Financial Institutions and Securities

WILMERHALE

Data Security Update

Last year, ChoicePoint publicly announced that it had sold personal information about over 100,000 consumers to identity thieves, sparking a frenzy of media and legislative attention on the issue of data security. Recently, ChoicePoint agreed to pay the largest civil penalty in FTC history to settle alleged law violations relating to the compromised information.[1] In the wake of ChoicePoint's announcement and the avalanche of additional breach notifications by other companies last year, states have been actively legislating, with 22 states joining California's ranks and enacting security breach notification laws last year and nine states—Arizona, Colorado, Idaho, Indiana, Kansas, Maine, Nebraska, Utah and Wisconsin—adopting new breach notification laws or revising their existing laws so far this year.[2] A number of states have also enacted or are considering security freeze laws allowing consumers to block access to their credit reports[3] or laws restricting the use of Social Security numbers. Many of these state laws purport to extend not only to entities and conduct that now fall through the cracks in federal regulation but also to financial institutions covered by federal privacy and data security regulations.

Where does this leave financial institutions, securities firms, retailers, educational institutions and others that may be subject to these state breach notification laws? Absent a national standard preempting state laws, it leaves them subject to thirty different and potentially conflicting state law obligations. In many cases, the practical reality is that companies will likely comply with the most rigorous state law applicable to them to avoid the logistical and public relations difficulties of treating similarly situated customers differently based only on their addresses. This effectively means that one or two states can undermine the policy choices made by federal regulators and by individual states in determining the proper balance between notifying consumers of breaches that could lead to identity theft and avoiding burdensome costs to entities suffering breaches that are unlikely to cause any consumer harm.

If Congress can agree on and pass a preemptive national data security standard, it could avoid this morass. Members of the House and Senate introduced over 20 competing bills on data security or privacy during the course of 2005, over a dozen of which directly addressed consumer notice of data security breaches, and more have been introduced in 2006. Yet, despite early predictions that the passage of a federal data security law was imminent, there are a number of thorny issues that need to be worked out before a federal law can be passed, from resolving jurisdictional overlap between Congressional committees to debates over substantive issues.

Federal banking regulators have filled in some of the gaps left by Congressional inaction. The federal Banking Agencies[4] have been active in issuing guidelines and guidance on data security obligations with respect to financial institutions. The Banking Agencies issued Final Guidelines on security breach response programs at the end of March 2005 that became effective immediately.[5] In addition, last fall, they issued interagency guidance on identity authentication procedures for online customer account access,[6] and in December, they followed up with guidance for small entities to comply with the security standards.[7] The Federal Trade Commission has been active on the enforcement side, making clear that it views data security and data privacy obligations as applying to all entities under its jurisdiction, regardless of whether they are "financial institutions" subject to the Gramm-Leach-Bliley Act. In addition to the ChoicePoint agreement referenced above, the FTC has obtained consent agreements from a number of other companies—including CardSystems Solutions, Inc.,[8] DSW Inc.,[9] and BJ's Wholesale Club, Inc.[10]—that it pursued for alleged failures to take reasonable security measures to protect sensitive data, claiming that such failures amount to an unfair trade practice in violation of Section 5 of the Federal Trade Commission Act.

Background

Data security and data privacy are not new issues for federal legislators or regulators. In 1999, Congress passed the Gramm-Leach-Bliley Act that in part required the promulgation of data privacy and data security rules by

various federal regulatory agencies with jurisdiction over the broadly defined category of "financial institutions." In response to this mandate, each of the tasked agencies promulgated detailed data privacy rules. The Banking Agencies issued detailed guidelines and the FTC promulgated rules setting forth standards for insuring the security, confidentiality, integrity and protection of customer information and requiring the creation and implementation of written information security programs. The SEC's privacy rule includes the requirement that covered entities adopt policies and procedures to safeguard customer information. The resulting rules and guidelines, however, focused only on financial institutions and did not extend, for example, to retailers or data brokers unless those entities otherwise fell within the definition of "financial institutions" because they offered financial products or services.

This focus shifted dramatically, however, early last year with data broker ChoicePoint's announcement that it had provided personal information regarding well over 100,000 individuals to identity thieves. ChoicePoint's announcement was prompted by California's data security breach notification law, passed in 2002. The California statute requires disclosure of any security breach to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person following the entity's discovery or notification of the breach.[11]

ChoicePoint's announcement was just the start of an avalanche of announcements on a nearly weekly basis by additional companies disclosing data security breaches impacting hundreds of thousands of individuals. It seemed that no industry was spared, with security breaches announced by such wide-ranging entities as data brokers (such as ChoicePoint), financial institutions, credit card processors, retailers, universities and colleges, and even the United States Air Force. By some estimates, security breaches compromised the confidentiality of personal information about over 52 million American consumers in 2005 alone.[12]

State Data Security Breach Notification Laws

Spurred by the growing number of highly publicized security breaches and the gaps in existing federal data security requirements, states have taken up the data security mantle. As of the beginning of May 2006, thirty states, including California, have enacted data security breach notification laws. Generally, these laws require an entity to notify customers in the event of the unauthorized acquisition of computerized data that compromises the confidentiality of "personal information" maintained by the entity. There are, however, a number of significant differences among these laws that make determining their applicability to a security breach a time-consuming and burdensome task for entities that operate on a nationwide, or even regional, scale.

Scope. Most state data security breach laws apply broadly to entities—including retailers, educational institutions, financial institutions and others—that do business within the state and collect, assemble or maintain personal information about state residents. A handful of state laws, however, currently have a more limited scope. The security breach notification law in Georgia applies only to "information brokers," generally defined as entities that, for monetary fees or dues, engage in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting or transmitting personal information about individuals for the primary purpose of furnishing the information to nonaffiliated third parties.[13] Maine's original breach notification law also applied only to information brokers,[14] however, in April, Maine amended its law to cover all "persons," including individuals, business entities, state agencies, and private and state universities and colleges.[15] The amendment takes effect January 31, 2007. Similarly, Indiana's original breach notification law applied only to state agencies,[16] however, in March, the governor signed a second bill into law that expands the consumer notification requirements to persons that own or license computerized data that includes personal information.[17] The new Indiana law will take effect on July 1, 2006.

Even if an entity falls within the broad scope of a state law in the first instance, it may be exempted from coverage under other provisions within the law. Twenty-two of the state laws contain some form of exemption for regulated entities. These exemptions vary from state to state, but can be generally divided into four categories:

- Broad exemptions for entities that maintain and comply with security breach procedures pursuant to rules, regulations, procedures or guidelines established by their primary or functional regulator;[18]
- Broad exemptions for entities that are subject to and in compliance with specified laws, such as the data security and privacy provisions under the Gramm-Leach-Bliley Act (GLBA);[19]
- Narrower exemptions for financial institutions subject to and in compliance with the Banking Agencies' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005;[20] and

- Narrower exemptions for entities subject to and in compliance with rules that provide greater or equal protection for personal information and at least as thorough notification requirements.[21]

In addition, twenty-five state laws contain exemptions from required notification procedures for entities that maintain their own notification procedures as part of an information security policy or program, provided that the procedures are consistent with the state law's timing requirements and that the entities notify consumers in accordance with their procedures in the event of a security breach.[22] Only Arizona, Indiana, Pennsylvania and New Jersey require that the entity's notification procedures be consistent with state law requirements other than timing or that the entity's notification procedures equal or exceed the state law's requirements. Indiana's new law requires that the entity's notification requirements be at least as stringent as the state law's requirements,[23] and Arizona's, New Jersey's and Pennsylvania's laws require that the entity's notification requirements be consistent with the requirements of the state laws, without limiting the requirement for consistency to timing obligations.[24]

Information Covered. Generally, state security breach notification laws apply only to defined sets of information, often termed "personal information."[25] Although there are many similarities between the state law definitions of personal information, there are important substantive distinctions as well that could lead the same information to be deemed covered under one state's statute but not under another.

