Docket No. 09-15971

In the

United States Court of Appeals

for the

Ninth Circuit

JOEL RUIZ, on behalf of himself and all others similarly situated,

Plaintiff-Appellant,

v.

GAP, INC. and VANGENT, INC.,

Defendants-Appellees.

Appeal from a Decision of the United States District Court for the Northern District of California, No. 07-CV-05739 · Honorable Samuel Conti

BRIEF FOR THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AND THE RETAIL INDUSTRY LEADERS ASSOCIATION AS *AMICI CURIAE* IN SUPPORT OF APPELLEES GAP INC. AND VANGENT, INC. FOR AFFIRMANCE

ROBIN S. CONRAD, ESQ.
AMAR D. SARWAL, ESQ.
NATIONAL CHAMBER LITIGATION CENTER, INC.
1615 H Street, N.W.
Washington, District of Columbia 20062
(202) 778-1800 Telephone

W. STEPHEN CANNON, ESQ.
RAYMOND C. FAY, ESQ.
Counsel of Record
EVAN P. SCHULTZ
CONSTANTINE CANNON LLP
1627 Eye Street, N.W.
10th Floor
Washington, District of Columbia 20006
(202) 204-3500 Telephone
(202) 204-3501 Facsimile

Attorneys for Amici Curiae, Chamber of Commerce of the United States of America and Retail Industry Leaders Association

COUNSEL PRESS · (800) 3-APPEAL

PRINTED ON RECYCLED PAPER

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 29(c), *amici* state as follows:

The Chamber of Commerce of the United States of America has no parent corporation, and no subsidiary corporation. No publicly held company owns 10 percent or more of its stock.

The Retail Industry Leaders Association has no parent corporation, and no subsidiary corporation. No publicly held company owns 10 percent or more of its stock.

Dated: November 16, 2009

By: s/ Raymond C. Fay
Raymond C. Fay

Attorney for Amici Curiae

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE

CASES:

STATUTES:

OTHER AUTHORITIES:

INTERESTS OF *AMICI CURIAE*

The Chamber of Commerce of the United States of America ("the Chamber") is a nonprofit corporation and the world's largest business federation. The Chamber represents 300,000 direct members and indirectly an underlying membership of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. The Chamber represents the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases raising issues of vital concern to the nation's business community.

The Retail Industry Leaders Association ("RILA") is the world's leading alliance of retailers, and of those who provide products and services to retailers. RILA represents many of the largest retailers in California and throughout the United States. Worldwide, RILA's members collectively account for more than $1.5 trillion in annual sales, provide millions of jobs, and operate over 100,000 stores, manufacturing facilities, and distribution centers both domestically and globally. In addition to other services that it offers to its members, RILA represents its members' interests through advocacy with various arms of the government and through the filing of briefs in judicial proceedings.

The Chamber and RILA have tens of thousands of members who, as businesses, routinely obtain electronic personal information of customers, employees, potential employees, and others. Members of the retail and business communities receive such electronic personal information for any number of reasons, aimed at increasing the efficiency and quality of their businesses and improving the experience of the customers they serve. These wholly legitimate purposes include screening job applicants (as occurred in this case); administering various human resources programs for employees; processing payment or shipping information from customers; running customer loyalty programs; and analyzing demographic trends involving marketing, consumers, products, and services. Without such information, most businesses would likely find it impossible to function in today's complex commercial world, which is increasingly dependent on electronic commerce and transactions.

The members of the Chamber and RILA take seriously their responsibility to safeguard personal identifying information. Unfortunately, a stark reality of today's business world is the existence of criminals who target businesses and their property, including valuable equipment like computers and valuable information like personal identification data. Despite the best efforts of retailers and businesses to protect their property and their data, sometimes the thieves succeed.

According to the arguments made by Mr. Ruiz, and properly rejected by the District Court, each and every one of these criminal acts that potentially compromises personal information could subject retailers and businesses to automatic liability. If Mr. Ruiz succeeds here, good corporate citizens will find themselves facing a new strain of baseless litigation along with the risk of adverse jury verdicts, founded on the mere speculative fear that someone might misuse stolen personal information. Accordingly, the members of the Chamber and RILA have an acute interest in the outcome of this case, and in this Court's affirmance of the District Court's summary judgment rejecting Mr. Ruiz's legal claims.

