The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

COMMENT LETTER

June 14, 2002

California Senate Bill 1386, June 2002

June 14, 2002

The Honorable Steve Peace
California State Senate
State Capitol, Room 3060
Sacramento, California 95814

Re: Senate Bill 1386

Dear Senator Peace:

The Investment Company Institute[1] is writing to express our strong opposition to provisions in Senate Bill 1386 that would require any person or business that maintains a computerized data system that contains personal information to disclose any breach of the security of the system. In addition to our concerns with the overbreath and vagueness of this bill, which are discussed below, we believe that, contrary to the intent of this bill, this bill will neither reduce nor prevent identity theft. It will, however, under the guise of addressing identity theft: cost California's residents millions of dollars annually; result in unintended consequences that are injurious to the public, including impeding law enforcement and providing an incentive for hackers to hack; and, result in unduly alarming California's citizenry.

If, in fact, the California Legislature is truly concerned with issues relating to identity theft, we respectfully submit that a better way to address such concerns would be to (1) work together with law enforcement to address concerns relating to hackers and cyber terrorists and (2) provide local law enforcement and the Office of the California Attorney General with sufficient resources to combat and prosecute identity theft.[2] We further submit that by continuing to pass additional laws that will cost Californians millions of dollars annually without providing any concomitant increase in protection from identity theft, the Legislature is doing a grave disservice to Californians. We strongly urge that you reconsider the wisdom of this bill for the reasons discussed below.

I. This Bill Will Cost Californians Millions of Dollars Annually

The Institute understands that the Legislature is unsympathetic to arguments raised by industry concerning the costs associated with implementing a piece of legislation. However, with respect to the imposition of the provisions of Senate Bill 1386 by the mutual fund

industry, please know that the costs that will be incurred by complying with this bill, which are estimated to be in the tens of millions of dollars, if not in the hundreds of millions of dollars, will likely be borne not by the mutual funds themselves, but by their shareholders. This is because of the unique structure of mutual funds. Mutual funds have no employees. Instead, all services necessary to operate a fund are contracted for by a fund's board of directors and all costs incurred in operating the fund and providing any require notice to shareholders are borne directly by the fund's shareholders. As such, any costs resulting from this bill likely will be passed on directly to a mutual fund's shareholders, thereby reducing their return on investment.

To say this bill will cost a mutual fund's shareholders millions of dollars is not an exaggeration. For example, one of the Institute's members based in California has 15 million shareholders. For each breach of this firm's security system, the cost of notifying its shareholders under this bill would be approximately $5 million (i.e., 15,000,000 times the cost of postage ($.373)). This is the cost that would result from just one breach involving one company. The true cost of the bill just to investors in mutual funds is likely to be far in excess of this example. It should be noted that this cost will be in addition to the hundreds of millions of dollars in financial losses that are suffered today by businesses and governments due to breaches of computer systems.[4]

While one might argue that a mutual fund could avoid these costs by having better security, there is no computer system that exists that has impenetrable security. Indeed, the most recent survey conducted of computer security by the Computer Security Institute (CSI) in conjunction with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad resulted in the following findings:

- 90 percent of respondents, which are primarily large corporations and government agencies, determined computer security breaches within the last 12 months;[5]
- 80 percent acknowledged financial losses due to computer breaches;
- The 44 percent of respondents t hat were willing or able to quantify their financial losses, reported $455,848,000 in financial losses during the past year.[6] Most of these losses occurred through theft of proprietary information and financial fraud; and
- 34 percent reported the intrusions to law enforcement.[7]

It is important to note that these survey results are derived from computer security professionals who responded to the survey and who "… are probably more knowledgeable than the average system administrator and the companies they work for more aware of the threats."[8] This is significant because it demonstrates that the firms that may be the most knowledgeable about and concerned with the security of their computer systems have experienced a hacking rate of 90 percent.

As noted by Bruce J. Gebhardt, CSI's Executive Assistant Director, former Special Agent-in-Charge of the FBI, San Francisco, in connection with this year's CSI/FBI survey,

The United States' increasing dependency on information technology to manage and operate our nation's critical infrastructures provides a prime target to would-be cyber-terrorists. Now, more than ever, the government and private sector need to work together to share information and be more cognitive of information security so that our nation's critical infrastructures are protected from cyber-terrorists.[9]

The Institute respectfully submits that, rather than enhancing the ability of law enforcement to work together with the private sector to address issues relating to computer security and

cyber-terrorism, S.B. 1386 will impede these efforts by requiring the public broadcast of every breach of a computer system, no doubt to the advantage of cyber-terrorists and other hackers and to the consternation of law enforcement's efforts.

