Security Act ("SB 1386").[9] For the first time, a legislature shattered the aging paradigm and at least implicitly, focused on a first line of defense: securing the systems that store personal information.[10] SB 1386 is unique in that it requires California state government agencies, organizations, and persons that do business in California (collectively referred to as "organizations" herein) to promptly notify California "residents" when they have a reasonable belief that a system breach occurred which possibly exposed data subjects' personal information to third parties.[11] Although SB 1386 has many notable deficiencies, it does provide a good starting point for addressing the issue of security breach notification and maintains a good balance between the interests of corporations and their data subjects.[12]

{4} It is important to understand the background and circumstances that led to the enactment of SB 1386 before analyzing its provisions and impact. Part II of this article will focus on computer security breaches and the resulting rise in identity theft that caused the California legislature to pass this bill. Part III will discuss the creation of SB 1386 and its strengths and weaknesses. Part IV will study efforts to require breach notification at the federal level. Part V will address the curative or protective measures that should be taken by: (1) organizations wishing to avoid a breach; and (2) individuals whose personal information was disclosed as a result of a security breach. Part VI will conclude by finding that using SB 1386 as the template for federal legislation would be unwise, unless the issues discussed herein are addressed.

II. SECURITY BREACHES AND THE RISE OF IDENTITY THEFT

A. Security Breaches

{5} According to one online security firm, the average U.S. company's computer security is attacked by intruders thirty times per week.[13] These intrusions are known as security breaches. What constitutes a security breach will vary depending on the source of the definition. The most generic definition of security breach is a successful attack on a computer system's security controls in order to penetrate the system to acquire or corrupt information on the system, thus disrupting the confidentiality, integrity, or availability of the information on the system.

{6} Security breaches can come from outside an organization – for example, via hackers trying to break into the system. Breaches may also come from inside, typically from disgruntled employees, embezzlers, or even system administrators who have viewed information they are not authorized to access.[14] To date, most breaches come from within organizations. Employees either exploit their legitimate access to data or exceed their authority to view data otherwise restricted by company policy. There is evidence, however, that this trend is changing.[15]

{7} A large part of the problem is that computer security is not viewed as a priority by many organizations. More importantly, it is not viewed as a priority by the people who authorize funding of security initiatives within organizations. There is not a strong organizational culture of data security throughout many organizations, even though they maintain or have access to the personal data of millions of Americans. This is due in part to the relative 'newness' of the electronic age, but . . . [is] more attributable to the absence of law and policy that would require organizations to take seriously the issues of data security and policy.[16]

For example, although eighty-percent of the companies participating in one study reported that

they had a security policy in place, only forty-seven percent said that this policy was embraced by line and functional leaders.[17]

{8} There are commonly two types of security breach victims.[18] The first is the person or organization that suffers from the breach and the second is the data subject whose personal information is contained on the system that was attacked. Generally, the data subject is a consumer who provided information to a business in order to purchase goods or obtain some other service, but might also be an employee whose personal information was provided to an employer to secure employment or employee benefits, or a patient at a hospital or doctor's office, or even a law firm's client.

{9} As noted above, the purpose of most malevolent breaches is to gain access to information. Sometimes breaches are, however, designed to gain an unfair advantage in the marketplace. Other times, and with growing frequency, the purpose of security breaches is to access personal information to commit identity theft.

B. The Rise of Identity Theft

{10} Identity theft is the taking of another person's social security number, date of birth, or other personal information for the purpose of assuming the data subject's identity in order to secure goods and services on the data subject's accounts.[19] Identity thieves may also use the victim's information to secure employment or apply for government services.[20] Credit reporting agencies reported a rise in identity theft cases from 35,235 in 1992 to 522,922 in 1997.[21]

{11} The FTC reported that identity theft complaints nearly doubled between 2001 and 2002.[22] In 2002, the FTC reported receiving 218,714 reports of possible or actual identity theft.[23] The U.S. Department of Justice estimates that as many as 700,000 U.S. consumers may fall prey to identity theft each year.[24] These complaints account for forty-three percent of the consumer fraud complaints filed.[25] A nationwide study conducted in 2002 revealed that one in twenty people was a victim of identity theft.[26] According to the U.S. Treasury, the cost of this illegal conduct is between two and three billion dollars per year for credit cards alone.[27]

{12} Varying estimates have been given for the amount of "out of pocket" expenses that afflict the average victim of identity theft.[28] The range is anywhere from $800.00 to $1,100.00.[29] The following additional identity theft damages have been noted: personal time spent fixing problems with personal accounts, loss of productivity, emotional distress, higher mortgage and interest rates, lack of purchasing power, and loss of vacation time spent dealing with theft issues.[30] The personal time the average victim spends attempting to restore his identity[31] is 175 hours.[32]

{13} Victims usually do not discover that someone has stolen their identity until fourteen months after the information is acquired.[33] Once discovered, it can take years to clear up identity theft issues.[34] Part of the problem is that merchants rarely tell customers about breaches voluntarily.[35] Instead, they wait for customers to complain about unauthorized activities.[36] The result of businesses withholding information from the public is that the government is less equipped to get an overall understanding of where resources should be applied, thus making the nation more vulnerable to cyber-attacks.[37] Moreover, if organizations do not report breaches to law enforcement authorities, the hackers remain in obscurity, free to act with impunity. In an

effort to curb computer security breaches and to empower victims of identity theft, the State of California enacted the first state computer security breach notification legislation in the United States.

III. THE CREATION OF AND REACTION TO SB 1386

{14} SB 1386 has become a hot topic in security and business circles nationwide.[38] One author believes that because of California's size and leading role in the high-tech industry, SB 1386 "could create a de facto national disclosure policy" even absent the passage of federal legislation on the subject.[39] Others have noted that this law could have a global effect.[40] In order to understand the circumstances that led to the passage of this law, it is important to understand its history.

A. History of SB 1386

{15} On April 2, 2002, the Stephen P. Teale Data Center ("Data Center"), a state-operated data storage facility[41] in California, was breached by an unknown attacker.[42] The Data Center houses social security numbers, first and middle initials, last names, and payroll deduction amounts on full and part-time California state employees.[43] The personal information of all 265,000 state employees was potentially exposed during the breach.[44] Although the Data Center breach occurred on April 5, 2002, it was not discovered until May 7, 2002, and employees were not notified until May 21, 2002.[45] The breach was discovered during routine maintenance on the system on May 7.[46] According to Kathleen Connell, the Controller for the State of California, the Controller's Office then directed the Data Center to "disconnect" the computer that had been breached.[47] At that point, the Controller's Office's representative on the Sacramento Valley Hi Tech Crime Task Force was notified of the breach.[48] The Task Force then took control of the criminal investigation.[49] The Task Force then advised the Data Center to determine whether any information was removed.[50] The Task Force also told the Data Center not to report the breach during the investigation.[51]

{16} A spokesman for the Governor of California suggested shortly after the breach that the state did everything it could to prevent the break-in.[52] During the investigation, however, it was discovered that the server that was breached sat outside the Data Center's firewall.[53] No explanation was given for this anomaly. Shortly after the incident, state officials also reported concern over the ease with which the hackers accessed the system.[54] The Data Center operators admitted they actually employed few of the existing Data Center security procedures in place to protect the system.[55]

{17} Furthermore, after the attack, conflicting information was reported regarding the regular maintenance of patches at the Data Center.[56] Early reports stated that patches[57] that should have been installed at the Data Center prior to the incident were not operating.[58] A California Controller's Office representative indicated, however, that the Data Center applied a required patch to one of two servers that held state employee payroll deduction information, but not the one that was breached.[59] This representative admitted that if the patch had been installed on both servers, "that attack would not have been successful."[60]

{18} The Data Center director was less than reassuring on the issue of whether personal information had been viewed, downloaded or printed during the attack. He suggested that

in order to actually steal, as opposed to merely viewing information, the hacker would need to penetrate a series of password-protected areas.[61] Of course, he could not say for certain whether this was accomplished.[62] In subsequent testimony before a California State Senate subcommittee, the director was quoted as saying "I don't think we will ever be one-hundred percent sure that the data has not been compromised."[63] Despite this lack of certainty, the director also reportedly stated that there was no evidence that the hacker had downloaded, printed or even accessed the state workers' personal information.[64] It is more likely, however, that the Data Center simply had no information to prove or disprove this theory.[65] Although it could not be directly tied to this particular breach, at least one state employee reported suspicious activities that indicated the strong possibility of identity theft following the breach.[66]

{19} Shortly after the Data Center breach, California State Senator Steve Peace announced that he would be delving into these issues during a June 12, 2002, hearing designed to start the process for preventing further attacks.[67] Shortly thereafter, Senator Peace reworked pre-existing bill SB 1386 to address the Data Center issues.[68] The principle features of the final version SB 1386 as enacted are as follows:

- Businesses, California state government agencies, and individuals who conduct business in California or own or license computerized personal information are required to disclose "any breach of the security of [California residents']. . . data. . . following discovery or notification of the breach."[69]
- "Breach of the security of the system[70] means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information" on the system.[71] The breach does not need to be reported unless the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[72]
- If an employee or agent acquires the information in good faith "for the purposes of the agency" and the information is not disclosed further, it does not constitute a breach.[73]
- Personal information is an individual's first name or first initial and last name in combination with a(n): (1) social security number;[74] (2) California driver's license or California Identification Card number; and/or (3) account number, credit or debit card number, in combination with the security or access code or password that would allow access to the account.[75] Notice of breaches of publicly available information alone is not required.[76]
- The disclosure must be "expedient" and made "without unreasonable delay."[77]
- If a California resident is harmed by the agency's failure to give notice as required by the Act, s/he may bring a civil suit for damages, injunctive relief and any other relief allowed by law.[78]
- Notice of the breach need not be given right away if measures are being taken to determine the scope of the breach and "restore reasonable integrity to the system."[79]
- Notice of the breach need not be given right away if the delay is "consistent with the legitimate needs of law enforcement." Once law enforcement determines that notification will not "compromise" the investigation, notice must be given.[80]
- Notice, as defined by SB 1386, is any of the following: written, electronic, or substitute notice.[81] Substitute notice is only appropriate when written or electronic notice would cost in excess of $250,000.00 or the party does not have

enough information to do the other forms of notice.[82]

- If the personal information subject to the breach was "encrypted," no notification is required.[83]
- The Act was effective July 1, 2003.[84]

B. Pros and Cons of Notice

{20} The notification provision is the heart of SB 1386.[85] On the surface, the benefits of notice appear to be obvious. Beth Givens, Director of the Privacy Rights Clearinghouse in San Diego, stated that the key to preventing identity theft is early detection. According to Givens, "the earlier you know, the easier it is for you to stop the damage."[86] The more time that passes following a breach, the lower the chance that the information will be used,[87] because criminals who possess this type of information tend to act quickly.[88] Consumers who receive early notice of such breaches can cancel their credit cards and contact credit bureaus in order to prevent thieves from opening bogus accounts.[89]

{21} Some argue, however, that data subjects gain no real advantage by receiving early notice of a breach.[90] In effect, public notice of the breach gives hackers the notoriety they crave.[91] Moreover, credit card companies suggest that when credit card numbers are acquired during a breach, consumers do not need to know because they are protected by "zero liability" or "no fault" consumer protection.[92] This "protection," however, can be illusory, mainly because many credit card companies require their cardholders to review their statements for unauthorized transactions. If the cardholders do not catch the transactions within a reasonable time period, the credit card companies may counter that the cardholders have been grossly negligent in reviewing their bills.[93] If cardholders know that there have been breaches with respect to their credit information, at least they can monitor their billing statements with jaundiced eyes. They may also decide to cancel their credit cards or request new credit cards and numbers in order to avoid the possibility that they might inadvertently overlook fraudulent transactions. If customers are not given this option and they fail to notice fraudulent transactions, their SB 1386 or common law complaints against the credit card companies for improper security or failure to provide notice may be countered with claims of comparative negligence or breach of contract.