INTRODUCTION AND SUMMARY OF ARGUMENT

In this case, two companies acted in an exemplary manner after a criminal stole two laptop computers, one of which contained certain personal information of about 744,000 people. Going above and beyond the laws of any state, Gap offered notice, credit-monitoring services, and insurance to every potentially affected individual. But if the plaintiff-appellant in this case prevails on his theory to recover for the speculative harm of fear of future misuse of personal information, then companies that provide an aggressive response to data breaches will face certain litigation from exactly the persons whom the aggressive response is intended to protect, just like the case that Mr. Ruiz has brought. As a result, companies will have a disincentive to provide notice except when laws clearly

require them to do so. If that happens, then Mr. Ruiz's case will, in the future, leave individuals with fewer options to make their own assessment of the risk of the actual harm that might result from the loss of personal data.

Mr. Ruiz's legal theory would create this disincentive because the 48 jurisdictions in the United States that have passed data notification laws require very different triggers for notice. For example, many states provide explicitly that notice is required only when there is a reasonable likelihood that the data breach will result in harm to an individual. Other states, such as Connecticut, flip the standard and provide that notice must be provided except where the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. *See, e.g.*, CONN. GEN. STAT. § 36a-701b(b). In still other states, including Texas, where Mr. Ruiz lives, notice is triggered based upon a determination that the unauthorized access of the data has compromised personal information. *See, e.g.*, TEX. BUS. & COM. CODE ANN. § 521.053. If companies face litigation based on strict liability whenever a loss of data occurs, then companies will contact only those individuals clearly required by state laws to be notified. Other potentially affected individuals will receive no notice that their personal data has been lost.

Similarly, Mr. Ruiz's attempt to recover for merely speculative harm would work a radical departure from the well-established law of negligence. In California

and in other jurisdictions, negligence requires an injury that is both present and appreciable. Yet the injury that Mr. Ruiz asserts is the very definition of speculative—he has not himself presented any material evidence that he or any other person notified about the laptop threat suffered any harm. In general, only a minute fraction of individuals whose data has been lost suffers actual misuse of personal data. Thus, allowing Mr. Ruiz to recover for such a purely conjectural, uncertain, future harm would expose every business in America to the specter of nonstop litigation whenever victimized by a crime that potentially compromises personal data.

In short, no state or federal court has ever permitted a bare "fear of identity theft" claim, like what Mr. Ruiz asserts here, to survive summary judgment. The precedent is uniform, and uniformly correct, because the requirement of actual injury is a fundamental element of tort claims. A shift from this unbroken precedent could have unintended ramifications, harmful to companies and to individuals alike, with regard to notification of individuals following a data breach.

Accordingly, this Court should affirm the District Court.

ARGUMENT

I. Appellant's Legal Theory Would Hamper The Ability Of Individuals To Receive Timely Notice Of Lost Data.

In this case, following the criminal theft of a laptop containing the personal information of some 744,000 individuals, Gap and Vangent decided to give notice

to ***everyone*** whose personal data was potentially contained on the stolen computer. Brief for Appellees, at 5. These companies did this for individuals across the country whose personal information might have been in the stolen laptop. *Id.* In giving this widespread notice, Gap and Vangent went far beyond the legal requirements of the many states that require a company to send notice of a data breach to affected individuals ***only*** when harm is reasonably likely to occur. But should this Court reverse the District Court, then Mr. Ruiz will have succeeded in establishing a legal foundation for holding "Gap and Vangent strictly liable for the loss of his personal data." Brief for Appellees, at 2. Put another way, Mr. Ruiz seeks to hold companies strictly liable for a speculative injury—the mere fear that individuals' lost data might be misused. If such a rule were to apply, companies would need to brace for a deluge of lawsuits, including class-action litigation, every time they send out data breach notices.