If a truly secure system existed, it would be utilized by private and governmental entities that today lose hundreds of millions of dollars to computer hackers and other cyber-terrorists. But, such a system does not exist and a bill such as S.B. 1386 will merely increase the costs resulting from breaches of computer systems. Moreover, as discussed below, this bill will likely provide an incentive to hackers to engage in more intrusive hacking.

II. The Bill Will Have Unintended Consequences That Are Injurious to the Public

The Institute is concerned that, in an attempt to prevent identity theft, this bill will have the unintended adverse consequences of encouraging (1) security breaches by hackers and (2) lax computer security procedures by persons maintaining computerized data systems. It is well known that computer hackers relish the attention derived from their ability to penetrate computer security systems. By contrast, businesses have very valid reasons for not publicizing a breach.10 Unfortunately, however, S.B. 1386 would no longer afford businesses the ability to remain silent about breaches of their system. Instead, the bill would require them to broadcast each and every breach to their customers—thereby ensuring the hackers the publicity they seek and encouraging other hackers to exploit the same and other computer systems.

It would not be surprising if, upon enactment of this bill, hackers target for hacking those businesses of which the hacker is a customer just to receive the public notice in order to determine whether their hacking efforts resulted in their penetrating databases that contained personal information. As such, the notification that would be required by the bill would wind up being a "report card" or sorts for the hacker—if the hacker does not receive the notice, it knows that the system does not contain such information, which in turn may provide an incentive to the hacker to try to penetrate the system again to access the personal information. We fail to understand how a bill that would encourage additional hacking of computer systems could be considered to be in the best interest of Californians.

Another likely unintended and adverse consequence of S.B. 1386 is its encouragement of businesses to have lax computer systems. As drafted, a business need only notify a person whose personal information was, or may have been breached, once the business discovers the system was breached.11 An easy way to avoid having to provide the required notice would be to never take the necessary steps to determine whether a breach has occurred. As such, those businesses that are conscientious about their computer security and that actively monitor the system on an ongoing basis will be disadvantaged by this bill because they are the same businesses that are most likely to discover a breach. By contrast, a business that maintains a computer system but never bothers to address the security of the system or monitor the system for breaches, need never worry about this bill because it will have no duty to report those breaches of which it has remained deliberately ignorant. Again, we fail to see how a bill with this result can be said to address concerns with identity theft.

III. The Notice Required by the Bill Will Needlessly Alarm the Public

The Institute is concerned that the notice that would be required by S.B. 1386 will result in needlessly alarming the public by requiring a notification of a breach in instances in which there has been no access to personal information and there is no concern with possible identity theft.[12] Moreover, as discussed above, such public broadcast of the breach may serve to impede the ability of law enforcement to combat hacking and cyber-terrorism. Also, even in instances in which personal information may have been accessed, providing a notice to the public will not enable them to take any meaningful prophylactic precautions to protect themselves in response to the notice.[13] Instead, by requiring such broad publication of a breach, the bill will needlessly alarm persons without regard to whether their information was breached and leave them to worry about something outside their control. As such, we are at a loss to understand how the bill could possibly be in the best interest of Californians.

IV. The Bill is Poorly Drafted and Will Have Far Reaching Consequences Not Consistent With Its Intent

A. "Breach" Includes Innocuous Access to Information

As proposed to be defined in the bill, "breach of the security of the system," would mean any unauthorized access to personal information contained in a database. As such, a breach would include not only a person from outside the company trying to hack into the company's computer system, but also an employee of the company accessing information that the employee is not authorized to access. With respect to the later type of breach, under the bill it matters not whether the unauthorized access was inadvertent or which malice intent; nor does it matter whether any personal information accessed was looked at, copied, reviewed, used, or misused; nor does it matter whether any personal information accessed was innocuous or material—just the mere fact that the employee had access to the information would trigger the notice requirements of the bill. As such, the bill fails to limit its reach to its stated intent—addressing identity theft and the misuse of a person's personal information—and winds up being an overly broad piece of legislation that will impact conduct having no nexus whatsoever to the misuse of personal information or identity theft.

B. The Bill Incorrectly Presumes the Extent of a Breach Can be Determined

In addition to the Institute's concerns with the bill reaching harmless or innocuous conduct, the Institute is concerned with the bill's simplistic and naïve view of computer systems. In particular, the bill seems to posit that in the event of a breach of its computer system, the business can determine what information was accessed in connection with the breach. This, however, is not always the case. As a result, under this bill, a business learning of a mere penetration of the system would have a duty to notify all persons whose information is contained in the system, even though no personal information may have been accessed and even though, as noted above, such notice may only result in needlessly alarming persons to an occurrence in response to which they cannot take prophylactic measures.

