Washington Journal of Law, Technology & Arts

Volume 4 | Issue 4 Article 5

5-23-2008

No Harm, No Foul: Limits on Damages Awards for Individuals Subject to a Data Breach

Derek A. Bishop

Litigation
Cite as: Derek A. Bishop, *No Harm No Foul:Limits on Damages Awards for Individuals Subject to a Data Breach*, [4] Shidler J. L. Com. & Tech. [12] (5/23/2008), *at* <http://www.lctjournal.washington.edu/Vol4/a12Bishop.html>

NO HARM NO FOUL:
LIMITS ON DAMAGES AWARDS FOR INDIVIDUALS SUBJECT TO A DATA BREACH

Derek A. Bishop[1]

Abstract

Recently, TJX, Inc. announced that computer hackers breached several of TJX's databases containing the driver's license and credit card numbers of over 47 million customers. Within a month, a class action lawsuit attempting to hold TJX responsible for losing control of this information was filed. In the past, class action lawsuits based on the release of consumer's personal data have failed because the plaintiffs have not alleged sufficient harms. This article examines legal claims relating to the release of personal data by companies during security breaches. To date, courts have refused to find individuals harmed by the negligent release of information, without proof that the information has been misused by a third party. In addition, courts have not found a substantial enough causal link between the release and the fraudulent use. This article also examines several doctrines which may in the future be used to limit potential defendant liability from class action claims stemming from the release of personal information.

Table of Contents

INTRODUCTION

<1>In January 2007, the parent company of T.J.Maxx and Marshall's department stores, TJX, Inc., revealed that hackers had accessed areas of their computer system containing retail transaction data dating from 2003.[2] TJX indicated that there were several breaches of their system between July 2005 and January 2007.[3] TJX has not specified which databases were breached, but it is believed that the hackers accessed information about transactions involving approximately 45.7 million credit cards.[4] Within two weeks, attorneys filed a class action lawsuit in U.S. District Court for the District of Massachusetts.[5] The plaintiffs seek monetary damages and an order requiring TJX to pay for credit monitoring.[6] In addition, several banks filed a lawsuit against TJX, attempting to recoup costs

incurred in replacing the credit cards of those affected by the breach.[7] The Federal Trade Commission and the Attorneys General of several states began a civil investigation into the breach and TJX's security procedures.[8] Most recently, TJX announced they incurred $12 million in expenses in the first quarter of fiscal year 2008, offsetting what was otherwise strong growth.[9] As computer data breaches become more common, it becomes more important to properly determine whether companies or organizations face tort liability for such breaches when customer information is released during those breaches.[10]

<2>The plaintiffs' allegations in the TJX case and other recent class action lawsuits share two important similarities. The plaintiffs allege that a business collected their personal information for the business' purposes, and then allowed a third party to improperly access that personal information. The purpose for collecting the plaintiff's information has varied, but has generally been unimportant. Likewise, the method used by the third party to gain access to the information has ranged from cases where the information was taken without an indication they were targeting the information, to cases where the information itself was targeted. Although the circumstances establishing these allegations vary greatly, these elements are at the core of each of the negligence class actions brought to date.

<3>A plaintiff bringing a negligence lawsuit must allege every element of the common law tort of negligence. These elements are the presence of a duty, the failure of the defendant to meet that duty, and damage to the plaintiff that is a cause and result of the failure to meet the duty.[11] Plaintiffs have had difficulty establishing that the defendant has a duty to protect their information, and that they have suffered some compensable damage from that release.[12] Courts have begun to define the contours of compensable damage to a plaintiff stemming from the release of their personal information.[13] To date, plaintiffs have been unable to demonstrate compensable harm from the release of information, which has led courts to dismiss the cases for lack of standing or for failure to state a claim. If a plaintiff is able to demonstrate compensable harm, any award should be limited by the doctrine of avoidable consequences.

