TRENDS IN STATE SECURITY AND PRIVACY LAWS AND REGULATIONS

Stephen S. Wu
Cooke Kobrick & Wu LLP

TABLE OF CONTENTS

Trends in State Security and Privacy Laws and Regulations

Dated: March 26, 2010

I. Introduction

Since our update last year, data breaches continue to be an everyday occurrence. At the same time, the consequences of data breach liability are becoming apparent. Merchants sued for data breaches are paying staggering amounts to investigate and settle the cases against them. The TJX Companies set aside $107 million to cover the litigation against it and regulatory actions. Heartland Systems set aside $73.3 million for breach expenses in 2009.

Although TJX and Heartland are huge cases, other companies discover (or perhaps fail to discover) smaller security breaches every day. For instance, former employees departing companies commonly misappropriate trade secrets as they leave their employment. Security breaches, both large and small, cost companies real money every day in investigation and remediation costs, litigation costs, customer anger, reputation losses, stock price declines, loss of competitiveness, and ultimately loss of revenue.

At the federal level, the House of Representatives passed H.R. 2221, the Data Accountability and Trust Act, calling for companies with sensitive data to implement an information security program and provide notification in the event of a security breach. Regardless of what happens to H.R. 2221, the states continue to experiment with data security and privacy laws. Although federal legislation will preempt inconsistent state legislation, the states have some room for legislation and are trying to fill in perceived gaps in security and protections offered by law to their citizens.

Part II of this paper covers the major developments in state security and privacy legislation and regulations since June 2009,

the date of our last Institute on Privacy and Data Security Law.[1] I cover these developments on a state-by-state basis. Part III discusses the prospects for uniform legislation in the area of data protection and breach notification. Finally, Part IV provides more general thoughts and conclusions concerning trends and possible future areas of legislation.

II. Update on State Information Security and Privacy Laws; Legislative Trends

A. Alaska Personal Information Protection Act Goes Into Effect

On June 19, 2008, the Alaska Personal Information Protection Act became law. On July 1, 2009, the law went into effect. The Alaska Act, which is similar to California's SB 1386,[2] contains a number of articles, including ones on breach notification,[3] credit report and credit score security freeze,[4] protection of social security numbers,[5] secure disposal of records,[6] and truncation of

---

[1] I did not cover in this document all of the many relevant bills that have not yet passed. Instead, I reported only the bills I thought were most significant. Also, I did not include coverage of laws that simply enhance the scope or penalty of cybercrime legislation prohibiting certain activities of individuals. I did, however, include cybercrime laws that will require the attention of businesses.

[2] Cal. Civil. Code §§ 1798.29, 1798.82.

[3] Alaska Stat. §§ 45.48.010-45.48.090.

[4] *Id.* §§ 45.48.100-45.48.290.

[5] *Id.* §§ 45.48.400-45.48.480.

[6] *Id.* §§ 45.48.500-45.48.590.

printed card information.[7] I covered the Alaksa Act in detail in last year's program materials, and I refer the reader to last year's materials for more information.

B. Developments in California

Last year, California enacted two significant new laws in the area of privacy and security. First, California addressed the disposal of personal information by enacting AB 1094, which provides a safe harbor for storage companies or landlords when they end up with others' records containing personal information. Second, California beefed up its anti-paparazzi privacy law with AB 524 by addressing what happens when images or recordings are sold, transmitted, published or broadcast. Governor Schwarzenegger, however, vetoed legislation, SB 20, to enhance the state's breach notification law to require notification to the California Attorney General, in addition to the parties that must be notified under existing law. He had vetoed the legislation once before in 2008. The bill's author introduced the legislation for a third time on February 18, 2010.

1. AB 1094 - Data Disposal Law

Under old law, businesses had an obligation to "destroy" or "arrange for the destruction" of records containg "personal information" that it will no longer retain. "Personal information" is defined in Civil Code § 1798.80(e), and includes more categories of information than the phrase "personal information" under California's breach notification law. AB 1094 changes the law to require businesses to "dispose" or "arrange for the disposal" of such records. The change from "destroy" to "dispose" may have no practical effect because the means of compliance, shredding, erasing, or making the information unreadable or undecipherable, remain the same under the new law. Cal. Civil Code § 1798.81.

