Statutes Annotated § 75-60 *et seq.* (effective December 1, 2005)

North Carolina's law requires notification when a breach of any record occurs, not just breaches of computerized data. A "record" is any "material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics."[54] The state also requires specific content in notices of a breach including: 1) a description of the incident in general terms, 2) the type of personal information that was the subject of the breach, 3) the general acts of the business to protect the personal information from further unauthorized access, 4) a telephone number that the person may call for further information and assistance, and 5) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.[55] If a business is required to notify more than 1,000 customers at one time, the business also must notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies of the timing, distribution, and content of the notice.[56]

North Dakota Century Code § 51-30-01 *et seq.* (effective June 1, 2005)

The category of personal information is expanded to include date of birth, mother's maiden name, employee identification numbers, an employer's name or address, digital or electronic signatures or an individual's birth, death, or marriage certificate.[57]

Ohio Revised Code Annotated § 1349.19 (effective Feb. 17, 2006)

In Ohio, a business entity must notify affected individuals of a security breach of their personal information if the breach is believed to "cause a material risk of identity theft or other fraud."[58] The notification must be made within 45 days following discovery of the security breach.[59] If a business is required to notify more than 1,000 customers at one time, the business also must notify all consumer reporting agencies.[60] Violators may be fined up to $1,000 per day for the first 60 days, up to $5,000 per day for the next 30 days and up to $10,000 per day after 90 days.[61]

Oklahoma Statutes title 74, § 3113.1 (effective June 8, 2006)

The Oklahoma statute applies only to state agencies.

73 Pennsylvania Consolidated Statutes § 2301 *et seq.* (effective June 22, 2006)

Under Pennsylvania law, notification is necessary if the breach of encrypted data involves a person with access to the encryption key.[62] If more than 175,000 residents are affected or the cost of notice exceeds $100,000, substitute notice is

---

[52] N.Y. Gen. Bus. Law § 899-aa(6).

[53] N.Y. Gen. Bus. Law § 899-aa(9); New York City Int. Nos. 139-A, 140-A, 141-A (2004).

[54] N.C. Gen. Stat. Ann. § 75-61(12).

[55] N.C. Gen. Stat. Ann. § 75-65(d).

[56] N.C. Gen. Stat. Ann. § 75-65(f).

[57] N.D. Cent. Code § 51-30-01(2)(a).

[58] Ohio Rev. Code Ann. § 1349.19(A)(1)(a), (B)(1).

[59] Ohio Rev. Code Ann. § 1349.19(B)(2).

[60] Ohio Rev. Code Ann. § 1349.19(G).

[61] Ohio Rev. Code Ann. § 1349.192(A).

[62] 73 PA. Cons. Stat. § 2303(b).

allowed.[63] The Attorney General may bring an action against violators of this act, as violations are deemed "unfair or deceptive acts or practices" in violation of Pennsylvania's consumer protection statutes.[64]

Rhode Island General Laws § 11-49.2 et seq. (effective July 10, 2005)

The Rhode Island legislation only requires notification if the security breach "poses a significant risk of identity theft."[65] And the threshold for substitute notice is lower than most other states. Such notice is allowed when costs will exceed $25,000 or the number of affected residents exceeds 50,000.[66] The Rhode Island law provides for civil penalties when notice is not given, up to $100 per occurrence, capped at $25,000.[67]

Tennessee Code Annotated § 47-18-2101 *et seq.* (effective July 1, 2005)

Tennessee allows a private right of action for damages or injunctive relief for injuries resulting from a violation of the security breach notification statute.[68]

Texas Business and Commerce Code § 48.103 (effective September 1, 2005)

Texas requires notification to national consumer reporting agencies if more than 10,000 Texas residents are affected by a security breach.[69] Texas requires the notice to consumer reporting agencies include an explanation of the timing, distribution, and content of the notification provided to individuals affected by the security breach.