{22} Whatever the strength of zero liability policies may be, the California Senate did not agree with this argument. As noted in the comments from the June 18, 2002 hearing of the Assembly Committee on Judiciary:

> All too often events of this sort go completely unreported. How can this be? The embarrassment of disclosure that a company or agency was "hacked," or the fear of lost business based upon shoddy information security practices being disclosed overrides the need to inform the affected persons. In other instances, credit card issuers, telephone companies and internet service providers, along with state and local officials "handle" the access of consumer's personal and financial information by unauthorized persons internally, often absorbing the losses caused by fraud as a matter of "customer service" without ever informing the customer of the unauthorized use of his/her account.[94]

{23} The California Senate was not only concerned with the effect a particular loss of credit

information might have on consumers in their contractual relationship with their credit card companies, but also with empowering cardholders and other data subjects to give them a voice in the decision-making process once their personal information is stolen.

C. Scope of the Notice Provision

{24} The scope of the notice provision places organizations in a bind because they must decide whether to give the minimum notice required by law or go beyond the express requirements. For example, analysts have warned that relying on the strict requirements of SB 1386 and merely notifying California customers of breaches is not advisable.[95] Notifying only Californians may not only subject the organization to criticism,[96] but businesses may simply find it easier to notify everyone rather than merely notifying California residents.[97] The bottom line is that "[c]ompanies do not want to get to the point of notification."[98] "Therefore, they have powerful incentive to secure data from the beginning."[99]

{25} Due to the complex nature of online transactions, it will be difficult to determine who must provide notice under SB 1386. This issue arises because data travels through intermediaries during online transactions.[100] It is, therefore, difficult to determine whether the sender's or recipient's information has been breached. SB 1386 leaves these questions unanswered.

{26} Once a breach has occurred and notice is required, an organization is immediately faced with the daunting task of assessing whether any of the data subjects whose information was potentially exposed were residents of California.

D. Conducting Business in California and Storing Information on its Residents

{27} Virtually every online merchant sells its products to California residents.[101] In accordance with the Act, storing confidential information pertaining to a single California resident on a single computer will require compliance.[102] No physical office or other property in California is required.[103] According to Scott Pink, Deputy Chair of the American Bar Association's Cybersecurity Task Force, "[i]f you are selling products or providing services to residents of California, it would probably be determined that you're conducting business in California under this law."[104] If a company maintains personal information on a potential customer, former customer, or other California resident on its system, then it must comply.[105]

{28} SB 1386 fails to establish criteria for determining whether data subjects whose personal information is involved in a suspected breach are residents of California.[106] Opponents of the law have noted that it is virtually impossible to determine which persons in a database are residents of California, mainly because the database owners often collect no information from the users that would allow this assessment to take place.[107] Even where residency information is obtained during a transaction, a customer who is a California resident at the time of the transaction may cease to be a resident at the time the breach occurs. The opposite is also true: a customer who is a non-California resident at the time of the transaction could become a California resident before the breach without the company's knowledge.[108] For this reason, many companies have legitimately criticized the bill for failing to provide a method by which a database owner can determine whether a data subject is a California resident,[109] especially where only e-mail or IP addresses were collected at the time of the transaction.[110]

{29} Organizations are uncertain whether the courts will employ the legal definition of "resident" used for establishing venue. It is also uncertain whether California courts will require businesses to regularly contact data subjects to update information regarding their residency. Businesses that rely solely on data received at the point at which they originally gathered information from the subject could find themselves at risk of civil suit under SB 1386. From a privacy perspective, it is ironic that the law could actually require that businesses insist on collecting and storing more information regarding California data subjects at the time of a transaction than ever before.[111]

{30} Organizations should update their customer contact information on a regular basis to avoid using SB 1386's public notice procedures.[112] This suggestion originates from the idea that a company is better advised to notify the individual customers affected rather than making a public announcement, because such an announcement will easily reach unaffected and potential customers as well. Although such an approach does not guarantee that the matter will not be exposed to the general public anyway, it may limit the scope of the unpleasant advertisement.

{31} Organizations must also consider the liability implications of only notifying California residents to the exclusion of all other data subjects.[113] One law firm has recommended that companies notify every potentially affected data subject in the United States in the event of a breach.[114] Segregating California residents for notice of breaches could create liability implications with respect to non-Californians who fail to also receive notice.[115]

E. Vagueness of Language Used

{32} Perhaps the most maligned aspect of the bill is its use of undefined terms. "Modern legislators simply do not understand [technology]," and this lack of understanding causes them to create vague legislation at the request of lobbyists and public interest groups.[116] Assailed as a byproduct of this problem, SB 1386's lack of definitions for key terms will make compliance for organizations and enforcement for the courts very difficult.

1. "Reasonable Belief" that "Acquisition" of Data Has Occurred

{33} As noted above, SB 1386 requires notification of data subjects once an organization has a reasonable belief that data acquisition has occurred. Thus, the law does not require actual proof that personal information has been compromised before notice is required. In other words, SB 1386 is not simply limited to situations where an organization knows a California resident's personal information has been acquired without authorization. Instead, the law expands the notice requirement to encompass situations where it is "reasonably believed" that such information has been acquired.[117] The "reasonably believed" language, therefore, requires notice to California residents even if an organization merely "suspects" the unauthorized acquisition of information.[118] Because reasonable belief that an acquisition has occurred is all that is required, mere access to data, not actual theft or use[119] of the information will trigger the statute's costly notice provision.[120]

{34} The Investment Company Institute (ICI), a coalition that represents the mutual fund industry, argued during the California Senate legislative proceedings for SB 1386 that this provision will not only be expensive for organizations to implement,[121] but it will unnecessarily alarm citizens who receive notice.[122] Therefore, the practical result of this bill may be a rash of false alarms delivered via the notice required by this law, even though no actual acquisition of customer

information has occurred.[123] This may result in the erosion of consumer confidence in Internet transactions[124] and cause companies to lose customers.[125] A barrage of notices warning consumers of security breaches might also eventually desensitize consumers and cause them to ignore the notices.[126] On the other hand, notification requirements may cause companies to improve information security, thus increasing consumer confidence.[127]

{35} Moreover, many organizations may not know that there has been a breach until employees start receiving bills or calls for charges they did not incur.[128] This occurs, in part, because it is difficult to prove that confidential data was not stolen once a computer system is breached.[129] This situation occurs most often with systems that either lack intrusion detection capability[130] or have logging capabilities that are not implemented or are improperly configured. It may also happen simply because a company lacks security measures that would allow any monitoring of their systems. Whatever the monitoring capability of a particular system may be, the Act itself is silent on the method that must be used to discover breaches.[131] Therefore, it is conceivable that under SB 1386, a company might take the position that it will take no affirmative action to discover that a breach has occurred, thus "keeping itself in the dark" in order to delay or avoid the expense and embarrassment of notice.[132] Although SB 1386 itself may not specifically require that companies employ a monitoring system to discover breaches, this does not mean that such an obligation would not be imposed by a court under contract or tort theories.[133] It is, therefore, the combination of SB 1386 and the prospect of tort and contract liability that results in the inescapable conclusion that employing tools to deter or detect security breaches is an implicit requirement of SB 1386.

{36} Other opponents of the terms "reasonably believed" and "acquired" cite the fact that it is difficult to discern what would constitute knowledge of a breach.[134] Because of this vagueness, it would, therefore, be plausible for a court interpreting SB 1386 to hold that any semblance of unauthorized activity triggers the disclosure requirements, especially where an organization does not employ adequate logging or intrusion detection systems to prove otherwise.[135] It is more likely, however, that organizations will be required to notify consumers at the point where they know the intruder has accessed personal information, thus putting himself in a position to copy, download or print it. Organizations that employ intrusion detection software and logging devices may be able to determine that an intruder has not accessed personal information, thus saving themselves the cost and humiliation of notification. Therefore, organizations which do not employ intrusion detection and other forensic tools which allow tracing of a hacker's movements before and after the system is penetrated may actually find themselves giving notice to California residents more often than those who have this tracing capability.

{37} As SB 1386 made its way through the legislative process, many businesses lobbied for language that would require proof of actual acquisition before notice is required. The Senate clearly intended to create a proactive bill that empowers data subjects before their stolen data is exploited. Proof of an actual acquisition, as opposed to a reasonable belief that data was acquired, would necessarily require harm to a data subject before the notice provision is triggered. After all, if actual acquisition were the standard, the only real proof of acquisition would be a case of identity theft involving a data subject whose information was obtained during the breach.[136] The authors of SB 1386, however, intended to be proactive in stopping identity theft. Therefore, the California Senate did not allow organizations to wait until a data subject was actually harmed before requiring notification.

{38} It is also possible that the California Senate considered the limits of current technology in assessing the point at which notice must be given. If the California Senate required "acquisition" rather than mere access before notification is required, technology would have to exist to prove this distinction. It would also render SB 1386 meaningless unless an organization has intrusion detection software sophisticated enough to determine when or if information was actually downloaded or copied.[137] Because current intrusion detection software can only determine when information has been accessed, reasonable belief of acquisition must necessarily occur once an organization knows that access has occurred. Even if intrusion detection software could show that information was not accessed and downloaded, it is impossible to say with any certainty that the hacker did not simply write down the accessed information with an old-fashioned pen and paper.[138]

{39} This issue is further complicated when the attack is committed by gaining access to, and subsequently employing, a legitimate user's ID and authentication. This type of breach is virtually impossible to detect regardless of the strength of the system's security, because many intrusion detection software packages are designed only to detect anomalies, not what appears to be normal user behavior.[139] The only way to detect such an intrusion is if the unauthorized user exceeds the scope of authority granted to the legitimate user by the system administrator.[140] When a legitimate user's access information is employed, provided that the user's authorization is not exceeded, an organization may never know that a breach has occurred until data subjects start experiencing identity theft problems.[141]

2. Why Only Electronic and Not Paper Records?

{40} As noted above, the definition of breach, which triggers the notice requirement, only applies to "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information" on the system.[142] From the perspective of privacy advocates, the most frustrating thing about SB 1386 is the fact that it is limited to electronic breaches, even though theft of papers records carries the same potential for identity theft.[143] For example, in 2002, Ligand Pharmaceuticals in San Diego settled a negligence suit with employees whose identities were stolen when it failed to protect personal information contained in paper records.[144] The records in question came from a company acquired by Ligand.[145] The files stolen contained social security numbers, names, birth dates and other data. A lab worker who discovered documents in boxes in a storage closet stole the information.[146] The employee then used the data to rent apartments, to open cellular phone accounts and twenty-five credit card accounts to which $100,000 in goods were charged.[147] Ligand reportedly settled with the affected employees out of court for a "significant six-figure amount."[148] This theft occurred despite the fact that Ligand had very strict policies for safeguarding its records.[149]

{41} Even if the records in the Ligand files contained information pertaining to a California resident, and even if the theft had occurred after July 1, 2003, SB 1386 would not have required Ligand to notify customers of this breach of its physical (as opposed to its electronic) security.[150] Although some argue that electronic data can be more easily transmitted in large quantities and, therefore, requires faster notice to stop the rapid spread of information, this argument will be of little help to the individual California resident whose data is stolen from paper records. Breach notification laws should address breaches of paper as well as of electronic records.