---

[7] *Id.* § 45.48.750.

AB 1094 also addresses a situation that may have become all too common with the economic downturn: a tenant leaves commercial space or vacates a storage facility, and the landlord or the storage company ends up with records containing personal information. Under old law, landlords had an obligation to notify tenants and any other person the landlord reasonably believes to be the owner about property remaining in the premises after the tenant has left. Cal. Civil Code §§ 1983(a), 1993.03(a). AB 1094 adds language stating that if property left on the premises consists of records, the tenant is the presumed owner of the records. "Records" has a broad definition that encompass electronic information.

Finally, AB 1094 adds a safe harbor intended for landlords and storage companies left holding records containing personal information after tenants vacate the premises. The bill adds language stating, "A cause of action shall not lie against a business for disposing of abandoned records containing personal information by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means." Cal. Civil Code § 1984(f)(1). While the language is broad enough to cover anyone left holding abandoned records, the legislature declared its intent to create a safe harbor for storage companies and commercial landlords. *Id.* § 1984(f)(2).

2. AB 524 – Anti-Paparazzi Law Changes

California has an anti-paparazzi law that creates liability for the physical or constructive invasion of privacy for trespass and for the recording activities associated with paparazzi. Cal. Civil Code § 1708.8. Under old law, the "transmission, publication, broadcast, sale, offer for sale, or other use" of video, sound, or physical impressions taken in violation of this law is not itself a violation. AB 524 creates an exception to this provision.

Under AB 524, a person can violate the anti-paparzzi law if the person transmits, publishes, broadcasts, sells, or offers a recording knowing that it was taken or captured in violation of the law and provides compensation for the rights to the recording. Cal. Civil

Code § 1708.8(f)(1). Such liability, however, attaches only to the first transaction following the taking or capturing of the recording. *Id.* AB 524 also adds provisions for civil fines for violations and inducing violations in an amount from $5,000 to $50,000, which county or city attorneys can seek. *Id.* § 1708.8(d), (e).

3. Proposed A.G. Reporting Requirement for Data Breaches

California State Senator Joe Simitian, the author of the original SB 1386 breach notification law in California, twice introduced legislation to augment the law by requring businesses or state agencies providing notice of breaches to also notify the State's Attorney General if the breach involved the personal information of more than 500 state residents. In both cases, Governor Schwarzenegger vetoed the legislation. The 2009 legislation appeared in S.B. 20.

This February 18, Sen. Simitian reintroduced the legislation as S.B. 1166 – for the third time. The Senate Judiciary Committee held a hearing on the bill on March 23, 2010. It remains to be seen whether the third time is a charm. This provision appears in other states' laws, but the State's funding crisis may underlie the Governor's reluctance to require the Attorney General's office to handle more paperwork.

C. Kentucky Breach Notification Bill

Kentucky is one of five states that does not have a breach notifcation law. The Kentucky House, however, took up a bill introduced on March 2, 2010 to require breach notification by businesses (but not state agencies). H.B. 581.

"Personal information" whose compromise would trigger notification includes the usual name[8] in combination with a

[8] Breach notification laws typically cover a name in the form of a first and last name, or a first initial and last name together.

driver's license number, Social Security number, or code in combination with an account number, like California's SB 1386. But it also includes credit and debit card numbers alone, or medical information, in combination with a name. No notification is necessary if the business establishes that misuse of the information "is not reasonably possible" after conducting a reasonable and prompt investigation.

H.B. 581 also contains restrictions on the use of Social Security numbers. The bill would prohibit disclosure of SSNs to the public, use of SSNs on cards, use of SSNs as a user name on a website without requiring a password or authentication device, printing SSNs on correspondence, or disclosing SSNs to third parties lacking a legitimate purpose for obtaining SSNs.