The resulting disincentive is inevitable: if Mr. Ruiz were to prevail here, then companies would send out notice of data losses only when the governing law clearly requires it. Companies like Gap and Vangent who serve notice more widely than the law requires could expect only a legal complaint in return. And individuals whose data has been taken could expect to receive notice less frequently, leaving them less informed, and so less able to take the actions they see fit to prevent actual harm resulting from active fraud. Such a situation would not

serve the interests of either companies or individuals. It is better for all to let the underlying policy of the notice laws be served—by giving individuals information they can use to make their own decisions of how to protect themselves—than to provide a disincentive to give notice.

A. Different states have different triggers requiring when to send out notice of data breaches.

In the United States, 48 jurisdictions have passed laws requiring companies to notify individuals of breaches of their personal data.[1] The states have very different standards.

For instance, the California law states that "[i]n this section, 'breach of system security' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person." In dozens of jurisdictions, the state legislatures call for notification using some variation of a formula that requires notification only when harm from misuse of the data is reasonably likely. Five states within the Ninth Circuit follow this approach. So, in Alaska, "disclosure is not required if . . . the covered person determines that there is not a reasonable

---

[1] These 48 jurisdictions include 45 states, plus the District of Columbia, Puerto Rico, and the Virgin Islands. *See* National Conference of State Legislatures, STATE SECURITY BREACH NOTIFICATION LAWS, http://www.ncsl.org/Default.aspx?TabId=13489. For the sake of convenience, this brief refers to all of these entities as both "states" and "jurisdictions."

likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach." ALASKA STAT. § 45.48.010(c). In Arizona, notice is required only where the breach "causes or is reasonably likely to cause substantial economic loss to an individual." ARIZ. REV. STAT. ANN. § 44-7501. In Hawaii, a company must send notification only in certain circumstances, and even then only "where illegal use of the personal information has occurred, or is reasonably likely to occur and . . . creates a risk of harm to a person." HAW. REV. STAT. § 487N-1. Similar provisions apply in Idaho (*see* IDAHO CODE ANN. § 28-51-105(1)), Oregon (*see* OR. REV. STAT. ANN. § 646A.604(7)), and Washington (see WASH. REV. CODE ANN. § 19.255.010). For a full list of the jurisdictions that require notice only when harm is likely to result, *see* Table 1, below.

B. The actions of Gap and Vangent demonstrate the incentives that companies currently have to send notice out widely.

In this case, the stolen laptop computer contained personal information for 744,000 people across the country. Upon discovering the data loss, Gap and Vangent could have limited their responses to the requirements of the laws in the different jurisdictions. That is, the companies could have broken down the list of individuals into groups based on the states in which the individuals resided, or based on the states in which the companies conducted business, and then they could have limited their response to the letter of the law in each of those

jurisdictions. So, Alaska residents could have received notice only where the data breach presented a reasonable likelihood of harm. And, under Arizona law, individuals would have received notice only when the breach was reasonably likely to cause substantial economic loss.

Instead, Gap and Vangent elected to provide notice to all individuals whose data was potentially on the stolen laptop. Rather than parsing closely the different laws to try to find a reason to withhold notice, the companies did exactly the opposite—they provided notice to ***everyone*** whose data was potentially in the stolen laptop. Indeed, they went beyond the requirements of any state law by taking the further steps of setting up a toll-free hotline and web page to help the job applicants, granting free credit-monitoring for one year to each of the individuals whose data had been taken, and even offering $50,000 in fraud insurance. Brief for Appellees, at 5.

Gap and Vangent could act in this responsible manner because no state imposes strict liability on a company that has suffered a crime resulting in potential loss of data. As a result, the companies here provided the early notice to help stop any actual misuse of data. Acting under a consistent body of law recognizing that data loss alone is insufficient to impose liability, the companies armed individuals with the information they needed to protect themselves from misuse of their data—before any such misuse occurred. Significantly, ***none*** of the 744,000 potentially

affected individuals have had their personal data misused due to the incident at issue here. Brief for Appellees, at 7-8.

C. The nationwide class action that Mr. Ruiz seeks to form would discourage companies from sending out notice more widely than is strictly necessary.