Although the exact wording varies, the majority of states define "personal information" as an individual's first name or initial plus last name in combination with one or more of the following data elements: (1) Social Security number; (2) state driver's license number or other state identification number; or (3) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.[26] Some states use this same general formulation, but specify that an account number need not be combined with a security code, access code or password and that those items may independently constitute data elements that, when combined with the person's name, would be deemed "personal information."[27]

In addition, some state laws expand the list of data elements to include such data as biometrics, date of birth and employee identification numbers.[28] New York, on the other hand, does not extend the list of data elements but rather extends the identifying information that, when combined with the data elements, constitutes covered information. Information is covered under the New York law if it consists of any of the three standard data elements above in combination with an individual's name or any other identifier, including but not limited to a number or personal mark, that can be used to identify the person.[29] Under the New York law, a person's telephone number in conjunction with his or her Social Security number could conceivably constitute covered information where it would not under the laws of most other states.

Four states specify that disassociated data elements can constitute personal information. Under both Georgia and Maine law, a data element by itself can constitute personal information if the information would be sufficient to perform or attempt to perform identity theft.[30] Under the new Indiana law, a person's Social Security number by itself constitutes personal information.[31] Finally, under New Jersey law, disassociated data that, if linked, would constitute personal information can constitute personal information if the means to link the data is also accessed.[32]

To further complicate matters, states vary on what, if any, information must be unencrypted to constitute "personal information." While the vast majority of state laws cover only information that is at least in part unencrypted, four states expressly include encrypted information if the encryption key has also been compromised.[33] Of the states that require at least some level of unencryption to be covered, there are variations in what types of information must be unencrypted.

- Most states specify that if **either** the identifying information (e.g., the individual's name) or the data element (e.g., the individual's Social Security number) are unencrypted then it falls within the definition of personal information.[34]

- However, some states require that **both** the identifying information **and** the data element be unencrypted for the information to constitute personal information.[35]

- Still other states require that the **data element(s)** be unencrypted.[36]

The practical effect of these variations can be great. For example, if the data breached included unencrypted consumer names and encrypted driver's license numbers, then the data would be "personal information" only under the first bullet above. If, however, the reverse was true

and the data included **encrypted** consumer names and **unencrypted** driver's license numbers, then the data would be "personal information" under the first and third bullets. Finally, if all of the data were unencrypted, then it would be "personal information" under all of the bullets.

All but three state laws cover only electronic or computerized records. North Carolina's law expressly covers personal information in any form whether computerized, paper or otherwise.[37] Indiana's new law extends to computerized data that have been transferred to another medium, including paper, microfilm or a similar medium, even if the transferred data are no longer in computerized format.[38] Wisconsin's law is not expressly limited to computerized information and so would appear to cover personal information in other forms as well.[39] This underscores the importance of an appropriate document destruction policy. For example, printouts thrown into a company garbage receptacle and retrieved by an unauthorized person might be subject to breach notification obligations under these state laws if the information in the printouts otherwise meets the definition of covered information.

Trigger for Consumer Notification. Some state laws require consumer notification upon the mere unauthorized acquisition of personal information or the acquisition of personal information by an unauthorized person.[40] Tennessee and Nevada, although falling into this general category of states requiring broad notification, curtail the breadth of their laws by limiting their definition of a "breach of security" to security incidents that "materially" compromise the security, confidentiality or integrity of personal information.[41] These laws would seem to leave a back door open for entities to argue that inadvertent disclosures that pose little or no risk of harm or misuse do not materially compromise the security, confidentiality or integrity of personal information and therefore do not require consumer notification.

Most state laws, however, include some express form of a harm or misuse threshold.[42] Generally, these thresholds are stated either in the affirmative, setting forth the circumstances under which notification would be required, or the negative, setting forth the circumstances under which notification would not be required, with a number of variations in each category.

In the states with affirmative triggers, notification may be required if:

- The breach has resulted in or could result in identity deception, identity theft or fraud;[43]
- Illegal use or misuse of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm;[44]
- The breach causes a material risk of identity theft or other fraud;[45]
- The breach causes a significant risk of identity theft;[46] or
- The breach has caused or will cause some degree of loss or injury.[47]

In the states with negative triggers, notification may **not** be required if:

- Misuse of the information is not reasonably possible;[48]
- The breach is a technical breach and does not seem reasonably likely to result in a risk of criminal activity;[49]
- A breach has not and will not likely result in harm;[50] or
- There is no reasonable likelihood of harm.[51]

In several of the states with notification triggers, however, there are additional requirements beyond the initial investigation that must be satisfied in order to avoid consumer notification. For example, Connecticut requires that an entity consult with relevant federal, state and local agencies responsible for law enforcement in making the determination,[52] and Florida and New Jersey require that a determination that the risk trigger is not satisfied be documented in writing and that the documentation be retained for five years.[53] Even absent express documentation requirements, best practices would include documentation of the investigation of the security breach and the conclusion that the risk threshold has not been satisfied to assist the entity in the event a state attorney general or regulator later learns of the breach and demands to know why consumer notification was not provided.

Other Notification Requirements. An entity that suffers a security breach must also be aware of other potential notification obligations beyond the obligation for consumer notice. Most states require an entity to give notice to nationwide consumer reporting agencies in the event that the entity provides over a specified number—ranging from 500 to 10,000—of consumer notices to state residents at one time.[54] Under Montana law, if an entity intends to send

a consumer a notice that suggests, indicates or implies that he or she may obtain a copy of his or her credit file, the entity must not only notify nationwide consumer reporting agencies, but must also coordinate the timing, content and distribution of consumer notices with the agencies.[55]

In addition, Maine, New Jersey, New York and North Carolina require notification of various state entities in the event that consumer notification is required. Maine requires information brokers to notify regulators within the Department of Professional and Financial Regulation, or, if the information broker is not regulated by the Department, the state attorney general of the security breach.[56] New Jersey requires entities, in advance of providing consumer notification, to report the security breach and related information to the Division of State Police in the Department of Law and Public Safety for investigation or handling.[57] New York requires entities to notify the state attorney general, Consumer Protection Board and the state Office of Cyber-Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and the approximate number of affected persons.[58] Finally, North Carolina requires businesses to notify without unreasonable delay the Consumer Protection Division of the state Attorney General's Office of the timing, distribution and content of the consumer notice if it is to be sent to more than 1,000 persons at a time.[59]

Timing for Consumer Notification. Although the language varies, the overwhelming majority of state laws contain flexible timing requirements, specifying, for example, that consumer notification be given in the most expedient manner possible and without unreasonable delay or as soon as practicable consistent with the legitimate needs of law enforcement.[60] Under these state laws, while entities may not unreasonably delay instituting and concluding breach investigations and sending out consumer notifications, they are not subject to a date-certain deadline. Only three states contain exact timing requirements—Florida, Ohio, and Wisconsin. Each of those states generally require that consumer notification be given not later than 45 days following discovery or determination of a breach, subject to the legitimate needs of law enforcement and to the time necessary to investigate the breach and restore system integrity.[61]

Delivery of Consumer Notices. All states permit written notification, but they vary on whether other methods can be used to delivery consumer notification and what, if any restrictions, are placed on those methods. For example, all states, with the possible exception of Wisconsin,[62] permit electronic notification of consumers; however, use of electronic notification may be subject to certain restrictions or requirements. Many states that permit electronic notice require that the notice conform with requirements under the federal E-SIGN law.[63] Other states incorporate specific state law requirements. Under Ohio law, for example, email notification may be used only if the person's primary method of communication with the resident is by electronic means.[64] Pennsylvania law permits electronic notice only if there is a prior business relationship and the entity has a valid email address for the individual.[65] New York law permits electronic notice if the individual has given express consent and prohibits an entity from requiring that a customer agree to electronic notice as a condition of establishing a business relationship or engaging in a transaction.[66] Further, it requires an entity to keep a log of electronic notices.[67]

