# The Lares Institute

Data Breaches and the Phantom Damage Allegation

July 2011

## TABLE OF CONTENTS

## I. EXECUTIVE SUMMARY

The Lares Institute is pleased to present the results of *Data Breaches and the Phantom Damage Allegation*. There are a number of different reasons for companies to take data security and privacy seriously, which include: regulatory enforcement; brand damage; loss of market capitalization; and many others. Indeed, the recent, privacy-related allegations against a long-standing British newspaper, which effectively put the newspaper out of business, show the serious implications of a privacy mishap. Moreover, identity theft is a problem that presents a number of different potential issues for individuals and companies, and it can include the creation of new credit accounts, issues with medical records in the case of medical identity theft, misuse of existing credit accounts, and others.

However, when data breach cases are litigated, there are questions raised as to whether the information that was breached was actually used for identity theft, and as a result, plaintiffs typically raise claims that they are subject to increased risk of identity theft, though they have not suffered economic harm. A case arising from a retailer's alleged data breach presents a typical view of courts:

> Therefore, because the specific factual allegations of the Amended Complaint do not allege that the Plaintiff has personally experienced any injury other than 'hav[ing] been subjected to a substantial increased risk of identity theft or other related financial crimes,' the Court must accept the specific allegations Plaintiff makes as a true representation of the injury that the Plaintiff has suffered.[1]

Courts almost unanimously reject plaintiffs' attempts to plead damages because the plaintiffs are unable to present specific evidence of losses or damage, and this can be expressed by courts as a lack of "standing" to bring a claim, a plaintiff's inability to prove causation, or damages. The goal of this study was to help determine whether the courts are coming to the proper conclusion by asking survey participants if they could trace any unreimbursed losses back to a data breach. 30 percent of the participants responded that they had received a data breach notification in the last twelve months, 2 percent claimed they had suffered identity theft which they could not trace back to a specific security breach, and only 1 percent responded that they were able to trace losses to a specific data breach.

Furthermore, participants were asked to state how they were able to trace their losses to a specific breach. The responses call into question whether the 1.4 percent of participants who claim they could trace the losses back to a specific data breach could, in fact, trace the losses. This study supports the decisions made by courts in rejecting data breach claims, because plaintiffs cannot show loss resulting from a data breach.

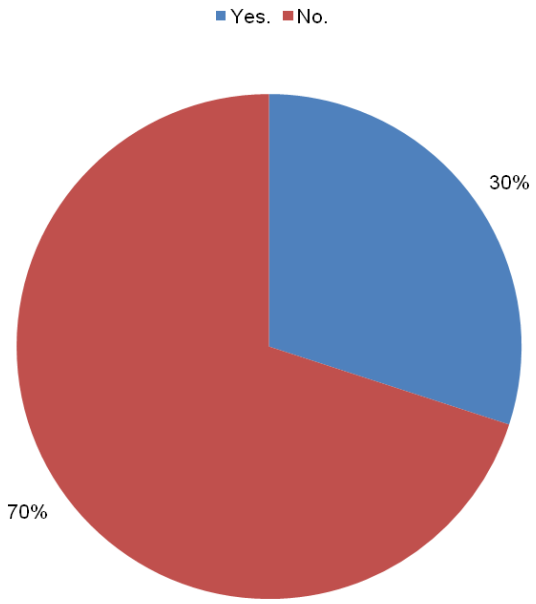
[1] *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 688–69, 66 Fed. R. Serv. 3d 447 (S.D. Ohio 2006) citing *Courtney v. Smith*, 297 F.3d 455, 459, 2002 FED App. 0248P (6th Cir.2002).

## II. KEY FINDINGS OF THE SURVEY

The survey focused on data breach notifications received by the survey participants, and whether they had any unreimbursed losses that were attributable to a security breach. The following section presents the findings of the survey.

Survey participants were asked whether they had received notice of a security breach within the last twelve months. 30 percent responded that they had, and 70 percent responded that they had not.