DETERMINING WHEN A PLAINTIFF HAS BEEN HARMED

<4>Plaintiffs have been unable to collect damages from class action lawsuits stemming from negligent protection of personal data. In previous cases, plaintiffs have failed to demonstrate compensable damage due to the release of the information.[14] Some courts have found that the unauthorized release of personal information itself is not a cognizable harm, instead requiring plaintiffs to provide evidence that the information was misused. Courts have also dismissed claims by plaintiffs who have suffered harm, when the plaintiff has not provided sufficient evidence the harm was caused by the release of information. Even if the court finds the plaintiff has suffered a compensable harm, a court may disallow recovery under the economic loss rule, which disallows compensation in tort for purely economic harms.[15]

Establishing Standing and the Element of Damages

<5>A threshold issue in figuring potential tort exposure is determining what constitutes harm from the inadvertent release of personal information. This issue arises in two ways. First, courts have dismissed, or remanded, claims for lack of subject matter jurisdiction where plaintiffs have failed to allege harm sufficient to sustain standing.[16] Second, plaintiffs must demonstrate a cognizable harm as an element of a prima facie case for negligent release of their information. In either event, the court is likely to dismiss the claims for lack of jurisdiction or for failure to state a claim.[17]

<6>In cases where a negligent release of information has led to physical harm, courts have permitted a lawsuit to proceed. In *Rembsberg v. Docusearch*, a man used false pretenses to obtain a woman's personal information from a data broker.[18] The man used this information to stalk and eventually kill the woman.[19] The court held the woman suffered harm sufficient to support the lawsuit, and the claim presented sufficient evidence to show that the release of information caused that harm.[20] This unfortunate set of facts demonstrates the potential harm an individual can suffer as a result of the unauthorized release of one's personal data.

<7>In the more typical case, however, an individual's information is released, but there is no evidence that the information was misused. Courts have held the release of information alone, without evidence of misuse, does not cause damage to the plaintiff.[21] These courts have held the risk of some undefined future harm to the plaintiff is too speculative to sustain a lawsuit.[22] Courts will generally dismiss or remand these cases either based on a lack of standing,[23] or for failure to allege the damage element of the prima facie case[24] depending on the procedural posture and the context of the case. In either instance, the court uses the same analysis to determine what constitutes damage.

<8>In *Giordano v. Wachovia Securities, L.L.C.*, the U.S. District Court for the District of New Jersey considered whether a release of plaintiffs' personal information, with no evidence of misuse, was sufficient to grant plaintiffs standing.[25] The *Giordano* plaintiffs were customers of Wachovia Securities, L.L.C., a financial services company providing advisory, brokerage and asset management to customers.[26] Defendant sent a list containing financial information, including names, addresses and social security numbers of thousands of customers, via UPS.[27] UPS subsequently lost the package in transit, and defendant believed that the package was damaged in transit and destroyed.[28] The named plaintiff failed to allege that her identity was stolen or the data misused.[29] The court found the loss of data, without allegations of misuse, failed to provide the plaintiffs with standing to bring the suit.[30] The court found the loss of plaintiff's financial data and costs incurred by the plaintiff in credit monitoring did not create a concrete and particularized harm.[31]

<9>Courts have since expanded the reasoning in *Giordano* in two similar class action lawsuits.[32] In these cases the plaintiffs alleged that the defendants allowed a third party to access their information.[33] The courts held the plaintiffs lacked standing, even where the information was accessed purposefully and illegally.[34] Both of these cases, *Key v. DSW, Inc.* and *Acxiom Corp. v. Bell*, held that a plaintiff lacked standing where the plaintiff was unable to prove that the information was used fraudulently.[35] Both of these courts granted the defendant's motion to dismiss based on the plaintiff's lack of standing.[36]

<10>The Seventh Circuit has most recently considered the question in *Pisciotta v. Old National Bancorp (ONB).*[37] ONB collected personal information from individuals seeking banking services such as loans and accounts.[38] The data of tens of thousands of ONB's site users was breached and ONB subsequently notified the individuals of the breach.[39] The plaintiffs filed a class action lawsuit on behalf of the individuals whose information was released.[40] Notably, the claim failed to allege that any plaintiff suffered any direct financial loss or was the victim of identity theft.[41] The Court of Appeals held the increased risk of harm stemming from the release of the personal information was sufficient to give plaintiffs standing, even where no actual injury was shown.[42] However, the Court of Appeals upheld the dismissal because it held Indiana state law did not recognize this increased risk of injury as a compensable harm.[43] It is unclear how widely accepted this reasoning will become in future cases.