In contrast to the wide-spread acceptance of written and electronic notice, less than half of the states permit telephonic notice,[68] and of those that do, several place restrictions on the circumstances under which telephonic notice may be provided. Similar to its requirement for electronic notification, New York requires that a log of telephonic notifications be kept.[69] North Carolina requires that the telephone notification be provided directly to the affected person.[70] Pennsylvania permits telephonic notice only if: (1) the customer can reasonably be expected to receive it; (2) the notice is given in a clear and conspicuous manner; (3) the notice describes the incident in general terms and verifies personal information but does not require the customer to provide personal information; and (4) the customer is provided with a telephone number to call or an internet website to visit for further information or assistance.[71] Utah, on the other hand, not only permits telephonic notification but also permits the use of automated dialing technology that is not otherwise prohibited by law.[72] Further, in addition to written, electronic and telephonic notification, Utah also permits a fourth method of general notification: an entity can satisfy its consumer notification obligation by placing a public notification of the breach in a newspaper of general circulation.[73]

All of the states except for Utah and Wisconsin set forth substitute notification provisions that an entity can use to satisfy its consumer notification requirements in the event that the number of consumers to be notified or the cost of notification exceeds threshold levels or the entity has

insufficient contact information to provide notification using the standard methods. Although the number and cost thresholds vary in some states,[74] most state laws specify that if the cost of notification exceeds $250,000 or the number of persons to be notified exceeds 500,000 persons, the entity may provide substitute notification.[75]

The methods of communication used to satisfy substitute notification requirements may vary as well. Most states require an entity to notify consumers: (1) by email if the entity has an email address for the consumer; (2) conspicuous posting on the entity's website, if the entity maintains a website; **and** (3) notification to major statewide media.[76] Texas law, however, permits an entity to satisfy substitute notification requirements by using any of these three methods of notification.[77] Indiana law also provides a lower requirement for substitute notification, requiring an entity to post the notice on its website and to provide the notice to major news reporting media in the geographic area where the affected Indiana residents reside.[78] In contrast, Montana permits an entity to provide substitute notice by email notification and posting on the entity's website **or** by notification to local and statewide media.[79] In addition, Ohio and Nebraska have special provisions for small businesses permitting substitute notification if a business has ten or less employees and the cost of providing customer notification will exceed $10,000.[80] Under Ohio's provision, the small business may provide notice by: (1) placing a paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located; (2) posting a notification on the entity's website, if it has one; and (3) notifying major media outlets in the geographic area in which the business is located.[81] Nebraska's provision requires the use of the same three notification channels as well as the use of email notification if the entity has email addresses for the affected individuals.[82]

Notice Content Requirements. With the exception of New York and North Carolina, the existing state breach notification laws do not specify what disclosures must be made in the consumer notice. New York requires that the consumer notification include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including the specification of which of the elements of personal information and private information were subject to the breach.[83] North Carolina requires that consumer notices be clear and conspicuous and include a description of: (1) the incident in general terms; (2) the type of personal information that was subject to the unauthorized access and acquisition; (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, if one exists; and (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.[84] Although Wisconsin does not specify the content of the notice, it does require entities that provide consumer notice, upon written request by a person who receives a notice, to identify the personal information that was acquired.[85]

Enforcement. Generally, the state breach notification laws are enforced by state attorneys general who are empowered to seek injunctive or other relief,[86] including in some states specified civil fines, costs of the investigation and reasonable costs of maintaining the enforcement action.[87] As a result of the civil fine provisions, an entity that is found to be in violation of the breach notification laws of multiple states could find itself facing significant financial liability even absent consumer injury. If consumer injury is present, another potential risk arises—private law suits. Although only a few state breach notification laws expressly authorize private rights of action under the notification law itself for consumers injured as a result of a violation,[88] a private litigant could attempt to pursue a cause of action based on the facts of the violation under other state laws such as state unfair and deceptive trade practices laws or state contract law based on privacy and data security promises the company may have made or due to the company's failure to adequately protect consumer data.[89]

As a result of these many differences between state laws, determining whether notification is necessary with respect to consumers in a given state requires a state-specific analysis. For companies that operate on a multi-state or nationwide level, this can create a substantial burden, underscoring the need for a national standard.

Federal Data Security Breach Notification Bills

Many members of Congress recognize the need for a nationwide breach notification standard. Congress has been working to reconcile the over twenty competing bills on data security or privacy that have been introduced.[90] This has been a particular challenge as these bills cross committee jurisdictional lines. The bills have been parsed out between six Congressional Committees:

- the Senate Committee on Commerce, Science and Transportation;

- the Senate Committee on Banking, Housing and Urban Affairs;
- the Senate Committee on the Judiciary;
- the House Committee on Energy and Commerce;
- the House Committee on Financial Services; and
- the House Committee on the Judiciary.

Each committee claims jurisdiction over aspects of the issue, and each, to an extent, is correct in that assertion: the issue of data security touches on financial institutions (falling under the banking committees' jurisdiction), general industry (falling under the commerce committees' jurisdiction) and law enforcement (falling under the judiciary committees' jurisdiction).

Currently, four Senate bills—S. 1326, S. 1789, S. 1408 and S. 1332—have been placed on the Senate legislative calendar, yet, there is no indication of when a floor vote will occur on any of these bills. On the House side, H.R. 3997 and H.R. 4127 were recently marked up and approved by the House Committee on Financial Services and the House Energy and Commerce Committee respectively, but, again, there is no indication of when a floor vote will occur on either.

On May 9, House Judiciary Chairman James Sensenbrenner introduced a new bill (H.R. 5318) taking a different approach to the data security breach issue. Rather than requiring **consumer** notification in the event of a security breach, it requires **governmental** notification. Under the bill, entities would be required to notify the United States Secret Service or the Federal Bureau of Investigation within 14 days of the discovery of a "major security breach."[91] An entity or individual would be subject to a fine of up to one million dollars, imprisonment for up to five years, or both if it knowingly failed to provide notice to the Secret Service or the FBI with the intent to prevent, obstruct or impede a lawful investigation of a breach and if the breach caused a significant risk of identity theft. While H.R. 5318 does not require consumer notification, it acknowledges that other state or federal laws could contain such a requirement and specifies that notification to the Secret Service or FBI must precede any consumer notification. The bill has been referred to the Subcommittee on Crime, Terrorism, and Homeland Security, and subcommittee hearings were held on the bill last week.

Narrow Versus Comprehensive Scope. One of the key points of disagreement is defining the scope of the various data security bills. Privacy proponents are pushing for a comprehensive bill addressing the broad spectrum of data privacy and data security issues. Industry, on the other hand, argues that these topics should be addressed separately and supports instead a tailored identity theft bill addressing consumer notification of security breaches.

There are a number of comprehensive bills currently before Congress, including:

- S. 1332, which contains provisions on enhancing punishment for and combating identity theft, regulating data brokers to require transparency and accuracy in records as well as error resolution processes, extending the requirement for data privacy and data security programs to non-financial companies, requiring consumer notification of security breaches, and restricting the solicitation, use, sale, purchase and display of Social Security numbers;
- S. 1408, which contains provisions extending the requirement for data security programs beyond financial institutions, requiring consumer notification of security breaches, requiring procedures for the placement, removal and temporary suspension of security freezes on credit reports, and restricting the solicitation, use, sale, purchase and display of Social Security numbers; and
- S. 768, which contains provisions on identity theft prevention including the establishment of a new Office of Identity Theft within the FTC, data security, privacy, breach notification and Social Security number protection.

These bills, however, by virtue of their breadth and complexity, are likely to move more slowly through Congress and gaining sufficient support for their far-ranging provisions is likely to prove difficult at best. In recognition of this, Senator Spector, the sponsor for S. 1332, introduced a follow-up bill, S. 1789, which is generally structured like the earlier version but eliminates the Social Security number restrictions and certain other provisions for combating identity theft. Bills that are even narrower still—such as S. 1326 and H.R. 4127, which focus mainly on data security and breach notification—are even more likely to move through Congress.