If the rule that Mr. Ruiz seeks were imposed, companies would have drastically different incentives. With the specter of strict liability hanging over them, companies whose systems were breached would face the prospect of burdensome litigation and potentially tremendous adverse verdicts.

In that scenario, companies would face a situation in which no good deed would go unpunished. Companies would be moved to scrutinize more closely the laws of each jurisdiction in which an affected individual lived, to determine whether the governing state law clearly required notification. This often would entail making a determination of whether harmful misuse of data was reasonably likely to occur. In the circumstances where the companies determined, following the appropriate legal criteria, that an individual did not face a likelihood of actual harm, companies would have a disincentive to give such notice. Without notice, individuals would lack the knowledge to make their own decisions about what precautions to take to guard against actual data misuse and would result in varied notice being provided based on the state in which the individual happened to reside.

This case illustrates precisely what is at stake. After Gap and Vangent sent out the notice to everyone whose personal information was in the stolen laptop, Mr. Ruiz responded by pursuing a nationwide class action. His class-action certification was not limited to individuals who may have been covered by California's law. Rather, the class action sought to include individuals residing in states whose laws might not have required notice by the bare fact that a laptop computer containing personal information was stolen. Mr. Ruiz sought to act as the lead plaintiff for "***[a]ll persons*** who applied for an in-store position with a Gap, Inc. brand store through Gap, Inc. and Vangent, Inc's . . . application process." Appellees' Supplemental Excerpts of the Record, at SER-97 (emphasis added). *See also id.,* at 113 (discussing inclusion of "out-of-state members" in the class).

Thus, Mr. Ruiz sought to include in his class individuals who lived outside of California, many of whose states provide for different notification standards than California's. Given that Gap and Vangent volunteered to follow a conscientious course of action, all affected individuals received the benefit of notice of the data loss. If Mr. Ruiz succeeds in imposing strict liability for data losses and for the fear of data misuse, companies will likely not freely volunteer the sort of widespread notice that the companies offered here, to avoid litigation precisely like the case that Mr. Ruiz has brought.

II. Negligence Law Recognizes Only Actual Injuries.

A. The "appreciable, nonspeculative, present harm" element of a negligence claim is essential in California and elsewhere.

A significant portion of Mr. Ruiz's theory of recovery relies on his assertion that Gap and Vangent failed to exercise due care, and so are liable under California's law of negligence. But it is fundamental to tort law that plaintiffs can receive compensation only for actual harms that manifest themselves in the present—types of harm that Mr. Ruiz simply did not suffer in this case.

As the District Court held, "Ruiz's case hinges on his increased ***risk*** of ***future*** identity theft." *Ruiz v. Gap, Inc.*, Inc., 622 F. Supp. 2d 908, 913-914 (N.D. Cal. 2009). This is not enough. "Under California law, ***appreciable, nonspeculative, present*** harm is an essential element of a negligence cause of action." *Id.* at 913 (citing *Aas v. Super. Ct.*, 12 P.3d 1125, 1138 (Cal. 2000) (emphasis added).[2] And these requirements are not unique to California. "[T]he essential elements of a negligence claim are the same or similar" in jurisdictions throughout the country. *Id.* at 916.

---

[2] "Appreciable and actual damage" is also an essential element of a breach of contract claim in California. *Id.* at 917 (*citing St. Paul Fire and Marine Ins. Co. v. Am. Dynasty Surplus Lines Ins.*, 101 Cal. App. 4th 1038, 1060 (2d Dist. 2002)). Thus, the concerns raised here about the impact on businesses of removing that "actual damage" requirement apply equally to breach of contract claims arising from alleged loss of personal information.

B. Fear of data misuse does not constitute an actionable injury.

The sort of harm that Mr. Ruiz asserts is his ***fear*** that his personal data might be misused in the ***future***. *See* Opening Brief of Appellant Joel Ruiz, at 41-42 (stating that Mr. Ruiz "does not presently have a diagnosed injury, *i.e.*, identity theft or fraud").[3] But this cannot support a negligence action. As the Seventh Circuit has held, "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy." *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007).