<11>The tort element of damage is a closely related, but distinct, concept from standing. Most significantly, standing

is a jurisdictional requirement to maintaining a suit in federal court, whereas proving damages is an element of a negligence claim. Courts have found that plaintiffs suffer no tort damages when a security breach leads to a release of personal information, using the same rationale and authority as the courts finding a lack of standing.[45]

"Fear of Identity Theft" as Compensable Damage

<12>In an effort to establish compensable damages, several plaintiffs have alleged injury based on their need to protect themselves from identity theft. In these cases, plaintiffs have analogized the release of personal information to exposure to a pathogen in fear of illness cases. In fear of illness cases, courts allow plaintiffs to collect damages based either on the emotional distress caused by a well grounded fear of contracting an illness, or for the costs incurred by medical monitoring to prevent future illness.[46] Through this analogy, plaintiffs' claim that their "fear of identity theft" gives rise to damages either by causing emotional distress in the form of plaintiff's worry about identity theft or by causing the plaintiff to incur costs for monitoring their credit reports to prevent identity theft. Courts have rejected this analogy in each case to date.

<13>In *Stollenwerk v. Tri-West Healthcare*, the U.S. District Court for the District of Arizona considered whether the fear of identity theft as a result of the release of personal information could establish the damages element of the plaintiff's claim.[47] In that case, burglars stole a hard drive containing the plaintiff's unencrypted personal data from the defendant health insurer's office.[48] The court refused to recognize a fear of identity theft for three reasons. First, the loss of control of an individual's data does not create a latent injury at the time of exposure.[49] Secondly, the public health rationale underpinning the fear of illness cases does not apply where an individual's personal data is released.[50] Lastly, the court held that any injury resulting from identity theft could be remedied with financial damages.[51] The court also noted that it was unable to locate a single case in which costs for monitoring were awarded without a risk to human health.[52]

<14>The *Giordano* court also considered and rejected fear of identity theft damages because the plaintiffs were unable to prove that their information was actually stolen. In the basic fear of illness case, the plaintiff must provide proof of exposure to a harmful level of pathogen.[53] In *Giordano*, there was no evidence that the package of personal information was targeted or stolen, or that any third party intended to misuse the information.[54] The court found the plaintiff failed to prove that he had a greater risk of identity theft due to the data release because they provided no evidence that the information was accessed.[55]

<15>***Establishing that the Data Loss Caused the Plaintiff's Damages***

<16>Even where a plaintiff is able to show damage, the plaintiff must also provide proof that the damage was caused by the breach. A plaintiff has significant difficulty proving that the identity thief obtained the information via the breach.[56] This difficulty is due in large part to the wide use of personal data in global commerce.[57] A customer's social security number or credit card details, for example, are stored with many organizations. A plaintiff is required to provide evidence that the identity thief obtained the information via a specific breach, or else risk dismissal of claims.[58]

<17>One of the plaintiffs in *Stollenwerk* was a victim of identity theft.[59] Plaintiff provided evidence that a third party attempted to open credit accounts in his name on six separate occasions, all after the relevant data breach.[60] The court held no reasonable jury could find the data breach caused the plaintiff's identity theft absent evidence connecting the information used fraudulently with the lost information.[61] The court specifically rejected, as *post hoc*

ergo propter hoc, the argument that the temporal relationship of the events proved causation.[62]

The Economic Loss Rule

<18>Under the traditional economic loss rule, tort law does not allow parties to recover damages for economic losses which are unaccompanied by some physical harm.[63] The "economic loss rule" limits compensation in tort for economic damages because economic losses are speculative and unforeseeably wide ranging.[64] In addition, economic losses are generally thought to be best allocated via contract.[65] In a typical identity theft situation, identity thieves use others' personal data without authorization to commit fraudulent acts.[66] This fraud often takes the form of fraudulent credit transactions and not physical harm to person or property.[67] A court strictly applying the economic loss rule would substantially reduce potential liability for companies releasing private information.