**Chart 1:**
Q. Have you received notice of a security breach in the last 12 months?




Of those who had received notice, 94 percent received between one and five, 2.7 percent received between six and ten, 2.7 percent received between eleven and thirty, 0 percent received between thirty and fifty, and less than 1 percent responded that they received more than fifty.

**Chart 2:**

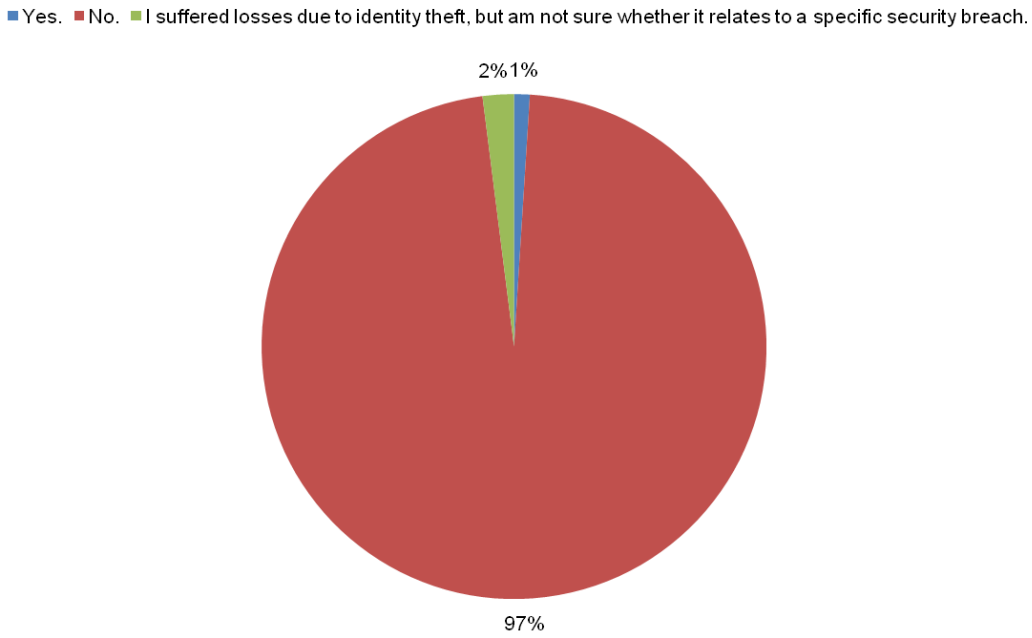
Q. If so, how many notices have you received in the last 12 months?

| Number of Notices Received in the Last 12 Months | |
|---|---|
| **Answer Options** | **Response Percent** |
| 1-5. | 94.0% |
| 6-10. | 2.7% |
| 11-30. | 2.7% |
| 31-50 | 0.0% |
| More than 50. | 0.7% |

Survey participants were then asked if they had any unreimbursed losses that they could trace to a security breach that occurred in the last twelve months. 97 percent responded that there were none, while 2 percent suffered losses due to identity theft, but were not sure if it related to a specific breach, and 1 percent said there were some losses that were traceable to a specific security breach.

**Chart 3:**

Q. Have you experience any unreimbursed losses that you could trace to a security breach that occurred in the last 12 months?




Survey participants were then told to state how they were able to trace their losses to a specific security breach. None of the answers were able to provide details tying a breach to a loss; at most they were only able to trace it back to the person who used the information, not to the actual breach, which included statements like “unknown text bill charges” and “A purchase in a state I do not (nor have ever) lived…”

## III. SURVEY METHODS

Results from this survey are based upon an internet-based survey instrument that sent surveys to a representative sample of individuals, which resulted in a sufficiently large number of responses. The survey was sent to 474 individuals in the United States, and 420 responses were received, for an 88.6 percent response rate. The margin of error of this survey is 5% at a 95% confidence level. The demographics of the survey sample generally track the U.S. Census, and are available upon request from the Lares Institute.

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings, such as non-response bias, as it is possible with any survey that individuals who did not participate would respond differently than those that did. Moreover, question wording, other survey concerns, and sampling error can result in error or bias in the findings of surveys. Finally, survey research is based upon the quality and integrity of confidential responses that the Lares Institute received from survey participants.