3. Conflicting Laws

{42} As SB 1386 made its way through the legislative process, opponents also criticized the bill because of its potential to conflict with federal law. One opponent noted that with the myriad of potentially conflicting federal and state laws facing corporations, they are "bewildered to comply with what appears to be several moving targets."[151] The president of the Software and Information Industry Association (SIIA), Ken Wasch, also suggested that compliance under SB 1386 would, "in all likelihood, conflict with the requirements of Federal laws such as Gramm-Leach-Bliley and the Children's Online Privacy Protection Act (COPPA), potentially subjecting companies to conflicting liability requirements."[152] It has also been suggested that federal laws, such as the Early Retirement Income Security Act (ERISA), may preempt SB 1386 to the extent it is applies to ERISA plans and group or multi-employer health plans.[153]

{43} Furthermore, it has been argued that the bill reflects an attempt to regulate interstate commerce by forcing companies outside of California to comply with its notice requirements when they store California residents' information. The power to regulate interstate commerce is reserved to the federal government under Article 8, Section 3 of the U.S. Constitution.[154]

F. Notice Exemptions

1. Encryption

{44} The most often discussed and questioned feature of SB 1386 is what has been referred to as the encryption "exemption." The authors of SB 1386 exempted encrypted data from the bill's definition of breach. In discussing this purported safe harbor, one storage security vendor Vice President stated that the law "is scary for any company. But if you're encrypted, you don't have to abide."[155] However, a close examination of the encryption exemption creates more questions than it answers. It would be more accurate to say that encryption may, but does not necessarily, result in exemption from the Act's notification requirements.[156]

{45} The main source of confusion is the fact that SB 1386 does not define the strength or level of the encryption that will exempt an organization from SB 1386's notice requirements.[157] The law does not expressly state that the encryption needs to be strong[158] or even reasonable. Furthermore, the California Senate did not expressly require a level of encryption similar to that currently used in any particular area of the economy.[159] For example, the authors could have required organizations affected by the bill to employ the encryption standard used by the federal government to protect sensitive information.[160] This omitted definition may cause organizations to feel more secure with their level of encryption than they should. It also might cause them to invest[161] in encryption technology that exceeds their needs and reduces system efficiency.

{46} Part of the problem with SB 1386 is that its authors appear to equate "encryption" with "security." Encryption, however, is not supposed to be the primary source of security.[162] It is designed to supplement an overall risk-based program.[163] It is part of the solution, not the solution. When considering encryption as part of a security program, a broad selection of encryption devices are available, ranging from those that are relatively easy to break to those that are virtually impossible to bypass with current technology.[164] Most encryption is done when transmitting data.[165] Secure Socket Layer[166] (SSL) is the technology most commonly employed to encrypt information when transferring it between computers over the internet.[167] Attacks on the data can, however, occur both before and after transitory encryption takes

place.[168] Although the type of encryption envisioned by SB 1386 is not stated, the bill must necessarily be referring to encrypting data as it rests on the system as well as encrypting it during transmission.[169] Encryption of data while at rest in the database is a far less common security method.[170] The problem is that encrypting data at rest leads to a serious "degradation of service."[171] It simply is not possible or practical to encrypt all data all the time."[172]

{47} SB 1386 is also flawed because the encryption provision reflects a lack of understanding of technology.[173] By failing to define encryption, the California Senate created future difficulty for organizations hoping to prove that they have encrypted their data and are therefore entitled to exemption from SB 1386's notice requirements. Once the data is stolen and a plaintiff brings suit against a defendant for failure to give notice of the breach under SB 1386, the defendant who experienced the breach will need to prove that the data was encrypted at the time it was acquired from the system. Unfortunately, even a security professional or forensic investigator might not be able to tell whether the data stolen was encrypted at the time it was taken from the system.[174] At best, the defendant will be able to say that it had an encryption policy in place, employed the necessary technology to encrypt the data, and did everything else it could to ensure that data was encrypted whenever possible.

{48} Furthermore, the use of encryption may reduce liability, but only if it is properly installed, configured and managed.[175] A defendant's success in using the encryption defense will depend heavily on proof that it took measures to ensure the integrity of its encryption key. Often, encryption key management systems are deployed but are not efficient and secure.[176] The potential exposure under SB 1386 requires that organizations not only encrypt their data, but also limit access to the program that encrypts and decrypts information.[177] In other words, even if the company encrypted all information on its systems as it rests in its database as well as in transit, the encrypted information may still be compromised depending on how the breach occurs.[178] For example, if an employee of the organization is able to secure the encryption key and access and copy the data in unencrypted format, even though she is not authorized to do so as part of her duties, the damage may be done in spite of an otherwise vigorous encryption policy.[179] Therefore, even organizations undertaking the burdensome task of encrypting all of the information on their systems, at rest and in transit, may lose the so-called encryption "exemption" unless they manage their encryption keys properly.[180] It should also be noted that even if the information is stolen in encrypted format, once that information is decrypted, or if the organization acquires a reasonable belief that the data was not actually encrypted at the time of the theft, SB 1386's disclosure provisions will likely be triggered.[181]

{49} Organizations using encryption must also be realistic when it is being applied to static information such as social security numbers, driver's license numbers and other data that does not change over time. A thief could easily download this information after breaching the system and then keep the encrypted information until technology exists to crack the encryption.[182] If the organization reasonably believes that the encryption has been cracked, notice will be required even if that reasonable belief is acquired many years after the initial breach and acquisition of the information. It is also important to note that when encryption is employed, it must be applied with respect to every copy of the data and on every system on which the data is housed.[183] This includes individual employees' desktops and laptops.[184] From the foregoing, it is clear that meeting the standards that will probably be required to successfully employ the encryption exemption is not as easy as it initially appears.

2. Temporary Law Enforcement Exemption

{50} As discussed above, notice of the breach need not be given immediately if the delay is "consistent with the legitimate needs of law enforcement." If an organization reports the breach to the police, it need not provide immediate notification to data subjects provided this delay is necessary to the investigation.[185] Notification can also be delayed while the company determines the scope of the breach and restores the integrity of the system.[186] Once integrity is restored, however, notice must be given if it will not "compromise" the investigation.

{51} This exemption may have a positive effect if it results in an increase in the number of incidents reported to police, something law enforcement has long-awaited.[187] The drawback of the exemption is that it temporarily thwarts the purpose of the bill—alerting consumers immediately so that they can be proactive in protecting themselves from identity theft.[188] It is unclear whether a law enforcement agency, as opposed to the organization itself, must decide when delayed notice is appropriate to meet "the legitimate needs of law enforcement." This issue arises because SB 1386 does not state by whom the decision must be made. Courts will most likely require that this decision be made by some law enforcement agency somewhere in the country. Law enforcement agencies in California will be under pressure to disclose the existence of the breach as soon as possible.[189] Because the bill has an impact on databases outside of California, however, the success of enforcement will heavily depend on the will of law enforcement authorities in other jurisdictions to vigorously apply the law enforcement provision. This aspect of the bill introduces politics to the enforcement process and gives rise to the possibility that law enforcement agencies outside of California may be encouraged by political pressure to protect local companies by conducting detailed and methodical (yet legitimate) investigations, thus expanding the time before notice must be given.[190] This could be deemed a significant advantage for organizations operating outside of California.

{52} The temptation may be to go to law enforcement immediately in order to help the organization "buy time" to plan and strategize.[191] Organizations have to be careful, however, not to overemphasize the law enforcement "safe harbor" as a means of unreasonably delaying notice. Although the investigation could take a great deal of time, nothing in the law allows this to be used as a means of indefinitely putting off notice to consumers. Moreover, nothing in the law requires consumers to wait until the completion of a law enforcement investigation before filing suit for negligence or breach of contract associated with the incident. If information pertaining to the breach is leaked to data subjects who have experienced actual losses as a result of a breach, they are free to file suit against the organization under common law or statutory theories of negligence and breach of contract without waiting for the completion of the criminal investigation.

{53} In the end, the decision to notify law enforcement must be made in consultation with counsel.[192] The company must weigh the loss of control over the investigation against the benefit of the delay provided by this temporary safe harbor. Getting law enforcement involved early may lead to quick apprehension of the culprit. It may also lessen the impact on the company's reputation if police announce the security breach to the public and simultaneously announce that the hacker has been arrested.[193] The possibility of being in a position of delivering positive news of the arrest with the negative news of the breach might tip the scales in favor of seeking help from law enforcement at the outset.

{54} Overall, the law enforcement provision is a necessary evil in balancing the interests of organizations and individuals. As noted above, however, organizations must be careful not to rely on this provision for long periods of time. Organizations must avoid over-reliance on this provision in order to avert the embarrassing possibility of the breach disclosure coming from another source. If data subjects are less angry when they hear of the breach, they are less likely to pursue litigation.

G. SB 1386 Authorizes Private Right of Action

1. Narrow Cause of Action

{55} Much ado has been made about the possibility that SB 1386 will lead to class action lawsuits and large judgments in civil suits.[194] The bill itself, however, only addresses a very narrow security breach liability issue. This law does not create a new cause of action against an organization for permitting a computer security breach to occur. It merely requires that breached organizations give notice once they have a reasonable belief that a data subject's personal information has been acquired. It is the failure to give notice, rather than the failure to prevent a breach from occurring, that triggers the right to file a civil suit for damages under SB 1386.