C. The Bill May Impact Non-Californians

The bill also fails to address how its provisions are to apply in the event the data system

that is breached is maintained outside the State of California even though it may (1) be used by a business in California or (2) contain information on residents of California. As such the bill would seem to have extra-territorial impact, resulting in California exporting its poor public policies to other states whose Legislatures, unlike California's, have not proposed to enact such misguided legislation and who are not willing to impose upon their citizenry the millions of dollars in costs that will result from passage of this bill. We recommend that this bill be amended to ensure that the "protections" intended by the bill are appropriately limited to constituents of the California Legislature so that industry can attempt, to the extent possible, to ensure that only those persons residing in California bear the substantial costs that will result from this bill.

* * *

For the above reasons, the Institute strongly opposes the enactment of S.B. 1386. As noted above, if, in fact, the California Legislature is truly interested in preventing identity theft, we recommend that, rather than passing misguided legislation such as S.B. 1386, it work together with law enforcement to address these concerns and, most importantly, that it commit the necessary resources to law enforcement and prosecutorial agencies to ensure that, if such theft occurs, it is expeditiously investigated and prosecuted.

Indeed, if the sponsor is intent on mandating that notice be provided of a breach, such notice would be more appropriately directed to the police or law enforcement agencies that could investigate and prosecute any violations of law. This approach would avoid the needless costs that would result from having to notify each person whose personal information was included in the security system; avoid the alarm that would result to persons who would be required to receive notice under the current version of S.B. 1386; and, ensure that hackers not be rewarded for their success hackings through publicity.[14]

Sincerely,

Tamara K. Reed
Associate Counsel

ENDNOTES

[1] The Investment Company Institute is the national association of the American investment company industry. Its membership includes 8,984 open-end investment companies ("mutual funds"), 504 closed-end investment companies and six sponsors of unit investment trusts. Its mutual fund members have over 88.6 million individual shareholders, including approximately 12.3 million shareholders in California.

[2] The Institute understands that, due to the limited funding provided to the Office of the California Attorney General by the Legislature, the Office has but one person dedicated statewide to prosecuting cases involving identity theft.

[3] As of July 1st of this year, the cost of a first class stamp will be $.37.

[4] See the third bullet in the following discussion.

[5] According to Bruce Schneier, Founder and Chief Technology Officer, Counterpane Internet Security, Inc., a renowned expert and author of several books on computer security, "What's interesting is that all of these attacks occurred despite the wide deployment of security technologies: 95% [of the 2001 survey's respondents] had firewalls, [and] 61% an

[intrusion detection system]… .” See Counterpane Internet Security, Crypto-Gram Newsletter (April 15, 2001), at p. 4 (emphasis added). Schneier’s comments were on the 2001 CSI/FBI survey in which 64 percent of respondents reported “unauthorized use of computer systems” during the previous year.

6 This $455,848,000 in losses was the cumulative total reported by 223 survey respondents.

7 See, “Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row.” CSI Press Release (April 7, 2002) (www.gocsi.com/press). As regards this last bullet, according to Bruce Schneier, “More people are reporting these incidents to police (36% in the previous year’s survey). Those who didn’t report were concerned about negative publicity and competitors using the incident to their advantage.” Id. Schneier’s comments were on the 2001 CSI/FBI survey in which only 36 percent of respondents indicated that they had reported intrusions to law enforcement.

8 Id.

9 See footnote 7.

10 For example, the business may be working with law enforcement to address the breach and does not want to tip the hacker off regarding the investigation. Also, the business may be concerned that by publicizing a breach it will: encourage other hackers to penetrate the system; encourage the same hacker to penetrate deeper into the system; unduly alarm customers; or be used to the business’s disadvantage by competitors.

11 See proposed Section 4 of the bill creating Section 1798.82(a) of the Civil Code. (Emphasis added.)

12 This is because the bill would require notification if personal information “was, or may have been, accessed by an unauthorized person.” See proposed Section 4 of the bill creating Section 1798.82(a) of the Civil Code. (Emphasis added.)

13 We understand that in response to the recent breach of the California’s personnel database, the State of California agreed to provide its employees with the ability to block access to the employees’ credit files maintained by credit agencies. While such block may limit the ability of identity thieves to obtain new credit in such persons’ names, it will likely have no impact on the ability of such thieves to utilize an employee’s existing credit or to use the employee’s identity in ways not impacting credit—e.g., bank accounts, securities accounts, retirement accounts, etc. Moreover, it is possible that facilitating the ability of these employees to place a block on the release of their credit information may lull them into a false sense of security by leading them to believe that such block provides them meaningful protection from a theft of their identity not involving a credit report, when, in fact, it does not.

14 While this recommendation would address many of the concerns with the bill, it does not address the extra-territorial reach of the bill nor the fact that the bill seems to presume that a business can determine the extent of a breach when its computer system is accessed by an unauthorized person.