D. Maine Developments

Maine amended its breach notification law in May 2009, and the changes took effect on June 17 of that year. Among the amendments were:

- A clarification that data subject to a "breach" means "computerized data that includes 'personal information.'" Maine Rev. Stat. § 1347(1).
- It is a violation "for an unauthorized person to release or use an individual's personal information acquired through a security breach." *Id.* § 1347-A.
- Notification may be delayed while the agency determines that notification will compromise the investigation. *Id.* § 1348(3).
- The deadline for breach notification following a delay caused by a law enforcement agency's criminal investigation is 7 business days after the agency determines that the notification will *not* compromise the investigation. *Id.*

Maine is also in the process of considering legislation that would repeal Maine's privacy law that limits the collection and use of personal information of minors. L.D. 1677. The effect of the new legislation would be to limit the requirement of verifiable parental

consent to collection of information for pharmaceutical marketing and would limit the scope of the law to cover minors from 13 to 17 years og age.

Under the existing law, enacted in July 2009 as L.D. 1883 and entitled "An Act To Prevent Predatory Marketing Practices against Minors," "verifiable parental consent" is required to collect personal information from any minors for any marketing purposes in any industry, or to use or transfer such information. Me. Rev. Stat. Ann. tit. 10, § 9552. A business may not use personal or health-related information for promoting products or services to the minor. *Id.* § 9553.

L.D. 1883 created considerable controversy and arguably conflicted with the federal Children's Online Privacy Protection Act, which applies to children younger than 13. L.D. 1677 appears to limit the conflict, because it applies to children from 13 to 17 years of age. Others argued that L.D. 1883 is unconstitutional. The State's attorney general agreed not to enforce the law.

E. Massachusetts Finalizes Data Protection Regulations

One of the key developments this year was the finalization of the Massachusetts data protection regulations. The Massachusetts Office of Consumer Affairs and Business Regulation issued regulations[9] on September 22, 2008 to implement the Massachusetts security breach and data destruction law.[10] After various iterations, and delays in implementation, the Office of Consumer Affairs and Business Regulation issued final regulations on November 4, 2009 to take effect on March 1, 2010.

Last year's program materials for this Institute described the Massachusetts regulations and statute in detail, and I refer the reader to those materials. Nonetheless, suffice it to say that the

---

[9] 201 CMR 17.00 *et seq.*

[10] Mass. Gen. Laws Chl. 93H, § 2(a).

long process of finalization is now done, and the Massachusetts regulations are now effect. The regulations require persons who own or license personal information about Massachusetts residents to develop, implement, and maintain a comprehensive written information security program to protect that personal information.

> Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

201 CMR 17.03.

The regulations set forth a list of information security controls that covered persons must implement in their information security programs. Examples include access control, encryption of personal information either transmitted or stored on portable devices, firewall protection, malware protection, and personnel training. 201 CMR 17.04.

So far, no other states have adopted Massachusetts-style laws requiring the implementation of a list of security controls. As mentioned in the next section, Michigan is basing its new data protection bill on Massachusetts' regulations, with a somewhat different approach, although it is not yet the law in Michigan. Nonetheless, it may take some time for other states to observe the

effect of the Massachusetts regulations and determine whether or not they want to adopt similar laws.

We may yet see mass adoption of the Massachusetts approach, but I suspect it will take many years for that to happen. We may sooner see a uniform law or federal legislation. It is equally plausible to me that a large number of states will see the Massachusetts approach as overbroad and avoid anything other than a simple statute calling for reasonable care of personal information similar to California's AB 1950.

F. Michigan Data Protection Bill

Michigan is the state closest to adopting a Massachusetts-style comprehensive set of data security standards, but it takes a different approach than Massachusetts. In S.B. 717, the Michigan Senate laid out a number of information security practices based on the Massachusetts law. Section 5 of the bill states that it applies to any person that "owns, licenses, stores, or maintains personal information" about a Michigan resident.