{56} SB 1386 limits damages to those arising from an organization's failure to give notice of the breach. Therefore, a plaintiff seeking damages under this bill would have to show that: (1) the defendant's system was breached; (2) the plaintiff is a California resident; (3) the defendant had a reasonable belief that the plaintiff's personal information (as defined in SB 1386) was acquired during the breach; (4) the defendant failed to give plaintiff notice as required by the bill; and (5) the plaintiff suffered damages as a result of defendant's failure to give her notice. The plaintiff will have the burden of proving that she is a California resident and suffered damages, but will also have to prove that it is more likely than not that she suffered damages as a result of the defendant's failure to give her notice.[195]

{57} Plaintiffs seeking to hold an organization accountable for damages that arise from the security breach itself will need to look outside SB 1386. The duty to exercise due care in protecting information from breach will be found in existing state and federal statutes[196] and the common law. These sources of law will provide the vehicles that will drive litigation in this area. For example, even before the enactment of SB 1386, when a system breach occurred, the data subject already had the option of filing suit for negligence or breach of contract[197] under appropriate circumstances. Therefore, public anger arising as a result of an organization's failure to give notice under SB 1386 will more likely serve as a catalyst that leads to the filing of a negligence or contract cause of action than as the sole cause of action in a case arising as a result of a computer security breach. In other words, any attorney pleading a case under SB 1386 for failure to give notice will necessarily include a negligence or contract claim to address any negligence that may have caused the breach itself.

2. Only "Customers" May Sue?

{58} SB 1386 limits the right to sue to "customers", yet another term undefined by the bill. The bill refers to data subjects generically throughout the bill, but then mysteriously limits the right to sue to "customers." This is unusual because the bill's notice requirement is not only imposed on companies (which have customers), but on California government agencies and individuals

as well. The use of the word "customer" would also appear to limit a company's employees from suing it for failing to give notice of a breach unless the employee is also a customer of the business.[198] The use of the term "customer" would also seem to remove suits against the State of California from its remedies unless the data subject could somehow prove that he or she was a "customer" of the state. This is ironic because it was a breach of employee information in a California state database that caused the bill to be passed in the first place.[199] Therefore, in the end, SB 1386 does not even address the specific circumstances that lead to its passage. This provision needs to be amended by the California legislature to allow suit by employees and all persons affected by an organization's failure to give timely notice.

H. SB 1386 Does Not Expressly Require Organizations to Establish a Security Program

{59} SB 1386 stops short of expressly requiring the implementation of a security program. There is, however, no question that SB 1386 implicitly sends the message that organizations and persons must "prevent, detect and monitor intrusions."[200] For example, it encourages organizations to employ encryption (which is only part of a security program). It also rewards companies that monitor their systems closely enough to recognize when activities reach the point where it is reasonable to conclude that personal information has been acquired. Companies that do not closely monitor activities on their systems may find themselves sending notices every time their intrusion detection system reveals an anomaly. Despite these efforts to reward a sound security program, nothing in SB 1386 expressly requires an organization to implement a security program.[201] The only duty expressly required in the bill is to give notice of a breach once reasonable belief of data acquisition occurs. The duty to safeguard personal information will be found outside SB 1386, in federal statutes,[202] contract law or negligence law.

IV. IS THERE A SOLUTION AT THE FEDERAL LEVEL?

A. SB 1386 Is At Odds With the Bush Administration Approach

{60} SB 1386 takes an approach that is at odds with the Bush Administration's cyber security policy. The Administration favors self-regulation and secret disclosures[203] to select government agencies, rather than public warnings.[204] The Administration has opposed breach notification and federally mandated security standards in favor of accommodating business concerns and encouraging voluntary submission[205] of information regarding breaches.[206] The Bush Administration avoided this type of disclosure law in developing its cybersecurity policy, as stated in *The National Strategy to Secure Cyberspace*.[207] The rapid growth of fraud and identity theft may give the Bush Administration little choice but to promote consumer notice over corporate self-regulation.

B. Federal Legislation

{61} The Bush Administration's pro-business approach has not stopped the introduction of two bills pending before the U.S. Congress. Although businesses do not generally support breach notification legislation, they do agree that if there is going to be legislation in this area, it should be addressed at the federal level rather than through piecemeal state legislation.[208] The fear is that if the individual states all create conflicting legislation requiring breach notification, organizations that do business nationwide will be buried in an avalanche of what could be conflicting obligations. The U.S. Senate currently has a bill pending that might avoid this feared

piecemeal approach. There is also a bill pending in the House of Representatives that would require breach notification in the banking industry.

1. Notification of Risk to Personal Data Act

{62} On June 26, 2003, just five days before the effective date of SB 1386, Dianne Feinstein, a U.S. Senator from California, introduced S. 1350, the Notification of Risk to Personal Data Act (NORPDA).[209] Many of the provisions in NORPDA are borrowed directly from SB 1386. Unfortunately, many of the borrowed provisions suffer from the same vagueness that plagues SB 1386. There are, however some subtle differences between NORPDA and SB 1386. The notable provisions in NORPDA are:

- NORPDA defines breach of system security as "the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information . . ." (emphasis added).[210]
- Under NORPDA, once a "breach of the security system" is discovered, notice must be sent to United States residents whose "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[211] This notice provision is obviously much broader than SB 1386 because it clearly would have international implications and affect every database owner in the world maintaining personal information (as defined in NORPDA) on U.S. residents.[212]
- NORPDA applies to agencies and persons engaged in interstate commerce. "Agency" includes most governmental bodies, the most notable exceptions being the Congress and the federal courts.[213]
- Like SB 1386, NORPDA does not require an organization to give notice of a breach if it already "maintains its own reasonable notification provisions as part of an information security policy for the treatment of personal information" and it actually "notifies subject persons in accordance with its information security policy in the event of a breach of security of the system."[214] (emphasis added). NORPDA, however, goes further than SB 1386 by defining acceptable notification procedures. In order for its "notification provisions" to be deemed "reasonable", an organization must:
    - "use a security program reasonably designed to block unauthorized transactions before they are charged to the customer's account"[215]
    - use a security program that requires notice to data subjects "after the security program indicates that the breach of the system has resulted in fraud or unauthorized transactions, but does not necessarily require notice under other circumstances" [216]
    - be "subject to examination for compliance with this Act by 1 or more Federal functional regulators (as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. section 6809)[[217]], with respect to the operation of the security program and the notification procedures." [218]
- Rather than authorizing a private right of action for damages, as allowed in SB 1386, NORPDA provides civil remedies ($5,000 per violation and up to $25,000 per day while the violation persists) that must be enforced by the Federal Trade Commission (FTC). [219] NORPDA does not, however, expressly or implicitly exempt organizations from private suits

and class-actions in the event of a breach.[220]

- Like SB 1386, NORPDA would allow equitable relief to enjoin ongoing or proposed violations of its provisions. Unlike SB 1386, however, these equitable actions would need to be filed by the FTC, not affected data subjects.[221] State Attorneys General would also be authorized by NORPDA[222] to enjoin organizations, enforce compliance with the Act, and obtain damages, restitution or other compensation on behalf of U.S. residents.[223]
- NORPDA would not affect other remedies available under law. For example, contract or negligence actions or actions filed under SB 1386 can still be pursued even if this bill becomes law.[224] State or local electronic breach notification laws that are inconsistent with NORPDA will be superseded, "except as provided under sections 1798.82 and 1798.29 of the California Civil Code."[225] Therefore, SB 1386 is preserved, but legislation on the subject passed by another state would be barred by the Supremacy Clause.[226]

3. The Identity Theft Consumer Notification Act

{63} In 2002, a former Bank One employee in Wisconsin gave a ring of identity thieves account information and social security numbers on 250 bank customers.[227] Upon discovery of the theft, Bank One fired the employee but failed to notify its customers.[228] Eight months later, a retiree who was a customer of the bank discovered that a new Jaguar had been purchased in his name.[229] Once this incident achieved notoriety in the local press, Bank One notified its customers of the data theft.[230]

{64} In response to this incident, two members of the U.S. House of Representatives from Wisconsin, Jerry Kleczka and Paul Ryan, introduced a bill requiring banks to notify customers if personal data is stolen.[231] The highlights of H.R. 818, the Identity Theft Consumer Notification Act,[232] are as follows:

- Notification to consumers would be required "upon discovering that the confidentiality or security of any nonpublic personal information maintained by the financial institution with respect to a consumer has been compromised in any way by an employee of the financial institution, or through any unauthorized entry into the records of the financial institution."[233] H.R. 818 is, therefore, different from NORPDA and SB 1386 because H.R. 818 is limited to personal information held by financial institutions.
- The language in H.R. 818 does not limit the scope of a security breach to computerized information. Unlike SB 1386 and NORPDA, it applies to paper records as well.[234] As noted previously, neither NORPDA nor SB 1386 apply to paper records and, therefore, treat similarly situated identity theft victims differently.
- Unlike SB 1386 and NORPDA, H.R. 818 would require more than mere notice to the consumer. It would also require that the financial institution assist the consumer in fixing the problems caused by the breach of security, including correcting and updating information in consumer credit reports as required by the Fair Credit Reporting Act.[235] H.R. 818 would also expressly require reimbursement for consumer losses incurred as a result of the breach or misuse of the data, "including any fees for obtaining, investigating, and correcting a consumer report of such consumer at any consumer reporting agency."[236] Finally, the financial institution would be required to assist consumers in repairing damage to their credit arising from the breach.[237] Section 618(a) of the bill would authorize private suit in an appropriate U.S. District Court (without regard for the amount in controversy) or in any other court of competent jurisdiction.[238]

- The statute of limitations provision requires that actions filed under the Fair Credit Reporting Act must be filed no later than 2 years after the date on which the violation is discovered or should have been discovered by the exercise of reasonable diligence.[239]
- Like SB 1386 and NORPDA, H.R. 818 contains a law enforcement safe harbor. H.R. 818's provision allows for a temporary "waiver" of the notice requirement "at the request of a law enforcement agency investigating such violation for such limited period of time as the law enforcement agency determines is essential for carrying out the investigation."[240] This language is far better than that used for the temporary law enforcement exemptions under SB 1386 and NORPDA because it makes clear that law enforcement authorities must make the decision that notification would interfere with the investigation.