Utah Code Annotated § 13-42-101 *et seq.* (effective January 1, 2007)

Utah allows for e-mail notification if that is the primary means of communication between the entity and the injured party.[70] Fines are capped at $2,500 for events relating to one consumer and $100,000 in the aggregate.[71]

Vermont Statutes Annotated title 9, § 2430 *et seq.* (effective January 1, 2007)

Vermont allows telephonic notice, as long as it is not a prerecorded message, and substitute notice if costs would exceed $5,000 or more than 5,000 state residents are subject to notification.[72] Notice must include a description of the incident in general terms, the type of personal information subject to the breach, the actions taken by the entity to protect personal information in the future, a telephone number for further information, and advice on monitoring credit reports to detect possible misuse.[73] Civil remedies are available to address violations of the Vermont law, and the Attorney General, State's Attorney, and courts also may dissolve business licenses within the state and revoke the certificate of authority to foreign corporations in some instances.[74] The entity must notify all consumer reporting agencies of the breach if more than 1,000 residents are affected.[75]

Washington Revised Code Annotated § 19.255.010 (effective July 24, 2005)

Washington creates a private right of action for civil damages or injunctive relief against entities that violate its law requiring notification of security breaches relating to personal information.[76] The law contains a safe harbor provision under which an agency "shall not be required to disclose a technical breach of the security system that does

---

[63] 73 PA. CONS. STAT. § 2302.

[64] 73 PA. CONS. STAT. § 2308.

[65] R.I. GEN. LAWS § 11-49.2-3(a).

[66] R.I. GEN. LAWS § 11-49.2-5(d)(3).

[67] R.I. GEN. LAWS § 11-49.2-6.

[68] TENN. CODE ANN. § 47-1-101.

[69] TEX. BUS. & COM. CODE § 48.103(h).

[70] UTAH CODE ANN. § 13-42-202(5)(a).

[71] UTAH CODE ANN. § 13-42-301(3).

[72] VT. STAT. ANN. tit. 9, § 2435.

[73] VT. STAT. ANN. tit. 9, § 2435(b)(5).

[74] VT. STAT. ANN. tit. 9, § 2435(f)(1).

[75] VT. STAT. ANN. tit. 9, § 2435(c).

[76] WASH. REV. CODE ANN. § 19.255.010(10).

not seem reasonably likely to subject customers to a risk of criminal activity."[77]

Wisconsin Statutes Annotated § 895.507 (effective March 31, 2006)

Wisconsin broadens the definition of personal information to include a driver's license or state ID number, DNA profiles, and unique biometric data.[78] Notification to consumer reporting agencies is necessary if more than 1,000 individuals are affected.[79] Entities must notify affected parties within 45 days of discovering the breach, informing those notified of the personal information that was acquired.[80]

Federal Legislation

Recognizing the difficulties imposed on businesses by varying, and sometimes conflicting, state laws, federal legislators from both parties introduced several data security bills in the 109th Congress.[81] But only one such bill, with very narrow application, became law. The Veterans Benefits, Health Care, and Information Technology Act of 2006 requires the Veterans' Administration to adopt rules for notifying veterans in the case of breach of their personal data.

Early indications suggest the 110th Congress will be active on privacy issues and that, as in the last Congress, multiple data breach notification bills will be introduced. Senator Feinstein (D-Cal.) has already introduced one data security breach notification bill. Some of those bills likely will mirror legislation introduced in the last Congress. Although it is too early to predict with any accuracy, we believe it is likely that a data breach notification law may finally pass Congress sometime this year. Businesses would welcome such legislation if it includes a preemption provision that would help to eliminate the compliance difficulties with state legislation, although another issue, the notification trigger, will be an important one as well.

Conclusion

Federal legislation preempting state security breach notification law would make the obligations of businesses clearer, in the event of a breach. Unfortunately, until such laws are passed, entities must comply with the various, and sometimes contradictory, state laws. Given the complex nature of the state statutory requirements, it is imperative that businesses address the specific concerns affecting their use of personal data, create a plan for the collection and handling of these data, and train their employees to follow this plan. In the event of a personal data security breach, following an entity-specific plan allows for the most efficient response and can significantly limit liability. Entity-specific assessments are necessary to create the most effective data security and privacy plans.

Christopher Wolf
202.416.6818 – cwolf@proskauer.com

Scott P. Cooper
310.284.5669 – scooper@proskauer.com

Tanya L. Forsheit
310.284.4508 – tforsheit@proskauer.com

Timothy P. Tobin
202.416.6870 – ttobin@proskauer.com

[77] WASH. REV. CODE ANN. § 19.255.010(10)(d).

[78] WIS. STAT. ANN. § 895.507(1)(b).

[79] WIS. STAT. ANN. § 895.507(2)(b).

[80] WIS. STAT. ANN. § 895.507(3)(a), (c).

[81] *See* the Federal Legislation section of the Proskauer Rose LLP Client Alert dated August 2006, containing a summary of prominent federal data breach notification legislation. Updated August 2006: States Continue To Pass Security Breach Notification Laws: Businesses Must Comply with Various and Sometimes Conflicting Regulations