Preemption. Preemption is a critical issue for both industry and consumer groups alike. Industry groups and federal regulators[92] argue that the current patchwork of state laws is unworkable and should be replaced with a single, nationwide standard for data security. Here the interests of both industry and federal regulators are aligned, and both support a federal standard that completely preempts state data security and data privacy laws. With respect to consumer breach notification, such broad preemption provisions can be found in a number of the bills before Congress:

- S. 1408 generally preempts any state or local law that requires a covered entity, or imposes liability on a covered entity for the failure "(1) to develop, implement, maintain or enforce information security programs to which [the] Act applies; or (2) to notify individuals of breaches of security pertaining to them."
- H.R. 3997 supersedes any state or local law with respect to the responsibilities of any person "(A) to protect the security or confidentiality of information on consumers maintained by or on behalf of the person; (B) to safeguard such information from potential misuse; (C) to investigate or provide notices of any unauthorized access to information concerning the consumer, or the potential misuse of such information, for fraudulent purposes; (D) to mitigate any loss or harm resulting from such unauthorized access or misuse; or (E) involving restricting credit reports from being provided, or imposing any requirement on such provision, for a permissible purpose pursuant to section 604 . . . ."
- S. 1326 supersedes any state or local law "that relates in any way to electronic information security standards or the notification of any resident of the United States of any breach of security pertaining to any collection of personal information about such resident."
- S. 1789 supersedes any state or local law "relating to notification of a security breach" except that a state can require inclusion of information about victim protection assistance in a breach notification letter.

Consumer groups and state attorneys general counter that these broad preemption provisions may provide inadequate protection for state residents. Federal law, they contend, should be a floor not a ceiling. To this end, they support preemption provisions such as those in S. 751 and S. 768 which preempt only inconsistent state laws and then only to the extent of the inconsistency, thereby permitting more protective state laws.

H.R. 4127 tries a compromise position. On the one hand, it contains a broad preemption provision superseding state or local laws that expressly require information security practices or notification to individuals of a security breach. On the other hand, it expressly carves out from preemption the enforcement of any state consumer protection law by a state attorney general as well as state laws regarding trespass, contracts, torts or fraud.

Notification Trigger. Setting the trigger for consumer notice is one of the most contentious points of debate in framing a breach notification law: set the trigger too low and covered entities will be overburdened with notification requirements and the public will be overwhelmed with notices; set it too high, and the public will not be informed about breaches that could lead to identity theft.

From the industry perspective, the issue is critical and affects their bottom line in direct and indirect ways. In addition to the cost of sending out customer breach notices,[93] the related public relations costs, and the likely dip in stock value,[94] a recent study by the Ponemon Institute found that sending out a customer breach notice can seriously impact an entity's customer base.[95] According to that survey, among respondents who had received a security breach notice:

- 19 percent had severed ties with the organization as a result of the breach, and an additional 40 percent were considering taking such action; and
- 58 percent experienced decreased trust and confidence in the organization.

In light of these concerns, industry groups support a trigger that ties notice to a significant risk of harm or misuse of the compromised information. Privacy proponents, including state attorneys general, on the other hand, object to a subjective trigger that gives the entity suffering a breach discretion to determine whether breach notices must be sent and favor a standard, like the California standard, that requires notification upon the mere access or acquisition of covered information.[96] They claim that requiring entities to notify consumers in the event of **any** security breach will encourage companies to improve security safeguards.

Most of the bills currently before Congress contain some form of a risk trigger, although the exact formulation varies.

- *Reasonable Risk:* S. 1408 requires consumer notice if an entity determines that a security breach creates a reasonable risk of identity theft.[97] A "reasonable risk" would exist where the preponderance of the evidence

available to the company shows that identity theft is "foreseeable" for one or more individuals affected by the breach. H.R. 3997 also uses a reasonable risk formulation, but tightens it by requiring consumer notice if sensitive financial identity information has been or is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates to commit identity theft or to make fraudulent transactions on the consumers' accounts. Following a manager's amendment, the risk trigger in H.R. 4127 was also changed from a significant risk trigger to a reasonable risk trigger. As amended, H.R. 4127 would require consumer notification unless there is no reasonable risk of identity theft, fraud or other unlawful conduct.

- *Significant Risk:* S. 1789 exempts an entity from consumer notice if it concludes that there is no significant risk of harm to individuals, notifies the U.S. Secret Service in writing, and the Secret Service does not indicate that consumer notice must be given. On the other hand, S. 1326 **requires** consumer notice if an entity determines that there **is** a significant risk of identity theft.
- *De Minimus Risk:* S. 1332 exempts an entity from consumer notice if the entity conducts a risk assessment in consultation with federal law enforcement and the attorney general of each affected state and concludes that there is a de minimus risk of harm to individuals.
- *Misuse Unlikely:* H.R. 3140 requires consumer notice unless an entity concludes that misuse of the information is unlikely to occur.

It is unlikely that a breach notice law could be passed without some form of trigger. Rather, the question is whether the trigger will be based on a "reasonable" risk or a "significant" risk of harm or misuse. Bills that, like S. 1789, incorporate a higher standard for notification but include provision for oversight by or consultation with a federal entity could strike a balance between industry's concern regarding over notification and privacy advocates' concern that industry will make self-serving determinations to avoid providing consumer notice.

Enforcement and Penalties for Non-compliance. Another point of contention is determining who has standing to enforce compliance or pursue civil actions for violations of the bills. Industry proponents favor an enforcement mechanism that vests exclusive enforcement authority in federal regulators. Allowing state enforcement of federal data security laws, they argue, would provide a back door for de facto state regulation. State attorneys general and privacy proponents counter that states must have enforcement authority because federal regulators lack the resources to aggressively pursue violations that impact state residents.

Most of the bills that have made any movement in Congress permit state attorneys general to pursue civil actions against violators to some degree or another. Some bills, like S. 1789, limit state attorneys general to seeking an injunction or civil penalties, while others, such as S. 1326 and 1332, permit them to seek actual, or even punitive, damages. S. 1408 may provide a compromise: it vests exclusive enforcement authority with the OCC, Federal Reserve Board, FDIC, OTS, National Credit Union Administration, Securities and Exchange Commission, and state insurance authorities for entities falling within their jurisdiction and permits state attorneys general to bring civil actions against other entities that are subject to the general catch-all jurisdiction of the FTC.

Nuts-And-Bolts. Although generally less contentious, provisions detailing the nuts-and-bolts of compliance—including timing for notification, permitted methods of delivery of consumer notices, content requirements and safe harbors to name but a few—must also be settled before a data breach law can be passed.

Conclusion

Industry has been pushing for an early consideration of the federal data security breach notification bills as more and more state data security laws have taken effect.[98] This push is motivated in part by the practical political reality that the longer the federal bills stagnate, the more difficult it will likely be to gain the passage of a data security bill that will adequately protect industry from overly burdensome notification requirements. Meanwhile, the number of states with data security breach notification laws continues to grow. Nine states have already enacted or amended data security breach notification laws this year, and legislation is pending in a number of additional states.

But the question remains: Will any of the federal bills finally gain the momentum necessary for passage? Much depends on external circumstances. If another large security breach erupts, the passage of a data security law is more likely. Absent such a breach and as more and more state data security laws become effective, congressional members may feel torn between the need for national standards and voting for a preemptive federal measure that contains lower standards for notification than their home state's laws.