V. HOW SHOULD BUSINESSES AND CONSUMERS PROTECT THEMSELVES?

A. Businesses

{65} The best way for an organization to avoid the effect of notification statutes and the litigation they might spawn is to secure its systems.[241] Companies should focus more on front-end security and avoid quick fixes.[242] In order to avoid being a victim of security breaches and avoid problems with breach notification laws, businesses should consider the following measures:

- Review your organization's policies[243] regarding access to sensitive information in existing systems and the systems of clients or business partners.[244]
- Access to personal information should be limited to those authorized persons in your company who need to know it.[245]
- Restrict the situations in which access to personal information may be downloaded and saved to laptops,[246] desktop computers[247] and other disk media issued to employees. Employees must be forbidden from transferring personal data maintained by the organization to the employees' personal computers.
- Review your organization's privacy policies posted on its website or in print ads. Make sure that your company can deliver on the promises made in those policies. For example, do not promise that all information is encrypted all of the time.
- Review your organization's password policies, making sure that passwords are not inadvertently accessible to other employees or outsiders.[248]
- Create or modify your organization's procedures for detecting and reporting breaches.[249]
- Determine whether your organization already requires the notification of data subjects whose personal information has been breached in a manner consistent with SB 1386's requirements.[250] If the procedures do not measure up, modify them so they comply with the law.
- Determine what "personal information" regarding California residents is contained on your system and document the information contained on each system.[251] Review your internal and external procedures to determine whether they provide reasonable protection against breach.[252]
- Install firewalls[253] and authentication protocols to protect personal data.[254]
- Employ audit trails to track events occurring on the system so you can determine who (or what) caused them.[255]
- Employ intrusion detection software[256] or other mechanisms by which you can determine the extent to which the system has been compromised and the extent to

which information has been accessed.[257]

- If your company does not have the skills or the forensic tools necessary to make the simple determination that there has been a breach, it should acquire those skills and capabilities immediately or retain the services of companies who specialize in this area.[258]
- Review and amend any third party storage agreements you have with external data centers,[259] making sure that those agreements require the vendor to notify your company in the event of a breach.[260] If you outsource your data storage, you need to have your legal counsel revisit those agreements, paying careful attention to the security provided at the data storage facility.[261] Take the time to learn about the security procedures employed at the storage facility and audit its procedures periodically.
- Educate, train and re-train employees about SB 1386 and the general practices and legal requirements for securing data.[262] Though it is an essential part of an effective security program under any circumstances, it could also help reduce the possibility of punitive damages if a negligence action is brought based on the security breach.[263]
- Establish a contingency plan that focuses on preserving and documenting evidence, especially when the system contains your clients' or your own trade secrets. [264]
- Consider whether it is feasible to separate data subjects' first names, initials and last names from social security numbers, driver's license numbers and other account information on the system. If this can be done without overburdening efficiency, two systems would have to be breached before notice is required.[265]
- Require that customers periodically update their addresses in your organization's database as a condition of online transactions.[266]
- Check your insurance policy to see whether it covers cyber crimes.[267] If it does not, perform due diligence to determine whether cyber insurance is feasible for your business.
- Have the suggestions herein reviewed by a computer security professional and your legal counsel to ensure that additional or different steps are not required by your organization's particular circumstances.

{66} If your system is breached:

- "[T]ake measures to determine the scope of the breach and restore reasonable integrity to the data system before notifying California residents."[268]
- Check to see whether the time/date stamp has been modified on any of the personal information files.[269]
- Where feasible, hire a reputable security company to perform any needed forensic assessment of the breach.[270] Using your own organization's personnel may result in law enforcement refusing to take action because chain of custody issues will be clouded by the company's self-interest potential.[271]
- Communications between the organization and law enforcement should be documented wherever possible. Indeed, everything that happens after the breach must be documented with the degree of care that would be exercised in preparing for a lawsuit.[272]

B. Consumers

{67} When identity theft occurs, it is generally the consumer who is "left to clean up the mess."[273] If you receive an SB 1386 notice from a business or California state agency, you should:

- Closely monitor all credit card and financial statements in search of unusual activity. Because of the ease with which information spreads, once your identity is stolen, you must monitor your accounts for years.[274]
- Change your credit card and bank debit accounts immediately.
- Notify your bank and credit card companies by phone and in writing and advise them that you are to be contacted before any new accounts are opened in your name.
- Contact the company that sent you the notice in writing and request as much information as possible regarding the nature of the breach (to the extent not covered in the notice), whether the company can confirm whether your personal information was, in fact, stolen from its system, the status of the investigation, whether any of the information stolen has been used for illicit purposes and the company's plans for fixing the problem.
- If it is your employer who suffered the breach: ask the same questions stated above and contact your union representative, if applicable.

VI. Conclusion

{68} Computer security breaches are occurring at an alarming rate, thus causing identity thefts to soar. Identity thieves are taking advantage of system vulnerabilities caused by some organizations' failure to employ effective security measures to protect personal information. The old paradigm, focusing mainly on criminal prosecution of hackers, has been tried and has largely failed. Organizations must be held accountable and required to be responsible for protecting personal information they store in computer databases as well as in file cabinets. The government has waited long enough for market forces to cause organizations to take computer security seriously.

{69} By enacting SB 1386, California has established a good starting point for addressing legislation in this area. The law, however, suffers from too much ambiguity to serve as the final template for national breach notification legislation. Although the law appears to strike a good balance between the needs of data subjects and organizations experiencing computer security breaches, the law fails to provide definitions for key terms that carry multiple meanings. For example, the law does not define the term "unencrypted" or the phrase "was, or is reasonably believed to have been, acquired." These omissions make it difficult for companies to comply with the law's ambiguous provisions and will most certainly complicate enforcement. The U.S. Congress should make sure that the type of encryption demanded under NORPDA or any federal breach notification legislation is specified clearly in the law.

{70} Furthermore, SB 1386 also fails to address security breaches involving paper records. This omission is surprising because theft of paper data also gives rise to identity theft. California and Senator Feinstein should follow the lead of the authors of H.R. 818 and expand the scope of SB 1386 and NORPDA to provide notice to victims of paper record breaches as well.

{71} Moreover, SB 1386 needs to be amended to define or replace the word "customer" in the provision allowing a private right of action. It simply does not make sense to draft a law

because of an event involving a breach of state computers that resulted in the disclosure of California employees' personal information, yet provide no cause of action for California state employees against the state. Restricting the right to sue to "customers" also limits the right of employees to sue their private sector employers (unless the employee also happens to be a customer) if the employers fail to give them notice of a breach. There is no justifiable reason for treating employees differently than customers. Both parties provide private information to the organization with the reasonable expectation that it will be kept safe. Unless there is a method by which organizations can be held accountable to their employees, employees will remain viable targets for identity thieves.

---

[*] Mr. Skinner is a graduate of the John Marshall Law School in Chicago, the former research fellow for the Center for Informatics Law, and is currently a Senior Information Assurance Analyst with SRA International Inc. in Fairfax, Virginia. The views expressed in this article are those of the author and not those of SRA International, Inc. Mr. Skinner would like to acknowledge the contribution of Vincent Sherwood, CISSP, Senior Information Security Consultant (www.diligentinformation.com) for assisting in reviewing the technological issues addressed in this article. This article is being reprinted in the Computer Security Institute's "Computer Security Journal" with the permission of the Richmond Journal of Law & Technology.

[1] Robert Lemos, *Data Thieves Nab 55,000 Student Records*, CNET News.com, *at* http://news.com.com/2100-1002-991413.html (Mar. 6, 2003).

[2] Alex Salkever, *To Thwart the Identity Thieves*, BusinessWeek Online, *at* http://www.businessweek.com/technology/content/feb2003/tc20030211_7896_tc047.htm (Feb. 11, 2003).

[3] Jonathan Krim, *8 Million Credit Accounts Exposed, Security Focus*, The Washington Post Company, *at* http://www.securityfocus.com/news/2552 (Feb. 20, 2003) (noting consumer fraud experts' criticism of the data processing center and credit card companies involved for their delay in giving notice to consumers whose accounts may have been compromised).

[4] Lemos, *supra* note 1.

[5] Mike Tarsala, *IBM Loses Hard Drive With Client Data*, CBS MarketWatch, *at* http://cbs.marketwatch.com/news/yhoo/story.asp?guid={510DBA82-AA06-484E-B97A-038E4D0BE1B4}&siteid=mktw&dist=&archive=true (Jan. 30, 2003) (detailing that the error caused IBM stock to drop $2.02 (2%) per share).

[6] In this incident, the breach went undiscovered for more than one month and no notice was given to the employees for another two weeks after the discovery. Patrick Thibodeau, *Bill Would Force Companies to Disclose Thefts of Personal Data*, Computerworld, *at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,76768,00.html (Dec. 16, 2002); *see also* Elaine LaFlamme, *Know the Liabilities of Data Collection!*, N.Y. Law. J., *available at* http://www.akingump.com/docs/publication/533.pdf (Feb. 3, 2003) (discussing the fact that during hearings investigating this incident, it was discovered that during the period the breach went unreported, someone sought to change the address on one state employee's credit card, and in Germany, someone attempted to access another worker's bank account).

[7] Press Release, *Senator Feinstein Seeks to Ensure Individuals Are Notified When Personal Information is Stolen from Databases*, U.S. Senator Dianne Feinstein of California, *at* http://feinstein.senate.gov/03Releases/datasecurityrelease.htm (June 26, 2003).

[8] *See* Erin Kenneally, *Who's Liable for Insecure Networks?,* San Diego Supercomputer Center, *at* http://security.sdsc.edu/publications/SectyDuty.IEEE.pdf (June 2002) (noting that even the news media tends to focus on the hacker rather than the lack of security issue).

[9] *See generally* Cal. Civil Code § 1798.82 (Deering 2003).

[10] *See* Alex Salkever, *Computer Break-Ins: Your Right to Know*, BusinessWeek Online, *at* http://www.businessweek.com/technology/content/nov2002/tc20021111_2402.htm (Nov. 11, 2002) (noting that the lapse that gave rise to the SB 1386 "may mark a dramatic shift in legal policy toward cybersecurity").

[11] The law applies to "California state agencies, but not to counties, school districts or their boards, commissions or agencies." *California Law Protecting Computerized Personal Information Takes Effect in July*, Segal Compliance Alert, *at* http://www.segalco.com/publications/compliancealert/31903.html (Mar. 19, 2003).

[12] Robert Vamosi, *Our Best Shot Yet at Stopping Identity Theft*, CNET/ZDNet Reviews, *at* http://www.zdnet.com/anchordesk/stories/story/0,10738,2913469,00.html (Apr. 30, 2003).

[13] Ariana Eunjung Cha, *Tempting Offer for Russian Pair, Part II of III*, Wash. Post, *available at* http://www.pewfellowships.org/stories/russia/russia_offer.htm (May 19, 2003).

[14] *New California Security Law Affects Organizations Nationwide*, Retex News, *at* http://www.retex.com/March%20Newsletter.pdf, at 4 (Mar. 2003).

[15] Deloitte & Touche's 2003 Global Survey revealed that ninety percent of the security attacks at eighty Fortune 500 financial companies were from external sources, while sixty to seventy percent of the attacks used to be internal. Thirty-nine percent of the companies who responded to the survey reported attacks in the past year, but only ten percent of those attacks were internal. Emma Nash, *Hackers Bigger Threat than Rogue Staff*, VNUnet.com, *at* http://www.vnunet.com/News/1140907 (May 15, 2003).

[16] *Testimony before the House Committee on the Financial Services Subcommittee on Oversight & the Investigations Subcommittee on Consumer Credit* (statement of Evan Hendricks, Editor/Publisher, Privacy Times), *available at* http://financialservices.house.gov/media/pdf/040303eh.pdf (Apr. 3, 2003), at 2.

[17] Nash, *supra* note 15.

[18] This by no means suggests that the types of victims are limited to these two classes.

[19] Posting by Jonathan Nicholson, Reuters, *at* http://www.tigertools.net/board/?topic=topic8&msg=809 (June 30, 2003).

[20] Robert Lemos, *Identity Theft Law Has E-tailers Worried*, ZDNet, *at* http://zdnet.com.com/2100-1105-1022341.html (July 1, 2003).

[21] *Governor Davis Signs Bills to Combat Identity Theft*, Office of the District Attorney, SCCGOV, *at* http://www.sccgov.org/content/0,4745,sid%253D12602%2526chid%253D22639%2526ccid%253D136518,00.html (Sept. 25, 2002) [hereinafter *Governor Davis Signs Bill*].