The bill, however, does not require that individuals and businesses comply with a set of requirements embodying these practices. Instead, S.B. 717 offers a carrot rather than a stick. Section 5 states that individuals and businesses that develop, implement, maintain, and monitor a comprehensive written information security program have civil immunity from liability. Section 13(1) of the bill states:

> A person that develops, implements, maintains, and monitors a comprehensive written information security program . . . is immune from civil liability for any damages resulting from unauthorized access or acquisition of data or electronic data that compromises the security, availability, confidentiality, or integrity of personal information maintained by that person.

Thus, S.B. 717 would not force businesses to adopt a comprehensive security program, but rather offers an incentive in the form of immunity to do so. If enacted, it remains to be seen which is more effective to bring about good security practices, a requirement to implement such practices or an incentive in the form of immunity from liability. For the moment, however, the bill remains with the Senate's Committee on Homeland Security and Emerging Technologies. Bill status information shows no activity on the bill since its referral to the Committee last August.

G. Mississippi Breach Notification Bill

The Mississippi House approved a breach notification bill, H.B. 583, in January 2010, and the Mississippi Senate amended and passed a version of H.B. 583 in March. The bill covers businesses holding the personal information of Mississippi residents. The House and Senate are conferring on the two versions of the bill to resolve the differences between the two versions. If enacted and signed by the Governor, Mississippi would join 45 other states with breach notification laws.

The "personal information" covered by H.B. 583 includes the same categories as California SB 1386 – name in combination with a driver's license number, Social Security number, or account number together with an access code. H.B. 583 § 1(1) (2010). Business would have to notify Mississippi residents if a security breach involved unauthorized access to their personal information. *Id.* § 1(2). No notification would be necessary if, following an investigation and consultation with law enforcement, the business "reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and assessed." *Id.* The affected business may delay notification during a criminal investigation. *Id.* § 1(4).

The Attorney General would have the authority to enforce the law. The bill calls a failure to comply with the requirements an "unfair trade practice." *Id.* § 1(7). The law does not include a private right of action.

H. Missouri's New Breach Notification Law

Missouri became the 45th state to enact a breach notification law. Mo. Rev. Stat. §§ 407.1500.1-407.1500.4. Missouri's governor signed the enabling legislation, H.B. 62, into law last July. It went into effect last August 28.

H.B. 62 covers "personal information" consisting of a name in combination with a driver's license number, Social Security number, or account number together with an access code. *Id.* §§ 407.1500.1(9). These are the usual elements of "personal information" seen in California's SB 1386. In addition, however, the Missouri law also covers personal information in the form of medical information, health insurance information, and identifier and access codes permitting a person to access a financial account. *Id.*

Businesses must notify Missouri residents if there is unauthorized access to residents' personal information that the businesses are maintaining. *Id.* § 407.1500.2(1). No notification is necessary if, following an investigation and consultation with law enforcement, the business "determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach." *Id.* § 407.1500.2(5). A business making such a determination must record it in writing and preserve the writing for five years. *Id.* In addition, a business may delay notification if law enforcement informs the person that notification may impede a criminal investigation. *Id.* § 407.1500.2(3).

The Missouri law states that the Attorney General has the "exclusive authority" to bring an action for damages or a civil money penalty. The "exclusive authority" phrase implies that there is no private right of action. The maximum penalty the A.G. may seek is $150,000 for one breach or a "series of breaches of a similar nature that are discovered in a single investigation." *Id.* § 407.1500.4.

I. Montana Amendments to Breach Notification Law

Last April, Montana added a public sector breach notification requirement to its existing private sector breach notification law. Mont. Code Ann. § 30-14-1704. The new law, enacted as H.B. 155, went into effect on October 1, 2009. It applies to "state agencies," and creates a breach notification requirement for agencies maintaining data containing personal information.

Montana state agencies must notify any person (whether or not a Montana resident) whose unencrypted personal information is acquired by an unauthorized person following a breach. *Id.* § 2-6-504(1)(a). Notification does not depend on a finding of likely harm. If a third party makes the required notifications, the agency does not need to notify the affected persons of the breach.

Like California's SB 1386, "personal information" means a name in combination with a driver's license number, Social Security number or account number together with an access code. *Id.* § 2-6-501(4). An agency may delay notification if a law enforcement agency determines that notification would impede a criminal investigation and requests a notification delay. *Id.* § 2-6-504(3).