NOTES

1. The FTC's agreement with ChoicePoint requires payment an unprecedented $10 million in civil penalties and creation of a $5 million consumer redress fund. *See* FTC News Release, *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm.
2. As of the beginning of May 2006, the states that have enacted breach notification laws are: Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Wisconsin and Washington.
3. This year, Utah's governor signed a security freeze bill that would require the fastest time for implementing a temporary suspension of a security freeze. The bill would require a consumer reporting agency to temporarily lift a freeze within fifteen minutes of a consumer's request (as opposed to the three day requirement in the laws of most states).
4. The Banking Agencies include the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS).
5. *See* http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20050323/default.htm. In 2004, the Federal Trade Commission had released guidance for businesses regarding how to respond to data security breaches and when to notify customers and other entities following a breach. This guidance is available at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm.
6. Authentication in an Internet Banking Environment, *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf.
7. Interagency Guidelines Establishing Information Security Standards, Small Entity Compliance Guide, *available at* http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/attachment.pdf.
8. In the Matter of CardSystems Solutions, Inc., Agreement Containing Consent Order, *available at* http://www.ftc.gov/os/caselist/0523148/0523148consent.pdf.
9. In the Matter of DSW Inc., Decision and Order, *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWDecisionandOrder.pdf.
10. In the Matter of BJ's Wholesale Club, Inc., Decision and Order, *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.
11. Cal. Civ. Code § 1798.82.
12. *See, e.g.,* Chronology of Data Breaches posted by Privacy Rights Clearinghouse, *available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm.
13. Ga. Code Ann. § 10-1-910 *et seq.*
14. Me. Rev. Stat. Ann., tit. 10, § 1346 *et seq.*
15. Me. Public Law, Ch. 583 (122nd Leg.).
16. Ind. Code § 4-1-11 *et seq.*
17. Ind. Code § 24-4.9-1 *et seq.* (effective July 1, 2006).
18. *See, e.g.,* Ariz. Bill 1338, § 44-7501(F) (exemption for person that complies with the notification requirements or security breach procedures pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator); Colo. H.B. 06-1119, § 6-1-716(3)(b) (exemption for entity regulated by state or federal law and that maintains procedures for a breach of security pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator); 2005 Conn. Acts. 148, § 3(f) (exemption for persons that maintain security breach procedures pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional regulator as defined in 15 U.S.C. § 6809(4)); De. Code Ann.. tit. 6, § 12B-103(b) (exemption for entities subject to regulation by state or federal law that maintain security breach procedures subject to laws, rules, regulations, or guidelines established by their primary or functional regulator); Fla. Stat. Ann. § 817.568(9)(b) (exemption for entities that maintain notification procedures pursuant to the rules, regulations, procedures, or guidelines established by their primary or functional federal regulator); Idaho S.B. 1374, § 28-51-106(2) (exemption for entities regulated by state or federal law and that maintain and comply with procedures for a breach of security pursuant to the laws, rules, regulations, guidances, or guidelines established by their primary or functional state or federal regulator); Kansas Bill 196, § 4(e) (exemption for entities regulated by state or federal law and that maintain procedures for a breach of security pursuant to the laws, rules, regulations, guidances, or guidelines established by their primary or functional state or federal regulator); Nebr. L.B. 876, § 4(2) (exemption for entities that are regulated by state or federal law and that maintain procedures for a breach of security pursuant to the laws, rules, regulations, guidances, or guidelines established by their primary or functional state or federal regulators); Ohio Rev. Code § 1349.19(F)(1) (exemption for financial institutions, trust companies, or credit unions, or any of their affiliates that are required by federal law, including but not limited to federal statutes, regulations, regulatory guidance, or other regulatory action, to notify customers of an information security breach with respect to information about those customers and that are subject to examination by their functional government regulatory agency for compliance with the applicable federal law); Pa. S.B. 712, § 7(b)(2) (exemption for entities that comply with notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional Federal regulator); R.I. Gen. Laws § 11-49.2-7 (exemption for entities that maintain security breach procedures pursuant to the rules, regulations, procedures or guidelines established by their primary or functional regulator); Utah Rev. Code Ann. § 13-42-202(5)(c) (exemption for persons that are regulated by state or federal law and that maintain procedures for a breach of system security under applicable law established by their primary state or federal regulators).
19. Ariz. Bill 1338, § 44-7501(J)(exemption for persons subject to Title V of the GLBA and covered entities under HIPAA); Ind. Code § 24-4.9-3 (exemption for data base owners that maintain their own disclosure procedures as part of a security policy or compliance plan under the USA Patriot Act, Executive Order 13224, the federal Driver's Privacy Protection Act, the federal Fair Credit Reporting Act, the GLBA, or the federal Health Insurance Portability and Accountability Act (HIPAA)); Minn. Stat. § 325E.61(4) (exemption for financial institutions as defined in the GLBA and entities subject to federal privacy and security regulations under HIPAA); 2005 Nev. Stat. §24(5)(b) (exemption for entities subject to and in compliance with the security provisions of the GLBA); R.I. Gen. Laws § 11-49.2-7 (exemption for providers of health care, health care service plan, health insurers, or covered entities governed by the medical privacy and security rules issued under HIPAA); Tenn. Code § 47-18-2107(i) (exemption for any persons subject to Title V of the GLBA); 2005 Wisc. Act 138, § 3m (exemption for (i) entities that are subject to and in compliance with the privacy and security requirements of the GLBA or persons that have contractual obligations to such entities if the entities or persons have in effect policies concerning breaches of information security; and (ii) health plans, health care clearinghouses, and health care providers if the entities comply with 45 C.F.R part 164).

20. La. Rev. Stat. Ann. § 3076 (exemption for financial institutions subject to and in compliance with Banking Agencies Interagency Guidance on Response Programs); N.C. Gen. Stat. § 75-65(h) (same); N.D. Cent. Code § 51-30-06 (exemption for financial institutions, trust companies or credit unions subject to , examined for, and in compliance with "the federal interagency guidance on response programs for unauthorized access to customer information and customer notice"); Pa. S.B. 712, § 7(b)(1) (same); R.I. Gen. Laws § 11-49.2-7 (same).

21. *See, e.g.,* Ark. Code Ann. § 4-110-106(a) (exemption for entities regulated by state or federal law that gives greater protection to personal information and at least as thorough disclosure requirements for security breaches); Me. Public Law, Ch. 583 (122nd Leg.), §12 (exemption for persons that comply with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal or state law as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of the state breach notification law). Maine's original breach notification law did not contain a regulated entity exception, and this exception is not effective until January 31, 2007.

22. Ariz. Bill 1338, § 44-7501(E); Ark. Code Ann. § 4-110-105(f); Cal. Civ. Code § 1798.82(h); Colo. H.B. 06-1119, § 6-1-716(3)(a); 2005 Conn. Acts 148, § 3(f); De. Code Ann. Tit. 6, 12B-103(a); Fla. Stat. Ann. § 817.5681(9)(a); Ga. Code Ann. 10-1-911(3); Idaho S.B. 1374, § 28-51-106(1); Ill. Comp. Stat. 530/1; Ind. Code § 24-4.9-3; Kansas Bill 196, § 4(d); La. Rev. Stat. Ann. § 51:3074(F); Minn. Stat. § 325E.61(1)(i)(h); Mont. Code Ann. § 30-14-1704(6); Nebr. L.B. 876, § 4(1); 2005 Nev. Stat. 485, § 24(5)(a); A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-163; N.D. Cent. Code § 51-30-06; Pa. S.B. 712, § 7(a); R.I. Gen. Laws § 11-49.2-7; Tenn. Code § 47-18-2107(f); Tex. Bus. & Comm. Code Ann. § 48.103(g); Wash. Rev. Code § 19.255.010(8); Utah Rev. Code Ann. § 13-42-202(5)(b).

23. Ind. Code § 24-4.9-3 ("data base owner's security policy must be "at least as stringent as the disclosure requirements" under state law).

24. Ariz. Bill 1338, § 44-7501(E); A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-163; Pa. S.B. 712 § 7(a).

25. Although some states use other terms such as "sensitive information" to denote covered information for purposes of this discussion, "personal information" is intended to mean covered information.