<19>Courts and legislatures may create an exception to the economic loss rule in cases of harm to consumers arising from security breaches.[68] In the past, courts have created exceptions to the economic loss rule where the policies underlying the economic loss rule were not met.[69] Some commentators believe that the underlying policies would not be advanced by the imposition of the economic loss rule in this case, and so courts may develop another exception.[70]

THE EFFECT OF THE DOCTRINE OF AVOIDABLE CONSEQUENCES ON THE FINAL DAMAGES AWARD

<20>If a plaintiff establishes damage from the negligent release of his personal information, the defendant can attempt to limit its liability for those damages. Under the doctrine of avoidable consequences, "any damages which could have been avoided by reasonable conduct on the part of the plaintiff" are not compensable in tort.[71] The doctrine of avoidable consequences is widely accepted in a variety of factual contexts.[72] In this context, the defendant might effectively use this doctrine to limit its liability under two separate theories. A defendant could pay the plaintiff's credit monitoring costs, for example. A state's credit freeze law might also serve to limit a plaintiff's damages.

Payment of Credit Monitoring Costs

<21>If a company offers credit monitoring services to those whose information was released, it limits its liability to damages incurred at the time of the offer. Credit monitoring services provide individuals with a copy of their credit report periodically. This credit report will detail all of the accounts opened in the individual's name. Individuals can immediately identify and close any accounts opened fraudulently, thereby limiting the damages suffered by the individual. Defendant's liability would be limited to fraud taking place before the implementation of, or in spite of, the credit monitoring program.

Credit Freeze Laws

<22>Credit freeze laws may also limit the amount of damages awarded to plaintiffs. To date, thirty nine states (and the District of Columbia) have enacted credit freeze laws, and the major credit agencies now offer a voluntary credit freeze upon request.[73] Using a credit freeze, a consumer can prevent credit agencies from sharing one's credit file with anyone, unless the consumer removes the freeze or otherwise specifically authorizes access.[74] A credit freeze

of this sort generally requires an individual to pay a small fee and make several phone calls.[75] This process effectively prevents the use of an individual's information to obtain credit, either legitimately or fraudulently.[76] If an individual can be reasonably expected to use a credit freeze to protect himself from the possibility of identity theft, then a court might limit the defendant's potential liability.

CONCLUSION

<23>Companies that collect large amounts of personal data face litigation if they lose control of that data. To date no court has found a plaintiff damaged by the mere release of the plaintiff's information. Courts have not found plaintiffs damaged when their information was accessed illegally. Instead, courts have required that the information be used fraudulently. If a plaintiff can provide evidence that the plaintiff suffered an actual loss, they must still prove that this loss was caused by the breach. Lastly, plaintiffs must convince a court that the economic loss rule should not apply in the case of identity theft. If a court finds a plaintiff has suffered compensable damage, defendants can act to limit their potential liability. Defendants can offer credit monitoring services, or may rely on a state credit freeze law. In either event, if a court finds some portion of the damages could have been avoided through reasonable efforts, then this portion of the damages would not be attributable to the defendant.

[<< Top]

Footnotes

1. Derek A. Bishop, University of Washington School of Law, Class of 2007. Thank you to Professor Anita Ramasastry, University of Washington School of Law, and Jennifer Campbell. Special thanks to Mark Melodia, Partner with the law firm of Reed Smith, LLP.