More generally, state agencies obtaining personal information must develop and maintain an information security policy to safeguard the personal information they manage, as well as breach notification procedures to provide the required notice. *Id.* § 2-6-504(4).

H.B. 155 also includes requirements for state agencies to protect individuals' social security numbers. Agencies must develop procedures to eliminate the unnecessary use of Social Security numbers, restrict access to SSNs, redact and dispose of documents containing SSNs, eliminate unnecessary storage of SSNs, and protect data containing SSNs on portable devices. *Id.* § 2-6-502. Existing state agencies must comply with this law by September 1, 2012.

J. Nevada's New Encryption Law

In 2005, Nevada created a law that required encryption of personal information electronically transferred outside of a business's networks. Nev. Rev. Stat. § 597.970. The operative provision of the statute provided, "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission." *Id.* § 597.970(1). Note that the legislature assumed that (1) information is secure within a security perimeter of a business, but not outside it, (2) "transmission" is the key risk, as opposed to the loss of media containing information, and (3) any kind of "encryption" is sufficient to protect transmission, without the need for specifying the strength of the encryption. From an information security perspective, these are unwarranted assumptions.

Last May, however, Nevada enacted S.B. 227, which amended its encryption law and repealed Section 597.970. The new law, codified at Nev. Rev. Stat. § 603A.215, covers "data collectors," which is a term referring to governmental agencies, universities, financial institutions, and any other businesses that handle personal information. *Id.* § 603A.030. It offers two routes to compliance.

First, data collectors doing business in Nevada and accepting payment cards for the sale of goods or services have an obligation to comply with the latest version of the Payment Card Industry (PCI) Data Security Standard. *Id.* § 603A.215(1). Data collectors not accepting payment cards have an obligation to encrypt electronically transmitted information outside their secure systems. *Id.* § 603A.215(2)(a). This requirement is similar to the repealed Section 597.970. In addition, however, data collectors must encrypt data on portable data storage devices containing personal information, if the devices go beyond the "logical or physical controls" of the data collector or its storage contractor. *Id.* § 603A.215(2)(b). The statute states that encryption must involve technology adopted by an established standards body and the use of appropriate cryptographic key management security controls. *Id.* § 603A.215(5)(b).

The law shares the definition of "personal information" with Nevada's breach notification law. The term means a name in combination with Social Security number, driver's license, or account number together with an access code. This definition is the same as the definition of the term in California's SB 1386.

If the goal is to require encryption of all data at all times, the law may fail. First, although Section 4.1 of the PCI Data Security Standard would require that merchant data collectors transmitting card information over open networks use strong cryptography to protect the information, Section 3.4 does not require the use of encryption of primary account numbers not transmitted through open networks. The controls over portable media in Section 603A.215(2)(b) would apply only if the data collector is not a merchant that collects payment card information for selling goods and services. Thus, if the data collector is a merchant, it may not have an obligation to encrypt personal information on portable media, like other kinds of data collectors.

Second, a merchant storing payment card information for the sale of goods and services need only comply with PCI and not Section 603A.215(2)'s controls over non-payment personal information. For instance, if the merchant also has non-card personal information, such as driver's licenses or social security numbers, for non-payment applications, PCI's encryption requirements do not apply. Moreover, Section 603A.215(2) arguably does not apply because it says it applies only if subsection (1) does not apply. And subsection (1) does apply because the data collector is a merchant collecting card information. Accordingly, data collector merchants collecting card information for sales appear to have no requirement to encrypt non-payment personal information.[11]

[11] The legislature perhaps should have stated that the encryption controls of subsection (2) apply only to the extent the data are protected by PCI. That way, it would cover non-payment personal information held by merchants that must protect payment personal information under PCI.