## IV. A SUMMARY OF THE APPLICABLE LEGAL STANDARDS

Plaintiffs in data breach litigation must prove that they have standing to bring a claim, as well as harm that is proximately caused by a defendant's conduct.[2] In dismissing a case for lack of standing, the Southern District of New York, stated:

> The Court concludes that Plaintiffs lack standing because their claims are future-oriented, hypothetical, and conjectural. There is no "case or controversy." And, as noted, several other courts have reached the same conclusion in factually similar cases, both where data have been lost and where data have been stolen. For example, in *Randolph,* where a laptop computer belonging to defendant's employee and containing the personal data of some 13,000 individuals was stolen from the employee's home, plaintiffs alleged that they had been "placed at a substantial risk of harm in the form of identity theft" and that they had "incurred and will incur actual damages in an attempt to prevent identity theft by purchasing services to monitor their credit information." The court in *Randolph* determined that plaintiffs had "failed to demonstrate an injury that is sufficiently 'concrete and particularized' and 'actual or imminent.' And, in *Giordano v. Wachovia Securities, LLC, supra,* where a report containing financial information about plaintiff and tens of thousands of other customers was lost in transit and plaintiff "only allege[d] a potential injury," plaintiff was found to lack

[2] See, Serwin, POISED ON THE PRECIPICE: A CRITICAL EXAMINATION OF PRIVACY LITIGATION, 25 Santa Clara Computer & High Tech. L.J. 883 (2009); Serwin, Information Security and Privacy: A Guide to Federal and State Law and Compliance, Chapter 34) (2nd. ed. West 2010).

> standing. (citing *Luis v. Dennis,* 752 F.2d 604, 608 (3d Cir.1984) ("the alleged injury is not of sufficient immediacy and reality to permit adjudication by a federal court")).[3]

The *Hammond*, court also examined whether, even assuming standing could be found to exist, whether a claim for proximately caused damages could be sustained.

> Even assuming, *arguendo,* that Plaintiffs could be said to have standing, Defendant's motion for summary judgment dismissing Plaintiffs' claims would be granted because Plaintiffs' alleged increased risk of identity theft is insufficient to support Plaintiffs' substantive claims. ("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. Plaintiff has not presented any case law or statute, from any jurisdiction, indicating otherwise. Plaintiff's alleged injuries are solely the result of a perceived and speculative risk of future injury that may never occur. Plaintiff has failed to show an actual resulting injury that might support a claim for damages. As damages are an essential element of each of plaintiff's claims, plaintiff's claims fail as a matter of law.").[4]

## V. CONCLUSION

The litigation process does not attempt, with very limited exceptions, to redress harms that have not yet occurred. As a result, as noted above, courts typically require plaintiffs to prove three distinct, but related elements to successfully bring a claim—standing, causation, and harm. Causation requires the person suing the company to show that the harm would not have occurred if it weren't for the actions of the company. Harm typically requires some form of economic damages, such as monetary loss (illegitimate charges on a credit card that are not reimbursed would fit in this category).

These requirements present often insurmountable hurdles for plaintiffs in data breach cases. Courts do not look favorably on claims based upon the possibility for future harm, and have been almost uniformly dismissing plaintiffs' attempts to recover in these cases. This study does not support a conclusion that companies should not have reasonable security practices, or that there are not risks that result from a lack of data security, and it should not be read to support a conclusion that data security isn't a core concern for all companies. It also does not focus on the cost to companies for data breaches, but instead focuses on whether plaintiffs in data breach cases suffer actual harm sufficient to state a claim for damages, and whether courts have accurately examined this issue. Based upon the results, it is clear that they have, because this study demonstrates that most individuals cannot prove any economic harm resulting from a data breach.

---

[3] *See*, *Hammond v. The Bank of New York Mellon Corp.*, 2010 WL 2643307 (June 25, 2010, S.D.N.Y.)(some internal citations omitted).

[4] *Id.* (internal citations omitted).