2. Larry Greenemeier, *Credit Card Data, A Hack And A Rush To Contain The Damage*, Information Week, Jan. 22, 2007, *available at:* http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml;jsessionid=BEUGUPJQ0VCMYQSNDLPSKHSCJUNN2JVN?articleID=196902211&_requestid=243506.

3. Larry Greenemeier, *T.J. Maxx Probe Reveals Data Breach Worse Than Originally Thought*, Information Week, Feb. 21, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=197007754.

4. TJX, Inc., Annual Report (Form 10-K) (March 29, 2007) *available at* http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm. More than three dozen banks in Massachusetts alone have reported that customers' credit cards were compromised. *See* Gregg Keizer, *Mass. AG Leads Multistate Probe Into TJX Breach*, Computerworld, Feb. 08, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010884&source=NLT_PM&nlid=8.

5. Jenn Abelson, *TJX Faces Class Action Lawsuit In Data Breach*, Boston Globe, Jan. 30, 2007, at C1, *available at* http://www.boston.com/business/globe/articles/2007/01/30/tjx_faces_class_action_lawsuit_in_data_breach .

6. *Id*.

7. Ross Kerber, *Banks in Region Set to Sue TJX Over Breach*, Boston Globe, Apr. 25, 2007, at C1, *available at*

http://www.boston.com/business/globe/articles/2007/04/25/banks_in_region_set_to_sue_tjx_over_breach . TJX settled with the banks in December 2007. *TJX settles with banks over data breach*, SECURITYFOCUS, Dec. 19, 2007, http://www.securityfocus.com/brief/647.

8. Gregg Keizer, *Mass. AG Leads Multistate Probe Into TJX Breach*, COMPUTERWORLD, Feb. 08, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010884&source=NLT_PM&nlid=8; Jenn Abelson, *TJX faces FTC Scrutiny in Data Breach*, BOSTON GLOBE, March 13, 2007, *available at http://www.boston.com/business/globe/articles/2007/03/13/tjx_faces_scrutiny_by_ftc?mode=PF*. TJX settled with the FTC on March 28, 2008. Grant Gross, *FTC settles with TJX, LexisNexis*, COMPUTERWORLD, Mar. 28, 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9072919&intsrc=hm_list

9. Ross Kerber, *TJX Puts Cost for Breach at $25M So Far*, BOSTON GLOBE, May 16, 2007, at D1, *available at* http://www.boston.com/business/personalfinance/articles/2007/05/16/tjx_puts_cost_for_breach_at_25m_so_far/ .

10. In addition to common law negligence theories, many plaintiffs bring claims based on violations of statutes. The Fair Credit Reporting Act (FCRA) is one example. *See* First Amended Class Action Complaint at 15, Harrington v. Choicepoint, Inc., No. CV05 1294 SJO JWJx (C.D. Cal. filed Feb. 22, 2005).

11. *See* RESTATEMENT (SECOND) OF TORTS § 328A (1965).

12. Courts have not yet found that defendants have a duty to protect personal information. Courts are beginning to find that individuals illegally obtaining and misusing personal information is foreseeable. The foreseeability of the risk is a primary consideration for courts considering whether to impose a duty to protect against that risk. For a fuller discussion of possible duties on collectors of data see Derek A. Bishop, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 SHIDLER J. L. COM. & TECH. 7 (Dec. 4, 2006), *available* at <http://www.lctjournal.washington.edu/Vol3/a007Bishop.html>.

13. In addition to defending negligence suits from individuals, TJX may have a problem with its shareholders. A major shareholder of TJX, Inc. filed a lawsuit in the Chancery Court of Delaware in an effort to obtain records showing how the company responded to the computer breach. *See Business in Brief*, BOSTON GLOBE, Mar. 21, 2007, at D2, *available at http://www.boston.com/business/globe/articles/2007/03/21/times_co_ne_units_ad_revenue_falls_in_february/* .