K. New Jersey Permits Interception of Web Communications

In October, New Jersey enacted cybercrime legislation signed by Governor Corzine authorizing the interception of wire or electronic communications of "computer trespassers." A.B. 3761 (2009). Persons acting "under color of law" are authorized to "to intercept the wire or electronic communications of a suspected computer trespasser transmitted to, through, or from a computer or any other device with Internet capability." *Id.* § 1(a). Such interception is permissible only if the owner or operator of the computer or device authorizes the interception, the person is lawfully engaged in an investigation, the investigator has reasonable grounds to believe the communication's contents are relevant to the investigation, and the interception does not acquire communications other than those to or from the computer trespasser. *Id.*

This legislation may pertain to our clients involved in telecommunications or clients who act as Internet Service Providers. These clients may face law enforcement requests to cooperate in the interception process.

The legislation attempts to provide an additional mechanism for law enforcement to protect the public from Internet threats. Criminal defendants can challenge the legality of the interception. A successful challenge would exclude the evidence from any trial, hearing, or proceeding. *Id.* § 1(c).

L. North Carolina Amendment to Breach Notification Law

Last July, North Carolina enacted S.B. 1017, which amends the state's breach notification law. N.C. Gen. Stat. § 75-65. The amendments change the nature of the breach notification by requiring a description of the incident, the type of information involved, and steps taken to prevent further unauthorized access. The new law also includes a requirement for providing contact information for consumer reporting atancies, the Federal Trade

Commission, and the North Carolina Attorney General's office to allow those affected to obtain more information about identity theft. *Id.* § 75-65(d).

S.B. 1017 also added a requirement to notify the Consumer Protection Division of the Attorney General's office in the event of a breach. The law had a provision requiring notification to the A.G. of the content of a breach notice, if notice went out to more than 1,000 people. The new section of the statute has no lower limit on the number of people affected; a notification must go to the A.G.'s office regardless of how few people are affected. The notice must inculde the nature of the breach, the number of consumers affected, investigative steps taken, prevention of future breaches, and information about the notice sent. *Id.* § 75-65(e1).

M. Texas Amendments to Breach Notification Law

Last June 19, Texas passed into law legislation that amended its breach notification law. The bill, H.B. 2004, makes a number of changes to expand the protections offered by the breach notification law. First, it adds health information to the definition of "sensitive personal information," the compromise of which would trigger a notification. Individually identifiable information about health condition, treatment information, and payment information are included. Tex. Bus. & Com. Code Ann. § 521.002(a)(2)(B).

Second, the businesses that must protect personal information with reasonable security controls now include nonprofit athletic or sports associations. *Id.* § 521.052(d). This section of the Texas data protection law is analogous to California's AB 1950.

Third, breach notification is triggered not only by the compromise of unencrypted personal information, but also encrypted personal information in situations where the attacker has the cryptographic key needed to decrypt the data. Interestingly, in some cases, it is

possible to have the decryption key without the ability to decrypt the data.[12]

Finally, the new Texas law creates a breach notification requirement for state agencies and local governments. Tex. Gov't Code Ann. § 205.010 (local governments); *id.* § 2054.1125 (state agencies). These government entities must comply with the notification requirements appearing in the breach notification law that applies to businesses. Tex. Bus. & Com. Code Ann. § 521.053.

N. Virginia Health Information Breach Notification Law

On March 3, 2010, the Virginia House and Senate passed a bill that would add health information as an additional category of information that would trigger a breach notification if it were compromised. The legislation, H.B. 1039, would require the notification of Virginia residents and Virginia's Attorney General if residents' medical information is compromised by a security breach. "Medical information" covered by the bill includes information about a person's health condition, history, diagnosis, or treatment; policy number, subscriber information number, or other identifier; or information about his or her application or claims history.

H.B. 1039 does not include a provision stating that a risk of harm is necessary to trigger a requirement of breach notification. An entity may delay notification if a law enforcement agency tells the entity that notification will impede a criminal investigation, a civil investigation, or national or homeland security. The bill would not

[12] In some instances, for example, the symmetric cryptographic key is provided to a recipient or stored, and the key itself is encrypted. The intended recipient uses a different secret key to decrypt the stored key and then uses the stored key to decrypt the data. Thus, in theory a business must make a breach notification where an attacker takes a laptop and "has the key" even though the attacker may be entirely unable to use the key to access the data. Perhaps, if the issue ever arose in a real case, the courts will hold that an attacker does not "have the key" if the attacker has the key only in an inaccessible encrypted form.

apply to entities that are covered by the Health Insurance Portability and Accountability (which must notify patients of data breaches under the HITECH Act[13]) or FTC breach notification requirements.