26. *See, e.g.,* Ariz. Bill 1338, § 44-7-501(L)(7); Ark. Code Ann. § 4-110-103(7); Cal. Civ. Code § 1798.82(e); Colo. H.B. 06-1119, § 6-1-716(d)(I); 2005 Conn. Acts 148, § 3(a); De. Code Ann., tit. 6, § 12B-101(4); Idaho S.B. 1374, § 28-51-104(5); La. Rev. Stat. Ann. § 51:3073(4); Minn. Stat. § 325E:61(1)(e); Mont. Code. Ann. § 30-14-1704(4)(a); Nebr. L.B. 876, § 2(5); 2005 Nev. Stat. 485 § 21; Ohio Rev. Code § 1349.19(A)(7); Pa. S.B. 712, § 2; R.I. Gen. Laws 11-49.25; Tenn. Code § 47-18-2107; Tex. Bus. & Comm. Code Ann. § 48.002(2); Utah Code Ann. 1953 § 13.42-102; Wash. Rev. Code § 19.255.010(5); . *Cf.* A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-161(1) (similar to above, but, providing that disassociated data that, if linked would constitute personal information, is personal information if the means to link the data is also accessed).

27. *See, e.g.,* Ga. Code Ann. § 10-1-911(5) ((i)account numbers are data elements by themselves if they can be used without other information such as password or access code and (ii) password, access code, or PIN are independent data elements); 815 Ill. Comp. Stat. 530/1; Me. Rev. Stat. Ann., tit. 10 § 1347(6) ((i)account numbers are data elements by themselves if they can be used without other information such as password or access code and (ii) password, access code, or PIN are independent data elements); Kansas Bill 196, § 3(g); N.C. Gen. Stat. § 75-65(10) (also adding data elements); 2005 Wisc. Act 138, § 1 (also adding data elements). Indiana's new law is a hybrid, specifying that a person's name in combination with credit card number alone is personal information, but if other financial account numbers or debit card numbers are at issue, then, the person's name plus those account numbers would not be personal information unless combined with any required security code, access code, or password. Ind. Code § 24-4.9-2.

28. *See, e.g.,* Ark. Code Ann. § 4-110-103(7) (additional data element – medical information); N.C. Gen. Stat. § 75-65(10) (additional data elements – employer taxpayer ID number, passport number, digital signature, biometric data, fingerprints, and any other numbers or information that can be used to access a person's financial resources); Nebr. L.B. 876, § 2(5) (additional data elements – unique electronic identification number or routing code, in combination with any required security code, access code or password; and unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation); N.D. Cent. Code § 51-30-01(2) (additional data elements – date of birth, mother's maiden name, employee identification number, digitized or other electronic signature); 2005 Wisc. Act 138, § 1 (additional data elements – DNA profile and unique biometric data including fingerprints, voiceprints, retina or iris images or any other unique physical representation).

29. A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), 899-aa.

30. Ga. Code Ann. § 10-1-911(5); Me. Rev. Stat. Ann., tit. 10 § 1347(6). Under Maine's amended breach notification law (effective in January 2007), information from third party claims databases maintained by property and casualty insurers is carved out of the definition of "personal information." Me. Public Law, Ch. 583 (122nd Leg.), § 4.

31. Ind. Code § 24-4.9-2.

32. A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-161(1)

33. Ind. Code § 24-4.9-3; A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899-aa; N.C. Gen Stat. § 75-61(14); Pa. S.B. 712, § 3.

34. *See, e.g.,* Ark. Code. Ann. 4-110-103(7); Cal. Civ. Code § 1798.82(e); Colo. H.B. 06-1119, § 6-1-716(d)(I); De. Code Ann., tit. 6, § 12B-101(4); Ga. Code Ann. § 10-1-911(5); Idaho S.B. 1374, § 28-51-106(1); 815 Ill. Comp. Stat. 530/2; Kansas Bill 196 § 3(g); La. Rev. Stat. Ann. § 51:3073(4); Me. Rev. Stat. Ann., tit. 10, § 1347(6); Minn. Stat. § 325E.61(e); Mont. Code Ann. § 30-14-1704(4)(a); Nebr. L.B. 876, § 2(5); A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005) § 899-aa(1)(b); R. I. Gen. Laws § 11-49.2-5; Tenn. Code § 47-18-2107; Utah Code Ann. 1953 § 13.42-102; Wash. Rev. Code § 19.255.010(5).

35. *See, e.g.,* 2005 Nev. Stat. 485, § 21; N.D. Cent. Code § 51-30-01(2); Tex. Bus. & Comm. Code Ann. § 48.002(2).

36. Ariz. Bill 1338, § 44-7501(L)(7); Fl. Stat. Ann. § 817.5681(5); Ind. Code § 24-4.9-2,§ 10(2); Ohio Rev. Code § 1349.19(A)(7); Pa. S.B. 712, § 2; 2005 Wisc. Act 138, § 1.

37. N.C. Gen. Stat. § 75-65(a).

38. Ind. Code § 24-4.9-2.

39. 2005 Wisc. Act 138.

40. *See, e.g.,* Cal. Civ. Code § 1798.82; 815 Ill. Comp. Stat. 530/1 *et seq.;* Me. Rev. Stat. Ann., tit. 10, § 1346 *et seq.;* Minn. Stat. § 325E.61 and § 609.891; 2005 Nev. Stat 485; A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005); N.D. Cent. Code § 51-30-01 *et seq.;* 2005 Tenn. Pub. Acts 473; Tex. Bus. & Comm. Code Ann. § 48.001 *et seq.*

41. *See, e.g.,* 2005 Nev. Stat 485; Tenn. Code § 47-18-2107(a)(1).

42. *See, e.g.,* Ariz. Bill 1338, § 44-7501(L)(1); Ark. Code Ann. 4-110-105; 2005 Colo. H.B. 06-1119, § 6-1-716(2); Conn. Acts 148; De. Code Ann. Tit. 6, 12B-102(a); Fla. Stat. Ann. § 817.5681(1)(a); Ind. Code § 24-4.9-3; Kansas Bill 196, § 3(h); La. Rev. Stat. Ann. § 51:3074(G); Me. Public Law, Ch. 583 (122nd Leg.), § 6 (effective January 2007); Mont. Code Ann. § 30-14-1704; Nebr. L.B. 876, § 3(1); N.J. Stat. Ann. § 56:8-161(12)(a); N.C. Gen. Stat. § 75-61(14); Ohio Rev. Code § 1349.19(A); Pa. Sen. Bill No. 712 (Printer's No. 1410); R.I. Gen. Laws § 11-49.2-4; Utah Code Ann. 1953 § 13-42-202; Utah Code Ann. 1953 § 13-42-202; Wash. Rev. Code § 19.255(d); 2005 Wisc. Act 139, § 895.507(2).). Maine's original breach notification law, which applied only to information brokers, did not contain a misuse threshold. Maine's revised law similarly does not contain a misuse threshold for notification by information brokers, however, it incorporates a misuse threshold applicable to notification by persons other than information brokers. Me. Public Law, Ch. 583 (122nd Leg.), § 6. The revised law becomes effective January 31, 2007.

43. Ind. Code § 24-4.9-3 (notification required if data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft or fraud affecting the Indiana resident); Kansas Bill 196, § 3(h) (security breach defined to include only an incident "that causes, or [that] such individual or entity reasonably believes has caused or will cause, identity theft to any consumer").

44. De. Code Ann. Tit. 6, 12B-102(a) (notice required only if the entity's "investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur. . ."); Idaho S.B. 1374, § 28-51-105(1) (notice required if an "investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur"); Me. Public Law, Ch. 583 (122nd Leg.), § 6 (for persons other than "information brokers", notice required "if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur"); Nebr. L.B. 876, § 3(1)(notice required if investigation determines that "use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur"); N.C. Gen. Stat. § 75-61(14) (defining "security breach" to only include an incident in which "illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer"); Utah Code Ann. 1953 § 13-42-202 (notice required if an investigation reveals that the misuse of personal information for identity theft or fraud purposes has occurred or is reasonably likely to occur). Idaho further limits the circumstances in which notice is required by defining a security breach to only include "the *illegal* acquisition of unencrypted computerized data that *materially* compromises the security, confidentiality, or integrity of personal information." Idaho S.B. 1374, § 28-51-104(2) (emphasis added).