14. In the TJX breach, there is proof that the information, of at least some individuals, was used fraudulently. Police in Florida arrested 10 people because they had illegally obtained $8,000,000 in gift cards and other goods using information stolen from the TJX computer system. *See* Ross Kerber, *Scam May Be Tied to Stolen TJX Data*, THE BOSTON GLOBE, Mar. 24. 2007, at A1, *available at http://www.boston.com/business/globe/articles/2007/03/24/scam_may_be_tied_to_stolen_tjx_data/*.

15. 86 C.J.S. *Torts* § 26 (2008).

16. Standing is a jurisdictional requirement found in the "Cases and Controversy" clause of Article III of the United States Constitution. Generally speaking it requires that a plaintiff demonstrate "an invasion of a legally protected interest" prior to the court adjudicating the matter. Although this is a federal constitutional requirement, most jurisdictions have similar rules. *See* Lujan v. Defenders of Wildlife, 504

U.S. 555, 560 (1992).

17. The court would dismiss, or remand, the claims under FRCP 12(b)(1), for lack of jurisdiction, or FRCP 12(b)(6), for a failure to state a claim upon which relief could be granted.

18. Remsburg v. Docusearch, Inc., 149 N.H. 148, 152, 816 A.2d 1001 (2003).

19. *Id*.

20. *Id*.

21. *See* Key v. DSW, Inc., 454 F. Supp.2d 684 (S.D. Ohio 2006); Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz Sept. 6, 2005) *aff'd in part, rev'd in part*, 254 Fed. Appx. 664 (9th Cir. 2007); Guin v. Brazos Higher Education Service Corp. Inc. 2006 WL 288483 (D. Minn. Feb. 7, 2006); Forbes v. Wells Fargo, 420 F. Supp.2d 1018 (D. Minn. 2006); Giordano v. Wachovia Securities, L.L.C., 2006 WL 2177036 (D.N.J. July 31, 2006); Bell v. Acxiom Corp., 2006 WL 2850042 (E.D. Ark Oct. 3, 2006); Walters v. DHL Express, 2006 WL 1314132 (C.D. Ill. May 12, 2006); Randolph v. ING Life Insurance and Annuity Co., 486 F. Supp.2d. 1, (D. D.C. Feb. 20, 2007).

22. *See Key*, 454 F. Supp.2d 684 ; *Stollenwerk*, 2005 WL 2465906; *Guin*, 2006 WL 288483; *Forbes*, 420 F. Supp.2d 1018; *Giordano*, 2006 WL 2177036; *Bell*, 2006 WL 2850042; *Walters*, 2006 WL 1314132.

23. *See Key*, 454 F. Supp.2d 684; *Giordano*, 2006 WL 2177036; *Bell*, 2006 WL 2850042; *Randolph*, 486 F. Supp. 2d 1.

24. *See Stollenwerk*, 2005 WL 2465906; *Guin* , 2006 WL 288483; *Forbes*, 420 F. Supp.2d 1018.

25. Giordano v. Wachovia Securities, L.L.C., 2006 WL 2177036 (D.N.J. July 31, 2006).

26. *Id* at *1.

27. *Id*.

28. *Id*.

29. *Id.* at *3.

30. *Id.* at *5.

31. *Id*.

32. Key v. DSW, Inc., 454 F. Supp.2d 684 (S.D. Ohio 2006); Bell v. Acxiom, 2006 WL 2850042 (E.D. Ark Oct. 3, 2006).

33. In *Key*, 454 F. Supp.2d 684, the defendant, DSW, had collected financial information on approximately 1.5 Million customers at DSW retail stores. In March of 2005, plaintiffs alleged that an unknown individual accessed the database containing that personal information, and acquired the personal information. Plaintiffs alleged that due to this improper release they suffered an increased risk of identity theft. In *Bell*, 2006 WL 2850042, the defendant, Acxiom, was a data bank that collected personal information for other companies to develop "a clear picture of the people buying its products and services." *Bell* at *1. Data thieves had accessed this information and downloaded several of Acxiom's databases of personal information. The data thieves were convicted of this theft and of selling the data to a direct mail marketer. The plaintiffs alleged a higher risk of receiving junk mail and of being a victim of identity theft.