O. Washington's PCI-Based Card Reissuance Liability Law

On March 22, 2010, Washington's governor signed a new law that holds businesses and card processors liable for the cost of reissuing cards following a security breach caused by their negligence. The legislation, H.B. 1149, goes into effect on July 1, 2010. H.B. 1149 § 3 (2010). Covered businesses are those that process more than 6 million card transactions a year and provide goods and services to Washington residents. *Id.* § 2(1)(c). The law also includes an unsual new type of liability – one imposed on vendors. Covered vendors are those providing card procssing technology or outsourcing vendors that maintain account information.[14] The new law will appear in chapter 19.255 of the Revised Code of Washington.

At the heart of H.B. 1149 is the provision holding processors and covered businesses liable for failing to take reasonable care to prevent unauthorized access to account information. They are responsible for card reissuance costs.

> If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is

[13] Health Information Technology for Economic and Clinical Health (HITECH) Act within the American Recovery and Reinvestment Act of 2009, Pub. L. No. 1111-5.

[14] The law appears to cover outsourcing vendors holding any kinds of data if they are holding account information. Thus, general cloud computing storage vendors are covered if they are providing services to processors or merchants holding account information.

> liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach.

H.B. 1149 § 2(3)(a) (emphasis added). In any litigation to recover such costs, the prevailing party is entitled to attorneys' fees and costs. *Id.*

In addition, the Washington law includes a novel vendor liability provision applying to situations where a technology or outsourcing vendor's negligence caused the damages.

> A vendor, instead of a processor or business, is liable to a financial institution for the damages described in (a) of this subsection to the extent that the damages were proximately caused by the vendor's negligence and if the claim is not limited or foreclosed by another provision of law or by a contract to which the financial institution is a party.

Id § 2(3)(b). Vendors have largely escaped liability for security breaches, but this provision changes the situation. If it becomes a trend, it may open the door to much greater liability.

The legislation, though, preserves defenses against the claimants, namely financial institutions, where the vendors have contracts with financial institutions limiting liability. *See id.* In general, the law states that it does not foreclose any applicable defenses, including those based on contracts or comparative fault. *See id.* § 2(5). In fact, in any trial, the trier of fact must make a finding concerning the percentage of fault that can be ascribed to each party. *See id.* § 2(6). Any liable party also receives a set-off based on the financial institution's separate recovery of reissuance costs from a credit card company. *See id.* § 2(7).

The other significant part of the new law is the section containing safe harbors from liability. The law provides two safe harbors.

First, no liability attaches to any party if account information was encrypted at the time of the breach. *Id.* § 2(2)(a). Encryption is defined to mean encryption "using standards reasonable for the" business in light of its size and transaction volume. *Id.* § 2(1)(f). Thus, unlike many other encryption laws around the country, totally weak encryption will not suffice for the safe harbor.

Second, no liability attaches to a party that was certified to be compliant with the Payment Card Industry Data Security Standard in force at the time of the breach. *Id.* § 2(2)(b). The provision also says that a party is compliant if it had an annual security assessment within the year before the breach. *Id.* Thus, no new assessment need be done. Nonetheless, if the PCI standard changes after the security assessment but before a breach, the safe harbor does not apply. Therefore, if the standard changes, covered entities should be reassessed. Nonetheless, the latest version is a year and a half old, so the standard does not seem to change often.

III. Prospects for a Uniform State Law on Data Protection

The body that develops uniform state laws in the United States, the Uniform Law Commission (ULC), is in the process of considering whether or not to move forward with the process of developing a uniform data security law. The ULC, formerly known as the National Conference of Commissioners on Uniform State Law (NCCUSL), is the group that created the Uniform Commercial Code. It has also developed a whole host of other uniform laws.