[22] Stephanie Armour, *Employment Records Prove Ripe Source for Identity Theft*, USA Today, *at* http://www.usatoday.com/money/workplace/2003-01-23-idtheft-cover_x.htm (Jan. 23, 2002); *see also* Paul Roberts, *California Comes Clean*, CSO Online, *at* http://www.csoonline.com/read/010903/briefing_clean.html (Jan. 2003) (noting that 1900 cases of identity theft were reported in Los Angeles County in 2002 alone – a 100% increase from the previous year).

[23] Nicholson, *supra* note 19.

[24] *Site Clues Consumers into Identity Theft*, USA Today, *at* http://www.usatoday.com/tech/2002/06/26/identity-theft-site.htm (June 26, 2002).

[25] Grant Gross, *Tech-Related Issues Top List of Fraud Complaints*, InfoWorld, *at* http://www.infoworld.com/article/03/01/22/030122hnfraud_1.html (Jan. 22, 2003).

[26] *California Law Fights Identity Theft*, Wired News, *at* http://www.wired.com/news/privacy/0,1848,59376,00.html (June 23, 2003).

[27] Rachel Konrad, *New Law Forces Companies to Warn Consumers of Computer Security Holes*, San Diego Union-Tribune, *at* http://www.signonsandiego.com/news/computing/20030623-0003-ca-wevebeenhacked.html (June 23, 2003). U.S. Treasury Secretary John Snow has called on Congress to "overhaul" the practices of consumer credit reporting practices to empower consumers in battling identity theft. Snow suggested the creation of a national alert system that would allow consumers to notify bank and merchants to be on guard against attempts to misuse personal data. Nicholson, *supra* note 19.

[28] Identity Theft Resource Center [IRTC], *The Risk to Homeland Security from Identity Fraud and Identity Theft: Testimony for the Joint Hearing of the House Judiciary Subcommittee on Immigration, Border Security and Claims & Crime, Terrorism and Homeland Security*, *at* http://www.idtheftcenter.org/html/homeland.htm (June 25, 2002) [hereinafter Foley Testimony] (detailing the testimony of Linda Foley, Executive Director, Identity Theft Resource Center, and noting that "[a] Florida Grand Jury recently impaneled to study the problem of identity theft concluded

that the average loss to business is $17,000 per victim.").

[29] Janine Benner, et al., *Nowhere to Turn: Victims Speak Out on Identity Theft*, *at* http://www.privacyrights.org/ar/idtheft2000.htm (May 2002) (noting that victims of identity theft estimate that they spent approximately $800 trying to fix identity theft issues); *see also* Foley Testimony, *supra* note 28 (discussing FTC estimates that the average victim incurs $1,100 or more in out of pocket expenses fixing identity theft problems); Piper Rudnick, *E-Commerce and Privacy Group Alert* (Jan. 2003), *at* http://www.piperrudnick.com/db30/cgi-bin/pubs/ECommerceJan03.pdf (giving the law firm Piper Rudnick's estimates that identity theft costs the average consumer approximately $1,000) [hereinafter Piper Rudnick Alert]; Salkever, *supra* note 2 (noting that, according to the Privacy Rights Clearinghouse, it costs the average consumer $800 to fix identify theft issues).

[30] Foley Testimony, *supra* note 28.

[31] Salkever, *supra* note 2.

[32] Foley Testimony, *supra* note 28; *see also Governor Davis Signs Bill, supra* note 21.

[33] Salkever, *supra* note 2.

[34] *Governor Davis Signs Bill*, *supra* note 21.

[35] George V. Hulme, *California's New Rules of Disclosure*, Banktech.com, *at* http://www.banktech.com/utils/printableArticle?doc_id=BNK20030630S0002 (June 30, 2003). According to the Computer Security Institute's 2003 Computer Crime and Security Survey, out of 376 organizations polled, each admitted experiencing a security breach in the past year, but half of the respondents said that they did not report the incident to anyone outside the company; only thirty percent contacted law enforcement authorities. *Id. See also* Aviva Litan & John Pescatore, *Stolen Credit Card Case Should Prompt Card Companies to Act*, Gartner.com, *at* http://www3.gartner.com/DisplayDocument?doc_cd=113282 (Feb. 20, 2003).

[36] Sarah D. Scalet, *Alarmed: Oh, Did We Forget to Mention That?*, *at* http://www.csoonline.com/alarmed/03142003.html (Mar. 14, 2003). Ms. Scalet notes that in February, 2003, a security breach at Data Processors International resulted in the compromise of eight million Visa, Mastercard, American Express and Discover Card numbers. It has been suggested that one percent of the Visa and Mastercard numbers in America were exposed during this breach. After the incident, the credit card industry argued that there had been no confirmed cases of these stolen credit card numbers being misused. Most companies involved opted to replace the cards as complaints came in rather than informing the customers directly. Some credit card companies take the position that the customers have zero liability for fraudulent purchases reportedly made on their cards. Therefore, there is no risk to the consumer. This approach ignores the practical realities of the situation. Credit card companies generally require customers to review their billings and report unauthorized charges within a certain period of time. If customers are notified that their records have been compromised, they can be especially vigilant in monitoring their monthly statements to watch for transactions resulting from the records exposure. If, on the other hand, the customer fails to notice the fraudulent charge in the billing after a designated period of time, the customer could lose the right to take advantage of the "zero liability" policy. Moreover, if the identity thief changes the user's address after stealing the information so the victim cannot review her monthly statements, the customer may be deprived of the option of promptly reviewing his monthly statements. *See generally Union Demands Safeguards in Wake of State Database Hacking*, Sacramento Bus. J., *available at* http://www.bizjournals.com/sacramento/stories/2002/06/03/daily33.html (noting that hackers sometimes change the victim's address in order to gain more time to use the card) (June 6, 2002) [hereinafter *Union Demands Safeguards*].

[37] Salkever, *supra* note 10.

[38] SecureTheory, *If It Weren't For the Weather . . ., at* http://www.securetheory.com/archives/2003_05.html (May 13, 2003) [hereinafter *If It Weren't For the Weather*].

[39] Salkever, *supra* note 10.

[40] Guidance Software, *Guidance Software's EnCase Enterprise Provides Incident Response Capabilities Needed to Support Compliance of California Law SB 1386*, *at* http://www.guidancesoftware.com/corporate/press/2003/20030414.shtm (Apr. 14, 2003).

[41] *Stephen P. Teale Data Center: About Us, at* http://www.teale.ca.gov/about/ (Aug. 30, 2003) (explaining that the Data Center is actually a department within the California state government that operates out of California's Business, Transportation & Housing Agency and which was created by Senate Bill in 1972, and that the center services 250 government agencies, and over "75,000 front-end user devices" are connected to its statewide

network).

[42] Dalibor Glavan, *Hackers Gain Entry to Key State Database Personnel Files*, *at* http://www.xatrix.org/print548.html (May 26, 2002) (observing that no suspect has been identified, although the FBI traced the address to a Lycos account in Massachusetts).

[43] DateLine UCDavis, *UC Not Impacted By Recent Hacking of Controller Files*, at http://www.dateline.ucdavis.edu/060702/dl_hack.html (June 7, 2002).

[44] Ed Fletcher, *Hacker's Work May Remain a Mystery*, THE SACRAMENTO BEE, June 7, 2002, available at http://www.psych-health.com/hack13.htm.

[45] *Assembly Committee on the Judiciary*, *SB 1396 Bill Analysis, Synopsis, at* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_cfa_20020617_141710_asm_comm.html (June 18, 2002) [hereinafter *June 18 Judiciary Committee Analysis*].

[46] Jennifer Coleman, *Senators Probe Computer Hacking of State Payroll Database*, N. COUNTY TIMES, June 7, 2002, *available at* http://www.nctimes.net/news/2002/20020607/53250.html (citing that fact that the breach was discovered during a "routine maintenance" check).

[47] Letter from Kathleen Connell, Controller of the State of California, to Allan Barcelona, President, California Union of Safety Employees (May 28, 2002) (on file with Richmond Journal of Law & Technology).

[48] *Id.*

[49] *Id.*

[50] *Id*. In an ill-advised effort to deflect attention from her office, Ms. Connell then went on to state that the Data Center was hampered by the absence of a permanent director for three and one-half years. *Id.*

[51] Coleman, *supra* note 46.

[52] Glavan, *supra* note 42.

[53] Coleman, *supra* note 46. "A firewall is a combination of software and hardware components that controls the traffic that flows between a secure network (usually a company LAN) and an insecure network (usually, but not necessarily, the Internet), using rules defined by the system administrator. The firewall sits at the connection between the two networks. All traffic, from one network to the other, passes through the firewall. The firewall either allows, rejects or drops the traffic based on the security policy (rules programmed into the firewall)." ITsecurity.com, *Firewall*, COMPUTER SECURITY DICTIONARY, *at* http://www.itsecurity.com/dictionary (last updated Jul. 1, 2003).

[54] Coleman, *supra* note 46.

[55] Coleman, *supra* note 46.

[56] Coleman, *supra* note 46.

[57] A patch is a segment of software code which modifies an existing application or utility in order to correct some shortcoming, without the need to replace the entire code. Typically a Security Patch will remove a newly discovered vulnerability which could otherwise be exploited by a hacker to cause an undesired effect on the target system. The patch is issued by the vendor. ITsecurity.com, *Patch*, COMPUTER SECURITY DICTIONARY, *at* http://www.itsecurity.com/dictionary (last updated May 25, 2003).

[58] Perry Kenny, *President's Letter*, CSEA VOICE, June 18, 2002, *available at* http://www.calcsea.org/president/csea_voice/20020618.asp.

[59] Fletcher, *supra* note 44.

[60] Fletcher, *supra* note 44. The Data Center may have been following a normal procedure of installing the patches to the backup system first before putting them on the main system. Coleman, *supra* note 46.

[61] Coleman, *supra* note 46.

[62] Coleman, *supra* note 46.

[63] Fletcher, *supra* note 44.

[64] Fletcher, *supra* note 44.

[65] *See* Fletcher, *supra* note 44. The computers' logs indicated that the breach was a one-time event. Many hackers

use automated tools to find vulnerabilities in systems. Once the tool finds an opening in a system, it reports this information back to the hacker. The hacker than uses this information to reenter the system using the information acquired during the first penetration. The Data Center director's statement was based on the hope that such a tool was used in this attack because he cited the fact that the usage logs indicated that this breach was a one-time event (i.e. there was no return by a hacker after the initial penetration). *Id.* In subsequent testimony before a Senate subcommittee, the director stated that an automated tool had been used. Coleman, *supra* note 46 (explaining that "[t]he hacker was testing the system by sending out a message to the database," which then "sent back an e-mail to the source saying there's this system that got hit. It wouldn't have told him that it's a payroll system or it's a state of California system.") If an automated tool was not used, however, the premise of this statement drops out. The Director also stated that the method used to breach the system did not allow the extraction of information. Fletcher, *supra* note 44. No further explanation for this statement was given. Finally, the director stated that the hacker tried, but failed, to set up two-way access. *Id.* In later testimony before the state Senate subcommittee, the director testified that the hacker would have had to penetrate several levels in order to access employee data. Coleman, *supra* note 46. During this testimony, he stated that there was no guarantee that the files were not accessed, but had "strong indicators" that no access occurred. *Id.* For example, he cited the fact that none of the records had been altered. *Id*. This presumes, of course, that alteration of records, and not theft of information, was the hacker's motivation.