34. *Key*, 454 F. Supp.2d 684, 688-89 (finding no standing where an unauthorized person obtained access to Defendant's database and acquired the personal information of 96,000 individuals); *Bell*, 2006 WL 2850042, at *2 (finding no standing where an unauthorized person exploited a hole in Defendant's security system and downloaded databases containing personal information).

35. *Key*, 454 F. Supp.2d at 689 (in addition, the court noted that the plaintiffs failed to allege that their information was specifically accessed, although the database containing the information was accessed illegally); *Bell*, 2006 WL 2850042 at *2.

36. *Key*, 454 F. Supp.2d at 691; *Bell*, 2006 WL 2850042 at *3.

37. Pisciotta v. Old Nat'l. Bancorp, 499 F.3d 629 (7th Cir. 2007).

38. *Id.* at 631.

39. *Id.* at 632.

40. *Id*.

41. *Id*.

42. *Id.* at 634.

43. *Id.* at 640.

44. Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992).

45. *See* Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz 2005) *aff'd in part, rev'd in part*, 254 Fed. Appx. 664 (9th Cir. 2007); Guin v. Brazos Higher Education Service Corp. Inc., 2006 WL 288483 (D. Minn. 2006); Forbes v. Wells Fargo, 420 F. Supp.2d 1018 (D. Minn. 2006).

46. The "fear of illness" line of cases allows a plaintiff to recover in tort where the plaintiff was exposed to a dangerous pathogen. The "fear of illness" damages are most generally found in cases involving known carcinogens, such as asbestos or high doses of radiation. However, they are also found where exposure to other deadly pathogens, such as HIV, is found. For a fuller discussion of "fear of illness" see Robert Michael Ey, *Cause of Action to Recover Damages for Fear of Future Contraction of Disease*, 8 Causes of Action (Second) 157 (2007).

47. Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005), *aff'd in part, rev'd in part*, 254 Fed. Appx. 664 (2007).

48. *Stollenwerk*, 2005 WL 2465906, at *5.

49. *Id.* at *3.

50. *Id*.

51. *Id*.

52. *Id.* at *4.

53. The standard varies by jurisdiction from "actual exposure", to "adequate possibility of exposure to give rise to reasonable fear of illness." *See* Robert Michael Ey, *Cause of Action to Recover Damages for Fear of Future Contraction of Disease*, 8 Causes of Action (Second) 157, § 12 (2007).

54. Giordano v. Wachovia Securities, L.L.C., 2006 WL 2177036, at *5 (D.N.J. July 31, 2006); *See also* Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906, at *5 (D. Ariz. Sept. 6, 2005).

55. *Giordano*, 2006 WL 2177036, at *3.

56. Jason Krause, *ID Theft is Real, But Winning Damages is Elusive*, ABA JOURNAL EREPORT, Nov. 3, 2006, http://www.abanet.org/journal/ereport/n3id.html.

57. *Id.*

58. Some commentators have suggested that a statistical analysis may be sufficient absent direct evidence on how the identity thief obtained the personal information at issue. *See, e.g.* ,John Kennedy and Parishi Sanjanwala, *Outside Counsel: Civil Suits Arising From Information Security Breaches*, NEW YORK LAW JOURNAL, Feb. 2, 2007, *available at* http://www.deweyleboeuf.com/files/News/2ce5b88c-7b7b-49b2-a216-d0d0d51cfb4b/Presentation/NewsAttachment/52eea70d-c03e-4b9e-8372-507e908233c8/5227.pdf.

59. The court first determined identity theft was a compensable harm before considering whether the identity theft was caused by the data loss. Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906, at *5 (D. Ariz. Sept. 6, 2005).

60. *Stollenwerk*, 2005 WL 2465906, at *6.