There is good reason to prohibit, along these lines, tort recovery for the mere fear of future misuse of personal data. Such harm is by definition speculative because no actual harm has yet occurred. In addition, as a factual matter, virtually all data breaches do not lead to any misuse of information. According to a 2007 study of actual data breaches performed by Id Analytics, for the category of data

---

[3] Mr. Ruiz also asserts that money he decided to spend for his own credit-monitoring services counts as damages. However, such a voluntary payment for a speculative harm is not sufficient to support a claim of negligence. *See Shafran v. Harley-Davidson, Inc.*, No. 07-CV-01365, 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008) (stating courts "have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy."); *see also Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 633 (7th Cir. 2007) (quoting the holding of the district court in that case stating "[t]he expenditure of money to monitor one's credit is not the result of any present injury, but rather the anticipation of future injury that has not yet materialized").

most vulnerable to fraud "the highest rate of misuse was 0.098 percent—less than one in 1,000 identities."[4] In a courthouse, such chances can hardly serve as the foundation for a plaintiff to show that he has suffered the necessary "appreciable" harm. And, of course, there is nothing "present" about a mere risk of harm in the future, no matter the odds that it could occur.

C. Permitting recovery based on Mr. Ruiz's theory would subject American businesses to tremendous litigation burdens and liability.

Holding that Mr. Ruiz deserves a trial in this case, where he has presented no material facts to support his claims, would amount to a license for free-for-all litigation against all businesses in America—indeed, virtually every institution, including governmental, educational, and both for- and not-for-profit organizations—that are unfortunate enough to have data stolen. Criminals have gained potential access to myriad personal records from U.S. organizations through hacking and other means, such as the theft of a computer, as occurred in this case. Following the reasoning of Mr. Ruiz, each of the individuals whose information was taken or accessed can sue for the mere fear that their personal data might be misused. Like Mr. Ruiz has done in this case, each of those plaintiffs could sue for

---

4 *See* ID Analytics, NATIONAL DATA BREACH ANALYSIS, www.idanalytics.com/assets/pdf/National_DataBreach_FAQ.pdf, at 1. The District Court denied a motion to take judicial notice of this study.

millions of dollars, attempt to certify a class action, demand in-depth discovery, and then amend their complaints to draw in still more parties, each of whom would in turn be subject to these burdens. All this would take place on the basis of a fear of a remote chance of actual misuse of personal data. This reasoning would constitute a radical departure in tort law, and would strike a blow to every business in America. The better course, for businesses and individuals both, is to maintain the current requirements of negligence law, which demand that a plaintiff present evidence of an actual injury—one that is appreciable, nonspeculative, and present—in order to recover.

* * * * *

In sum, this case demonstrates why no court has allowed a case like Mr. Ruiz's to proceed beyond summary judgment. This Court should not open the door by holding that Mr. Ruiz's claims, based on the speculative harm of fear of future identity theft, present triable issues. First, such lawsuits raise the danger that individuals whose personal data has been stolen will lack information they need to take action to protect themselves. If this Court allows plaintiffs such as Mr. Ruiz to hold companies strictly liable for data losses, then companies may choose to provide no more notice than the varied existing notification laws clearly require. That would serve the interests of neither companies nor of individuals. Second, the fear of future data theft is so speculative that the current law of negligence does not

recognize it as an actionable injury. A holding by this Court recognizing such a fear as an injury would mark a fundamental change in the law of negligence. It would also leave retailers, other businesses, universities, and governmental entities vulnerable to nonstop litigation based on the mere fear of a future harm. Following a data security incident or the theft of physical property that contains personal identification information, there is always an amorphous fear of potential identity theft. But this unsubstantiated risk has never sufficed to serve as the basis for compensation in tort law. This Court should not now permit such a stark departure from existing law, based on mere speculation.

CONCLUSION

For the foregoing reasons, the judgment of the District Court should be affirmed.