[66] Shortly after the incident, a state lottery employee reported that she received a letter asking her to verify her change of address request. *Union Demands Safeguards*, *supra* note 36. Changing the address on the identity theft victim's credit or other information is sometimes the first step taken by an identity thief after theft of the data. *Id.* This enables the thief additional time to use the information by keeping the billings from going to the victim's address for her review. *Id.*

[67] Ed Fletcher, *Senator Will Probe Hacking Response*, Sacramento Bee, May 22, 2002, reprinted in CSEA Voice, June 5, 2002, *at* http://www.calcsea.org/president/csea_voice/20020605-04.asp.

[68] The bill went through many revisions in an effort to cure perceived defects noted by members of the business community. Some, but not all of those concerns were addressed before final passage. Edward Hurley, *California Screaming: Companies Must Disclose Security Breaches*, SearchSecurity.com, *at* http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci912476,00.html (June 30, 2003).

[69] Cal. Civ. Code § 1798.29(a) (Deering 2003); *see also Id.* § 1798.82(c). Data centers and other businesses or persons maintaining personal information on behalf of another must notify the owner of the information (not the data subject) of any breaches in their systems. The information owner is then responsible for notifying the data subjects. *Id.* § 1798.82(c).

[70] The act applies to businesses of all sizes. StrongAuth, Inc., *StrongAuth's SB 1386 Frequently Asked Questions*, § 201b, *at* http://pki.strongauth.com/sb1386/sb1386faq.html (last visited Sept. 10, 2003). The type of computer or system used is irrelevant. Id. at 5, Section 201d. The act does not distinguish between stand-alone systems (those not connected to the internet of other computers) and networked systems. *Id.* at § 201e.

[71] Cal. Civ. Code § 1798.29(d).

[72] *Id.* § 1798.29(a)

[73] *Id.* § 1798.29. If a company has an existing policy regarding access to particular data, any access that exceeds authority would be deemed unauthorized. StrongAuth, *supra* note 70, § 107. In fact, anyone who accesses information on a system without legitimately using a user ID and password will probably be deemed to have breached the system. *Id.* The provision allows an exception for "good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency, provided that the personal information is not used or subject to further unauthorized disclosure." This provision does not provide organizations with much relief. It suffers from the lack of flexibility that would allow a company to withhold disclosure even if the company believes further misuse will not occur. Emily Hackett & Kaye Caldwell, *California Enacts Privacy Legislation*, TRUSTe-Advocate Newsletter, *at* http://www.truste.org/partners/newsletter/october2002.html (Oct. 2002). For example, if an employee accesses personal information (as defined in SB 1386) from a computer file that he is not authorized to access and for a purpose unrelated to his job, the company must notify the data subjects whose data was reasonably believed to have been acquired even if the company notices this activity immediately and can say with a certainty that the information was not disseminated further.

[74] The Social Security Number is the "key piece of data used by identity thieves to commit credit and bank fraud." Beth Givens, *Identity Theft Precautions for California State Employees, at* http://www.privacyrights.org/ar/

CalifDataHacking.htm (June 11, 2002).

[75] Cal. Civ. Code § 1798.29. SB 1386's definition of "personal information" is fairly narrow. Hurley, *supra* note 68. Not all types of information deemed personal in other contexts are covered by SB 1386. The general definition of personal identifying information is much broader than the types of information covered by this Act. For example, the California penal code defines "personal identifying information" broadly to include: name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person." Cal. Penal Code § 530.5 (2003). The federal Privacy Act defines "records" protected by the Act to include:

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

5 U.S.C. § 552a (2003). Most of these types of personal information are not covered by SB 1386.

[76] Cal. Civ. Code §§ 1798.29(f), 1798.82(a).

[77] *Id.* §§ 1798.29, 1798.82. SB 1386 does not, however, mandate that notice occur within a set time period. Hurley, *supra* note 68.

[78] Cal. Civ. Code § 1798.84. During hearings prior to the passage of SB 1386, the Information Technology Association of America (ITAA) noted its concern that there was no cap on liability included in the bill. Assembly Comm. on Appropriations, *SB 1386 Summary*, at 2-3, *available at* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_cfa_20020813_145811_asm_comm.html (Aug. 14, 2002).

[79] *Id.* § 1798.82.

[80] *Id.*

[81] Substitute notice may be done by e-mail, conspicuous posting on the website of the party whose system was breached, via notice to statewide media (presumably in California, though not stated), or via the party's own notification procedures as long as they comply with other provisions of SB 1386. *Id.* § 1789.29(h).

[82] It is unclear what a company would be required to say in web site or media notices. *Piper Rudnick Alert, supra* note 29, at 5.

[83] Cal. Civ. Code § 1798.82.

[84] Act effective July 1, 2003, ch. 915, § 5, 2003 Cal. Stat. 90. One author has noted that the delayed effective date of SB 1386 was at the request of Merrill Lynch so it could revamp its security to encrypt its financial data so it could take advantage of this provision in the bill. LaFlamme, *supra* note 6.

[85] SB 1386 was introduced Feb. 12, 2002. S.B. 1386, 2002 Leg. (Cal. 2002), *available at* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020212_introduced.pdf (Feb. 12, 2003) [hereinafter *S.B. 1386, Feb. bill*]. The notification provision was not contained in the original version of the bill when it was introduced by Senator Pace. S.B. 1386, reprinted as amended, *available at* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020320_amended_sen.pdf (Mar. 20, 2002) [hereinafter *S.B. 1386, Mar. amendment*]. The bill was amended in the California Senate to include this provision. This early version of the law allowed organizations to report the breach "as soon as practicable." S.B. 1386, reprinted as amended (Cal. 2002), *at* 2, § 2(a) [hereinafter *S.B. 1386, June amendment*], *available at* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020620_amended_asm.pdf (June 20, 2002); June 18 Judiciary Committee Analysis, *supra* note 45, at 5. This language was deleted when the bill was amended in the California Assembly, because it was feared that this provision would be used by agencies or businesses to wait, "for example, an entire year to notify affected employees and individuals." *Id.* In addition, the Committee added the potential impedance of an ongoing law enforcement investigation as a proper justification for delaying notice. A prior draft of the bill also required notice "to any person whose personal information was, or may have been, accessed by an unauthorized person." On June 20, 2002, this language was amended to require notice to persons "whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person." *S.B. 1386, June amendment.*

[86] Thibodeau, *supra* note 6; *see also* SIFT Security Intelligence, *SIFT Note 2003-01 (Jan. 15, 2003)*, *available at* http://www.iia.net.au/SIFT_Note_2003_01.pdf (Sept. 1, 2003). It has also been noted that when companies publicly

share information regarding attacks, patches are applied, thus reducing the chance for further exploitation of targets.

[87] Coleman, *supra* note 46.

[88] Coleman, *supra* note 46. The Director of TransUnion's victim fraud unit believes that "[t]ime is against them if they wait too long." *Id.* As discussed in more detail in the encryption discussion, this may not always be the case when static encrypted information, such as social security numbers and birth dates, are involved and the thieves can hold on to the encrypted information until decryption techniques become available. *Id.* Most criminals, however, are not interested in waiting a few years to exploit the fruits of their labor. *Id.*

[89] Ryan Singel, *Bill to Force Data Theft Notices*, Wired News (June 27, 2003), *at* http://www.wired.com/news/privacy/0,1848,59419,00.html (Aug. 28, 2003).

[90] *June 18 Judiciary Committee Analysis, supra* note 45. The Investment Company Institute (ICI), a coalition that represents the mutual fund industry, opposed the notice provision, stating, "persons will be unable to take any meaningful prophylactic action to protect themselves in response to the notice." *Id.*

[91] Ellen Messmer, *Calif. Breach-Disclosure Law Raises Questions, Concerns*, NetworkWorld Fusion, *at* http://www.nwfusion.com/news/2003/0630california.html (June 30, 2003).

[92] Anonymous Posting, *No Good Deed Goes Unpunished*, Matthew Lewis Carroll Smith Web Blog, *at* http://www.mlcsmith.com/blog/ (Jan. 15, 2003) (relating a consumer's experience with identity theft; the bank's response to the consumer's inquiry was, "you're covered so it's no big deal.").

[93] Visa, *Zero Liability* [hereinafter *Visa Zero Liability Policy*], *at* http://www.usa.visa.com/personal/secure_with_visa/zero_liability. html?it=h2/index.html (Aug. 28, 2003). For example, Visa's "Zero Liability" policy states that it provides 100% protection for the customer. It then reminds customers to monitor their monthly statements for unauthorized transactions. By way of the following notation, Visa cautions its customers that zero liability does not always mean what it says:

> Cardholders should always regularly check their monthly statements for transaction accuracy. Financial institutions may impose greater liability on the cardholder if the financial institution reasonably determines that the unauthorized transaction was caused by the gross negligence or fraudulent action of the cardholder – which may include your delay for an unreasonable time in reporting unauthorized transactions.

Id. Visa notes that this is an improvement over its former policy, which required cardholders to report unauthorized transactions within two days of discovery. Discover Financial Services, *100% Fraud Protection*, *at* http://www2.discovercard.com/simple_secure/fraudprotection.shtml (last visited Sept. 1, 2003). Discover also requires cardholders to "immediately" notify the company if they think that their cards were used without their permission, but Discover's policy does not expressly state what it will do in the event that cardholders fail to act in accordance with this instruction. *Id.* The credit card industry's argument ignores the fact that the costs associated with the fraudulent transactions, which are "absorbed" by the credit card companies under zero liability policies, are then promptly passed on to consumers, either directly through higher consumer credit card fees or indirectly through increased credit card retailer fees, which are, in turn, passed on to consumers via price increases on goods and services.

[94] *June 18 Judiciary Committee Analysis*, *supra* note 45.

[95] LaFlamme, *supra* note 6.

[96] Jerald M. Savin, *Businesses Must Disclose Security Breaches*, CalCPA Online, *at* http://www.calcpa.org/members/knowledge/articles/webprivacy.html (last visited Aug. 28, 2003).

[97] Kevin Poulsen, *California Disclosure Law Has National Reach*, SecurityFocus, *at* http://www.securityfocus.com/news/1984 (Jan. 6, 2003).

[98] Benjamin Wright, *Data Privacy in California*, News in Electronic Commerce Law, *at* http://ourworld.compuserve.com/homepages/Ben_Wright/e-biz.htm (Feb. 2003). Many businesses have expressed little concern over the notice provision because they have existing policies which require notice. Konrad, *supra* note 27 (citing a spokeswoman for Dell Computer who stated that Dell has had such procedures in place for a long time); *see also* Messmer, *supra* note 91 (quoting an eBay spokesman who claimed that eBay has been breached numerous times and already has a notification policy); Hulme, *supra* note 35. Security experts believe, however, that most businesses outside of the heavily regulated banking and health care sectors are not prepared for dealing

with this law. Hulme, *supra* note 35.