45. Ohio Rev. Code § 1349.19(A) (defining "security breach" to only include incident that "causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state"); 2005 Wisc. Act 139, § 895.507(2) (Notice is not required if the "acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.").

46. R.I. Gen. Laws § 11-49.2-4 (Notification "is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired.").

47. Ariz. Bill 1338, § 44-7501(c)(1) (defining "security breach" to include only an incident that "materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual"); Pa. Sen. Bill No. 712 (Printer's No. 1410) (defining "security breach" to only include incident "that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth."); Mont. Code Ann. § 30-14-1704 (defining a "security breach" to only include an incident that "causes or is reasonably believed to cause loss or injury to a Montana resident").

48. N.J. Stat. Ann. § 56:8-161(12)(a) ("Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible.").

49. Wash. Rev. Code § 19.255(d) ("A person or business under this section shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.").

50. 2005 Conn. Acts 148 (Notification "shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."); Fla. Stat. Ann. § 817.5681(1)(a) (Notification "is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information had been acquired and accessed."). Florida further limits the circumstances in which notice is required by defining a security breach to include only the "*unlawful* and unauthorized acquisition of computerized data that *materially* compromises the security, confidentiality, or integrity of personal information maintained by the person." Fla. Stat. Ann. § 817.5681(4) (emphasis added).

51. Colo. H.B. 06-1119, § 6-1-716(2) (Notification is not required if "the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur."); Ark. Code Ann. 4-110-105 (Notification "is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers."); La. Rev. Stat. Ann. § 51:3074(G) (Notification "is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.").

52. 2005 Conn. Acts 148 (requiring "an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement").

53. Fl. Stat. Ann. § 817.5681 § 10(a) ("determination [of no risk] must be documented in writing and the documentation must be maintained for 5 years"); N.J. Stat. § 56:8-161(12)(a) ("Any determination [of no risk] shall be documented in writing and retained for five years). Under Florida law, the failure to document and retain documentation for a no-risk determination could subject an entity to a fine of up to $50,000. Fl. Stat. Ann. § 817.5681(10)(b).

54. The following states require notification of consumer reporting agencies if over:

- 500 consumer notices are provided at one time. Minn. Stat. § 325E.61(2);
- 1,000 consumer notices are provided at one time: Colo. H.B. 06-1119, § 6-1-716(2)(d); Fla. Stat. Ann. § 817.5681(12); Ind. Code § 24-4.9-3; Kansas Bill 196, § 4(f); Me. Rev. Stat. Ann., tit. 10, § 1348(4); 2005 Nev. Stat. 485 § 24(6); A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-163; N.C. Gen. Stat. 75-65(f); Ohio Rev. Code § 1349.19(6); Pa. S.B. 712, § 5; Tenn. Code § 47-18-2107(g); 2005 Wisc. Act 138. Colorado, however, excludes persons subject to Title V of the GLBA from this notification requirement.
- 5,000 consumer notices are provided at one time: A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(8)(b);
- 10,000 consumer notices are provided at one time: Ga. Code Ann. § 10-1-912(d); Tex. Comm. & Bus. Code § 48.103(h).

55. Mont. Code Ann. § 30-14-1704(7).

56. Me. Rev. Stat. Ann., tit. 10, § 1348(5).

57. A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-163.

58. A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(8).

59. N.C. Gen. Stat. § 75-65(f).

60. *See, e.g.,* Ariz. Bill 1338, § 44-7501(A); Ark. Code Ann. § 4-110-105(a)(2); Cal. Civ. Code § 1798.82(a); Colo. H.B. 06-1119, § 6-1-716(2)(a); 2005 Conn. Acts 148, § 3(b); De. Code Ann., tit. 6, § 12B-102(a); Ga. Code Ann. § 10-1-912(a); Idaho S.B. 1374, § 28-51-105(1); Ill. Comp. Stat. 530/10; La. Rev. Stat. Ann. § 51:3074(c); Ind. Code § 24-4.9-3; Kansas Bill 196 § 4(a); Me. Rev. Stat. Ann., tit. 10, § 1348(1); Minn. Stat. § 325E.61(a); Mont. Code Ann. § 30-14-1704(1); Nebr. L.B. 876, § 3(1); 2005 Nev. Stat. 485 § 24(1); A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-163; A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(2); N.C. Gen. Stat. § 75-65(a); N.D. Cent. Code § 51-30-02; Pa. S.B. 712, § 3; R.I. Gen. Law, § 11-49.2-3(a); Tenn. Code § 47-18-2107; Tex. Bus. & Comm. Code Ann. § 48.103(b); Wash. Rev. Code § 19.255.010(1); Utah Code Ann. 1953 § 13-42-202(2).

61. Fla. Stat. Ann. § 817.5681(1)(A); Ohio Rev. Code § 1349.19(B)(2); Wisc. Stat. § 895.507(3).

62. Wisconsin specifies that notice must be provided by mail or by a method that the entity has previously used to communicate with the subject. So, if an entity has used email or the telephone to communicate with consumers, presumably those means of communication could also be used to provide consumer notification. 2005 Wisc. Act 138.

63. Arizona and Colorado permit electronic notice if the notice is consistent with E-SIGN or if the primary means of communication by the entity with the resident is by electronic means. Ariz. Bill 1338, § 44-7501(D)(2); Colo. H.B. 06-1119, § 6-1-716(1)(c).

64. Ohio Rev. Code § 1349.19(E).

65. Pa. S.B. 712 § 2.

66. A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(5).

67. *Id.*

68. For states that permit telephonic notice, see, Ariz. Bill 1338, § 44-7501(D)(3); Colo. H.B. 06-1119, § 6-1-716(1)(c); 2005 Conn. Acts 148 § 3(e); De. Code Ann., tit. 6, § 12B-101(3); Idaho S.B. 1374, § 28-51-104(4); Ind. Code 24-4.9-3; Mont. Code Ann. § 30-14-1704(5)(a)(iii); Nebr. L.B. 876, § 2(4)(b); A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(5); N.C. Gen. Stat. § 75-65(e); Ohio Rev. Code § 1349.19(E); Pa. S.B. 712, § 2; Utah Rev. Code Ann. § 13-42-202(5)(a). Wisconsin could permit telephonic notice provided that the entity has previously used the telephone to communicate with the subject. 2005 Wisc. Act 138.

69. A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(5).

70. N.C. Gen. Stat. § 75-65(e).

71. Pa. S.B. 712, § 2.

72. Utah Rev. Code Ann. § 13-42-202(5)(a).

73. Utah. Rev. Code Ann. 1953 § 13-42-202(g)(a)(iv).

74. *See, e.g.,* Ariz. Bill 1338, § 44-7501(D)(4) (threshold set at $50,000 cost of notice or 100,000 individuals notified); Colo. H.B. 06-1119, § 6-1-716(1)(c)(IV) (threshold set at $250,000 cost of notice or 250,000 individuals notified); De. Code Ann., tit. 6, § 12B-101(3) (thresholds set at $75,000 cost of notice or 100,000 individuals notified); Idaho S.B. 1374, § 28-51-104(4)(d)(threshold set at $25,000 cost of notice or 50,000 individuals notified); Kansas Bill 196, § 3(c)(3) (threshold set at $100,000 cost of notification or 5,000 individuals notified); Me. Rev. Stat. Ann., tit. 10§1347(4)(c) (thresholds set at $1,000 cost of notice or 1,000 individuals notified); Nebr. L.B. 876, § 2(4)(d)(thresholds set at $75,000 cost of notice and 100,000 individuals notified); Pa. S.B. 712, § 2 (thresholds set at $100,000 cost of notice or 175,000 individuals notified); R.I. Gen. Laws § 11-49.2-6(d) (thresholds set at $25,000 cost of notification or 50,000 individuals notified).