TABLE 1

JURISDICTIONS THAT REQUIRE NOTIFICATION OF DATA BREACHES WHEN HARM WILL LIKELY RESULT

STATE	STATUTE	STATUTORY TEXT
Alaska	ALASKA STAT. § 45.48.010(c)	[D]isclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach.
Arkansas	ARK. CODE ANN. § 4-110-105(d)	Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.
Arizona	ARIZ. REV. STAT. ANN. § 44-7501(G),(L)(1)	A person is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur . . . that causes or is reasonably likely to cause substantial economic loss to an individual.
Colorado	COLO. REV. STAT. § 6-1-716(2)(a)	[A]s soon as possible . . . unless the investigation [by the business] determines that the misuse of information . . . has not occurred and is not reasonably likely to occur.

Connecticut	CONN. GEN. STAT. § 36a-701b(b)	Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.
Delaware	DEL. CODE ANN. tit. 6, § 12B-102(a)	If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible.
Florida	FLA. STAT. § 817-5681(10)(a)	[N]otification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed.
Hawaii	HAW. REV. STAT. §§ 487N-2(a), 487N-1	[F]ollowing discovery or notification of the breach. 'Security breach' means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person.

Iowa	IOWA CODE § 715C. 2(6)	[N]otification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach.
Idaho	IDAHO CODE ANN. § 28-51-105(1)	If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible.
Kansas	KAN. STAT. ANN. § 50-7a02(a)	If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible.
Maryland	MD. CODE ANN. COM. LAW § 14-3504(b)(2)	If, after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach.
Maine	ME. REV. STAT. ANN. tit. 10, § 1348(1)(B)	[S]hall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.

Michigan	MICH. COMP. LAWS § 445.72(12)(1)	Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state [whose information was subject to the breach].
Missouri	MO. REV. STAT. § 407.1500(2)(5)	[N]otification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach.
Nebraska	NEB. REV. STAT. § 87-803(1)	[W]hen it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.

New Hampshire	N.H. REV. STAT. ANN. § 359-C: 20(I)(a)	[W]hen it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.
New Jersey	N.J. STAT. ANN. § 56: 8-163(a)	Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible.
Ohio	OHIO REV. CODE ANN. § 1349.19 (10)(B)(1)	[F]ollowing its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.
Oklahoma	OKLA. STAT. tit. 24, § 163A	[F]ollowing discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.

Oregon	OR. REV. STAT. § 646A.604(7)	[N]otification is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, the person determines that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach.
Rhode Island	R.I. GEN. LAWS § 11-49.2-4	Notification of a breach is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired.
South Carolina	S.C. CODE ANN. § 39-1-90(A)	[F]ollowing discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.
Utah	UTAH CODE ANN. § 13-44-202(1)(b)	If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.

Virginia	VA. CODE ANN. § 18.2-186.6(B)	If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay.
Vermont	VT. STAT. ANN. tit. 9, § 2435(d)(1)	Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination that the misuse of the personal information is not reasonably possible pursuant to the requirements of this subsection.
West Virginia	W.VA. CODE § 46A-2A-102(a)	[F]ollowing discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.

Wyoming	WYO. STAT. ANN. § 40-12-502(a)	[W]hen it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Wyoming resident.

Respectfully submitted,

s/ Raymond C. Fay

November 16, 2009

W. STEPHEN CANNON
RAYMOND C. FAY
Counsel of Record
EVAN P. SCHULTZ
CONSTANTINE CANNON LLP
1627 Eye Street, N.W.
Washington, DC 20006
(202) 204-3500 Telephone
(202) 204-3501 Facsimile

ROBIN S. CONRAD
AMAR D. SARWAL
NATIONAL CHAMBER LITIGATION CENTER, INC.
1615 H Street, N.W.
Washington, DC 20062
(202) 463-5337 Telephone

Attorneys for *Amici Curiae*

CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C) and Ninth Circuit Rule 32-1, this brief is proportionately-spaced, has a typeface of 14 points and contains 5,486 words, excluding the table of contents, table of authorities, and signatures and certificates of counsel.

s/ Raymond C. Fay
Raymond C. Fay

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on November 16, 2009.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

s/ Raymond C. Fay
Raymond C. Fay