The ULC clarifies and harmonizes state law in order to provide consistency from state to state and minimize the difficulty for individuals and businesses to have to comply with a patchwork of inconsistent state laws. The ULC intends for uniform laws to promote economic development by creating a single set of rules in areas of the law for foreign governments and businesses to manage. The ULC drafting committees create uniform laws in an open drafting process through the work of commissioners who are practicing lawyers and experts in their fields, as well as other legal

experts and advisors and observers from other legal organizations. Once the ULC completes a uniform law, it promotes that law to the states and encourages them to adopt it.

The ULC now is just beginning the process to take up a uniform data security law. One ULC commissioner, Steve Chow, submitted a proposal to form a study committee to determine the feasibility of having a uniform data security law. Presumably, the study committee would need to approve the concept before any drafting could begin. At this time, Steve Chow's concept for a uniform act would be to provide minimum data security standards to protect against unauthorized access to personal information. He listed two examples of entities that the law would cover, namely businesses and banks.

The ULC asked Steve Chow to do more research into the project and report back at the Midyear Meeting of the ULC Committee on Scope and Program in Tucson on January 8, 2010. Minutes from the meeting state that Steve Chow was unable to complete a proposal for the Midyear Meeting due to other obligations, but he intends to present an extensive proposal at the July 2010 Annual Meeting of the Committee.[15]

In short, we will not see a uniform state law on data protection anytime soon. The ULC has not yet constituted a study committee to determine the feasibility of such a project. Even if approved in July 2010, a drafting committee would have to form, and its work could last two years before it creates a draft for debate by the ULC and eventual approval. And once any such law is approved, it may take another long period of time for the states to adopt the law.

---

[15] Minutes from the Midyear Meeting of the Committee on Scope and Program, Uniform Law Commission, at 11-12 (Jan. 8, 2010), *reprinted at* http://www.uniformlaws.net/nccusl/Docs/Scope/Scope%2001-08-10%20mn.pdf.

IV. Trends in Security and Privacy Laws

My general impression of trends in state security and privacy legislation is that things have not changed much since last year, although the seeds are planted for more radical changes in future years. For instance, so far, the Massachusetts legislation and regulations calling for a comprehensive written information security program have not led to mass adoption of similar laws in other states. The Michigan data protection bill makes Michigan the next in line to create a regime similar to that of Massachusetts, but the bill does not seem to be active, and no other states are following.

Instead of states jumping on board with the Massachusetts approach, we have seen incremental change. For exaample, this past year saw the adoption in Missouri of breach notification legislation requiring notice to consumers affected by security breaches. Missouri became the 45th state to adopt such legislation, which is in effect in 44 other states plus the District of Columbia, Puerto Rico, and the Virgin Islands. It remains to be seen what happens with H.R. 2221 at the federal level, but as mentioned above, Mississippi and Kentucky are now taking up breach notification legislation. If these bills pass, only Alabama, New Mexico, and South Dakota would be without any breach notification laws on the books.

I expect states to continue testing the effectiveness of relatively modest and incremental legislation. Yet, with the huge cost of data breaches, small and large, it is more important than ever for businesses to adopt security programs from a risk management perspective, even if they have no legislative or regulatory requirement to do so. Businesses face the prospect of liability for breaches after the fact, even if they have no legislative or regulatory requirement to prevent breaches in the first place. Moreover, if the Washington law placing liability on merchants, processors, and vendors for card reissuance inspires other similar laws in other states, we may see a significant change in the way breach response cost liability is apportioned.

The other general impression I have from the legislation and speaking with people in industry this past year is that businesses across the country are becoming more interested in implementing encryption solutions this year. It may be that the Massachusetts regulations' requirement for encryption, coupled with other encryption laws, is driving the new interest. New interest may also stem from the highly-publicized data breaches involving unencrypted information. The cost effectiveness of encryption and its solutions as a partial answer to protecting sensitive information may also play a role. The interest may arise from a combination of these and other factors. Regardless, I believe our clients will start to ask more questions about encryption this year, and we will see more of them procuring encryption solutions.