[99] Wright, *supra* note 98.

[100] *See* B. Mahadevan and N.S. Venkatesh, *A Framework for Building On-Line Trust for Business to Business E-Commerce, at* http://unix2.iimb.ernet.in/~mahadev/trust1.pdf (Nov. 30, 2000) (discussing the business implications for interception of online data transmission, as presented at the November 2000 IT Asia Millennium Conference in Bombay, India); cf. Press Release, *Sigaba Corp. Details Top Ten Requirements of a Secure E-Mail Solution*, Sigaba Corp., *at* http://www.sigaba.com/news/pressreleases/2-27-02tenreq.html (Feb. 27, 2002).

[101] Litan & Pescatore, *supra* note 35.

[102] StrongAuth, *supra* note 70.

[103] StrongAuth, *supra* note 70. The breadth of this provision arguably calls into question the issue of whether California's attempt to regulate companies outside the state is an effort to affect interstate commerce, a power reserved to Congress under the Constitution.

[104] Poulsen, *supra* note 97.

[105] *Piper Rudnick Alert, supra* note 29, at 4.

[106] Hackett & Caldwell, *supra* note 73, at 7.

[107] Erik Laykin, *New California Law to Impact Global Business – SB 1386*, Online Security, *at* http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=102 (Apr. 22, 2003).

[108] Messmer, *supra* note 91 (noting the problems that will occur when databases are not updated to keep track of consumers who establish new residences).

[109] Letter from Ken Wasch, President, Software & Info. Indus. Ass'n, to The Honorable Gray Davis, Governor, California (Sept. 16, 2002) (on file with Richmond Journal of Law & Technology). Obtaining and storing physical addresses at the time of the transaction would not necessarily be helpful, because up to 17% of U.S. residents change their physical address each year. *Id.*

[110] *Id.* at 3. SB 1386 does not contain a provision allowing for delayed notification while the companies determine the current addresses of their data subjects. Hackett & Caldwell, *supra* note 73, at 8. The author of the bill was asked to remedy this issue by allowing companies to rely on the addresses contained in their records at the time of the breach, however, this request was declined. Hackett & Caldwell, *supra* note 73, at 8.

[111] Although some critics have argued that this law could cause organizations to avoid collecting and retaining information regarding California residents, the task of trying to keep California residents out of your database could prove to be more expensive than complying with the law. *If It Weren't For the Weather*, *supra* note 38. Such a policy would also be fiscally unsound for businesses seeking to attract customers nationwide. It would also invite legal liability because an organization can never be totally sure that a person in its database has not become a resident of California since the time it first obtained that person's information.

[112] *April 2003 Update*, Montebello Partners, Internet Security Update, *at* http://www.montebellopartners.com/Security/Default.asp (April 2003).

[113] *Id.* at 5.

[114] *Piper Rudnick Alert, supra* note 29, at 6.

[115] *Piper Rudnick Alert, supra* note 29, at 6.

[116] *If It Weren't For the Weather, supra* note 38.

[117] Deborah Birnbach and Kimberly Nuzum, *New Law Requires Disclosure of Security Breaches*, Testa, Hurwitz & Thibeault Client Bulletin, *at* http://www.tht.com/pubs/SearchMatchPub.asp?ArticleID=939 (May 14, 2003).

[118] *See* Thibodeau, *supra* note 6 (explaining that companies have to report "not only actual compromises, but suspected compromises as well.").

[119] The Investment Company Institute (ICI) also complained during California Senate hearings because the bill requires notice whether or not there is "a suspected or expected case of identity theft resulting from the breach." Personal Information, *Privacy: Hearing on S.B. 1386 Before the Assembly Committee on Business and Professions*, 2002 Leg. (Cal. 2002), *available at* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_cfa_2–

20804_191651_asm_comm.html (Aug. 6, 2002).

[120] *Id.*

[121] Some organizations are already decrying the breadth of SB 1386 as they prepare for difficult implementation. *Meeting Minutes from the University of California at Davis Technology Infrastructure Forum at III*, *at* http://tif.ucdavis.edu/meetings/02_26_03/ (Feb. 26, 2003). For example, during the meeting cited herein, some members noted "that the task of identifying all staff and faculty who store personal information on their computers is close to impossible." *Id.*

[122] Personal Information, *supra* note 119 (estimating that the cost of compliance for the mutual fund industry will be in the "tens of millions of dollars.").

[123] Laykin, *supra* note 107, at para. 9; *see also* Hackett & Caldwell, *supra* note 73, at 7. Critics complain that the law creates a gray area that does not make clear what constitutes a "security breach." Vamosi, *supra* note 12, at para. 6.

[124] Laykin, *supra* note 107, at para. 9.

[125] Vamosi, *supra* note 12.

[126] Konrad, *supra* note 27.

[127] Konrad, *supra* note 27, at paras. 11, 20.

[128] Armour, *supra* note 22.

[129] StrongAuth, *supra* note 70, at § 108.

[130] An IDS is defined as follows:

> An intrusion detection system is now an essential part of network security defen[s]es. Firewalls will stop most unwanted traffic. But firewalls need to allow some traffic or there could be no connection with the Internet. Such 'legal' traffic can allow intruders into your LAN. . . . An intrusion detection system can detect dubious activity on the network. This can be by recogni[z]ing attack patterns, or by comparing network usage with security policy. For example, the policy may state that a particular workstation can only be used during standard office hours. If it logs on at 3:00 am, it would be reasonable to assume that something untoward is happening.

ITSecurity.com, *Firewall*, Computer Security Dictionary, *supra* note 53.

[131] *Piper Rudnick Alert, supra* note 29, at 5.

[132] *Piper Rudnick Alert, supra* note 29, at 5; *see also* Marcia Savage, California Security Law Could Bring Opportunity, CRN.com, *at* http://www.crn.com/sections/News/top_news.asp?ArticleID=42043 (May 16, 2003) (suggesting that small or less security-savvy companies could claim that they did not report a breach because they did not know about it).

[133] *Piper Rudnick Alert, supra* note 29, at 6. Organizations should be careful not assume that ignorance is bliss under SB 1386. Failing to monitor an organization's system in order to avoid discovering breaches that might trigger the notice provision would be ill-advised. StrongAuth, *supra* note 70, at § 109. Ignoring or outright avoiding information that might indicate that an organization's system is insecure could result in a finding that the organization has violated the standard of care in the industry and was, therefore, negligent. *Id.* Even if such a "see no evil hear no evil" policy could avoid liability under SB 1386, the damage to an organization's reputation when this fact is eventually exposed could be far more costly than the cost of compliance. *Id.*

[134] Poulsen, *supra* note 97, at para. 3. The statute also fails to define the word "compromised." One commentator aptly noted that "[o]nly God, or the California Supreme Court, whichever has higher jurisdiction, knows what the word 'compromises' means." *Posting of Tom Frerichs to TalkBack (April 28, 2003), at* http://forums.zdnet.com/group/zd.Anchordesk/anchordesk/anchordesktb.tpt/@thread@93153@forward@1@D-,D@ALL/@article@93153?EXP=ALL&VWM=hr&ROS=1& (commenting on Vamosi, *supra* note 12). It is, therefore, impossible to know for certain when an intrusion has resulted in a compromise. Armour, *supra* note 22, at para. 12.

[135] Poulsen, *supra* note 97, at para. 10.

[136] There is also a serious question as to whether a single incident or even a handful of incidents involving data

subjects with information stored on a breached system would motivate an organization to find that the acquisition of data resulted from the breach of the Defendant's system, as opposed to acquisition from some other source (i.e. credit card receipts stolen from the garbage, interception of data in other internet transactions, etc.).

[137] One company advertises that with its software, "organizations can forensically examine an incident in order to determine with 100 percent accuracy what information was accessed, created or deleted." Press Release, *Guidance Software's Encase Enterprises Provides Incident Response Capabilities Needs to Support Compliance of California Law SB 1386*, Guidance Software, *at* http://www.guidancesoftware.com/corporate/press/2003/20030414.shm (Apr. 14, 2003).

[138] Thibodeau, *supra* note 6 (noting that while an organization may know when someone has hacked into the system, the organization can't "know if [the hacker has] acquired information or if they have just looked at information . . . [p]otentially, you will have to send out notices to a lot of people just because you don't know" whether the information itself has been acquired.)

[139] StrongAuth, *supra* note 70, at § 108.

[140] StrongAuth, *supra* note 70, at § 108.

[141] Of course, if that organization's data subjects suffer a rash of identity thefts, a company could be deemed to have a reasonable belief that data acquisition has occurred.

[142] Cal. Civ. Code § 1798.29(d).

[143] Armour, *supra* note 22, at 3.

[144] Susan J. Wells, *Stolen Identity: When Employees Suffer From Identity Theft, Employers Also Pay the Price*, HR Magazine (reprinted by MSNBC) *available at* http://www.ucan.org/News/MSNBC1-12-03/msnbc.htm (Dec. 1, 2002).

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] "The most common definition of physical security is that it is the application of physical barriers and control procedures to protect information and information systems." ITSecurity.com, Computer Security Dictionary, *Security*, *supra* note 53.

[151] *Security: Identity Theft*, HIPAA Implementation Newsletter, LPF.com, *at* http://www.lpf.com/hipaa/issue53.html (March 14, 2003).

[152] Laykin, *supra* note 107, at 2.

[153] *California Law Protecting Computerized Personal Information Takes Effect in July*, Segal Compliance Alert, *at* http://www.segalco.com/publications/compliancealert/31903.html (March 19, 2003). Before passage, many opponents also noted their fear that SB 1386 would launch the creation of a complex and confusing patchwork of state legislation on this subject that would give rise to preemption issues where those state laws conflict with federal legislation on related topics. August 14 Appropriations Committee Analysis, *supra* note 78 (recounting that the Information Technology Association of America (ITAA) noted its concern about piece-meal creation of different legislation at the state level). There have also been unsubstantiated allegations that SB 1386 may violate "current international conventions, directives, regulations or obligations." Saundra Kae Rubel, *News You Can Use – Got California Customers? There's a New Law For You*, Privacy Knowledge Base, *at* http://www.privacyknowledgebase.com/newsUse017_s.jsp (July 9, 2003).

[154] *If It Weren't For the Weather, supra* note 38.

[155] *Will CA Law Spur Storage Crypto?,* Light Reading.com, *at* http://www.byteandswitch.com/document.asp?doc_id=31689&site=byteandswitch (April 22, 2003).

[156] StrongAuth, *supra* note 70, at § 201(l).

[157] Vamosi, *supra* note 12 (noting that "if customer data is encrypted, a company is exempt," but explaining that the strength of the encryption is not dictated by the law); *see also Will CA Law Spur Storage Crypto?, supra* note 154;