75. Ark. Code Ann § 4-110-105(e)(3)(A); Cal. Civ. Code § 1798.82(g)(3); 2005 Conn. Acts 148 § 3(e); Fla. Stat. Ann. § 817.5681(6)(c); Ga. Code Ann. § 10-1-911(3); Ill. Comp. Stat. 530/10; Ind. Code § 24-4.9-3; La. Rev. Stat. Ann. § 51:3074(E)(3); Minn. Stat § 325E.61(1)(g)(3); Mont. Code Ann. § 30-14-1704(5)(a)(iv); 2005 Nev. Stat. 485, § 24(4)(c); A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-163; A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(5); N.C. Gen. Stat. § 75-65(e)(4) (also adding inability to identify particular affected persons as basis for providing substitute notice); N.D. Cent. Code § 51-30-05(3); Ohio Rev. Code § 1349.19(E)(4); Tenn. Code § 47-18-2107(e); Tex. Bus. & Comm. Code § 48.103(f); Wash. Rev. Code § 19.255.010(7)(c).

76. Ariz. Bill 1338, § 44-7501(D)(4); Ark. Code Ann § 4-110-105(e)(3)(A); Cal. Civ. Code § 1798.82(g)(3); Colo. H.B. 06-1119, § 6-1-716(1)(c)(IV); 2005 Conn. Acts 148 § 3(e); Fla. Stat. Ann. § 817.5681(6)(c); Ga. Code Ann. § 10-1-911(3); Idaho S.B. 1374, § 28-51-104(4)(d); Ill. Comp. Stat. 530/10; Kansas Bill 196, § 3(c)(3); La. Rev. Stat. Ann. § 51:3074(E)(3); Me. Rev. Stat. Ann., tit. 10, § 1348(4)(c); Minn. Stat § 325E.61(1)(g)(3); Nebr. L.B. 876, § 2(4)(d); 2005 Nev. Stat. 485, § 24(4)(c); A. 4001, 2005 Leg., 211th Sess. (N.J. 2005), § 56:8-163; A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(5); N.C. Gen. Stat. § 75-65(e)(4); N.D. Cent. Code § 51-30-05(3); Ohio Rev. Code § 1349.19(E)(4); Pa. S.B. 712, § 2; R. I. Gen. Laws § 11-49.2-5; Tenn. Code § 47-18-2107(e); Wash. Rev. Code § 19.255.010(7)(c).

77. Tex. Bus. & Comm. Code Ann. § 48.103(f).

78. Ind. Code § 24-4.9-3.

79. Mont. Code Ann. § 30-14-1704(5)(a)(iv)(b).

80. Ohio Rev. Code § 1349.19(E).

81. *Id.*

82. Nebr. L.B. 876, § 2(4)(e).

83. A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899aa(7).

84. N.C. Gen. Stat. § 75-65(d).

85. 2005 Wisc. Act 138.

86. In some states, enforcement authority is also granted to other state agencies. *See, e.g.,* Fla. Stat. Ann. § 817.5681(b) (granting enforcement authority to the Department of Legal Affairs); Me. Rev. Stat. Ann., tit. 10, § 1349(1) (granting enforcement authority to the appropriate state regulators within the Department of Professional and Financial Regulation for licensed information brokers and otherwise to the state attorney general).

87. *See, e.g.,* Ariz. Bill 1338, § 44-7501(H)(providing for a civil penalty not to exceed $10,000 per breach); Fla. Stat. Ann. § 817.5681(b) (providing for civil fines up to $500,000 for failure to provide notification in the requisite time period and up to $50,000 for a failure to abide by state documentation and document retention requirements); Idaho S.B. 1374, § 28-51-107 (providing for a fine of not more than $25,000 per breach if an entity intentionally fails to give notice); Ind. Code § 24-4.9-3 (providing for civil penalties of not more than $150,000 per deceptive act and recovery of the attorney general's reasonable costs in the investigation and maintenance of the action); Me. Rev. Stat. Ann., tit. 10, § 1349(2) (civil fine of not more than $500 per violation, up to a maximum of $2,500 per day the information broker is in violation); Mont. Code Ann. § 30-14-1705, 30-14-142 (setting forth civil fines including civil fine of $10,000 for each willful violation); A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), § 899-aa(6) (providing civil penalty of the greater of $5,000 or up to $10 per instance of failed notification (up to $150,000 total) for knowing or reckless violation); R.I. Gen. Laws § 11-49.2-6 (setting forth civil penalties of not more than $100 per occurrence and not more than $25,000 total); Tex. Bus. & Comm. Code Ann. § 48.201(a) (setting forth civil penalty of at least $2,000 but not more than $50,000 per violation and authorizing attorney general to recover reasonable expenses including attorney's fees, court costs, and investigatory costs); Utah Code Ann. 1953 § 13-42-301(3) (setting forth civil fines of not greater than $2,500 for a violation or series of violations concerning a specific customer and not greater than $100,000 in the aggregate for related violations concerning more than one customer).

88. *See, e.g.,* Cal. Civ. Code § 1798.84(b) (authorizing private right of action); La. Rev. Stat. Ann. §51:3075 (authorizing civil action to recover actual damages); N. C. Gen. Stat. § 75-65(i) (providing that no private right of action may be brought by an individual *unless* the individual is injured as a result of the violation); Wash. Rev. Code § 19.255.010(10)(a) (authorizing civil action to recover damages).

89. A few states expressly provide that a violation of the breach notification law may constitute a violation of other state law as well or may be evidence of such a violation. *See, e.g.,* 815 Ill. Comp. Stat. 530/1 (violation of the breach notification law constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act). *Cf.* 2005 Wisc. Act 138, § 4 (failure to comply with the section is not negligence or a breach of any duty but may be evidence of negligence or a breach of a legal duty).

90. A number of external events also diverted momentum from the issue of data security, including the two vacancies in the United States Supreme Court and the subsequent confirmation hearings as well as hearings and bills under consideration in the aftermath of Hurricane Katrina and the renewal of the Patriot Act.

91. H.R. 5318 defines a "major security breach" as any security breach involving: (1) the acquisition of personal information about 10,000 or more individuals; (2) databases owned by the Federal Government; or (3) primarily data in electronic form containing personal information about employees or contractors of the Federal Government involved in national security matters or law enforcement.

92. FTC Chairman Deborah Platt Majoras and Comptroller of Currency John Dugan have both argued for broad preemption of state data security laws.

93. According to some estimates, the cost of sending out customer breach notices could run as high as $25 per consumer letter. *See e.g., States Get Clearer Picture of Extent of Data Breaches as New Laws Take Effect,* BNA Banking Report (Feb. 27, 2006), at 439.

94. As reported, Choicepoint "experienced a more than 20% decline in its stock price at one point" following its breach disclosure. *The Challenge of Electronic Data: Corporate Legal Obligations to Provide Information Security,* Wall Street Lawyer, vol. 10 at 7 (March 2006).

95. National Study on Data Security Breach Notification, Sept. 26, 2005, *available at* http://packetstorm.ussrback.com/papers/general/Security_Breach_Survey.pdf.

96. Cal. Civ. Code § 1798.82(a).

97. Sen. George Allen (R-Va) tried to narrow the reasonable risk trigger in S. 1408 to circumstances in which a breach is "more likely than not" to result in identity theft, but the amendment was defeated 8-14.

98. This sense of urgency is further underscored by the shortened federal legislative calendar: this year is an election year, and members of Congress are likely to push for an early adjournment to permit them to campaign.

IF YOU HAVE ANY QUESTIONS OR NEED ADDITIONAL INFORMATION, PLEASE CONTACT:

David Medine +1 202 663 6220 david.medine@wilmerhale.com

J. Beckwith Burr +1 202 663 6695 beckwith.burr@wilmerhale.com

Yoon-Young Lee +1 202 663 6720 yoon-young.lee@wilmerhale.com

Franca Harris Gutierrez +1 202 663 6557 franca.gutierrez@wilmerhale.com

Helen G. Foster +1 202 663 6892 helen.foster@wilmerhale.com

Natacha D. Steimer +1 202 663 6534 natacha.steimer@wilmerhale.com