61. *Id.*.

62. *Id.* at *7.

63. *See* Robins Dry-Dock & Repair v. Flint, 275 U.S. 303 (1927) (holding that a defendant is not liable to contracting parties for purely economic reasons); State of Louisiana ex rel. Guste v. M/V Testbank, 752 F.2d 1019 (5th Cir. 1985) (holding that a boat that spilled PCP in the Mississippi River is not liable to the fishermen that were unable to use the water for fishing, unless their boat suffered some physical manifestation of damage).

64. *See* East River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 870 (1986); Moorman Mfg. Co. v. Nat'l Tank Co., 91 Ill.2d 69, 81, 435 N.E.2d 443 (1982); Saratoga Fishing Co. v. J.M. Martinac & Co., 520 U.S. 875, 885 (1997) ("the "economic loss" doctrine, already do[es], and w[ill] continue to, limit liability in important ways."); People Exp. Airlines, Inc v. Consolidated Rail Corp., 100 N.J. 246, 495 A.2d 107 (1985).

65. *See East River S.S. Corp*, 476 U.S. 858; *Moorman Mfg. Co.*, 435 N.E.2d 443; *Saratoga Fishing Co.*, 520 U.S. at 885 ("the "economic loss" doctrine, already do[es], and w[ill] continue to, limit liability in important ways."); *People Exp. Airlines, Inc*, 495 A.2d 107.

66. Press Release, Fed. Trade Comm'n, FTC Issues Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity (October 29, 2004), *available at* http://www.ftc.gov/opa/2004/10/facataidtheft.htm.

67. Although rare, negligent handling of personal data can result in harm to the individual. In one notable case, a commercial data broker sold a woman's personal information to an unauthorized man. This man then used the information obtained to find and kill the woman. Remberg v. Docusearch, Inc., 149 N.H. 148, 816 A.2d 1001 (2003).

68. For example, the Illinois legislature has created an exception to this rule specifically covering identity theft. 815 ILL. COMP. STAT. ANN. 505/10a(a) (West 2007). *But see* Banknorth NA v. BJ's Wholesale Club,

Inc., 442 F. Supp.2d 206, 212 (M.D. Pa. 2006) (holding that the economic loss rule bars the award of damages to plaintiff bank for the replacement of debit cards where the defendant released the financial information).

69. For example, the economic loss rule applies only to situations of negligence. *See* People v. Ware, 2003 WL 22120898, at *2 (Cal. Ct. App. 2003). *See also* People Exp. Airlines, Inc v. Consolidated Rail Corp., 100 N.J. 246, 264, 495 A.2d 107 (1985) (holding in part that a defendant may be found liable for economic damages where the plaintiffs comprise an identifiable class that the defendant knows are likely to suffer economic damage from its conduct). *But see* City of Chicago v. Beretta U.S.A. Corp., 213 Ill. 2d 351, 421-22, 821 N.E.2d 1099 (2004) (refusing to adopt the *People Express* standard, instead relying on traditional notions of the economic loss rule).

70. First, individuals in most cases lack the ability to truly negotiate and allocate the risk. This is true especially with regard to a consumer transaction such as those at issue in the TJX breach. It is impracticable for an individual to contract with all those that obtain his information, and due to the relative bargaining power any contracts would be unlikely to reallocate the risk. *See* 151 Cong. Rec. S7620-7622 (2005) (comments by Sen. Specter); Beth Givens, *The Information Marketplace: Merging and Exchanging Consumer Data*, Privacy Rights Clearinghouse, Apr. 30, 2001, http://www.ftc.gov/bcp/workshops/infomktplace/comments/givens.htm. (discussing the pervasive use of personal data throughout each individual's life); Vincent R. Johnson, *Liberating Progress and the Free Market from the Specter of Tort Liability*, 83 Nw. U. L. Rev. 1026, 1044 (1989). Second, the potential class of individuals affected by a breach is readily ascertained and controlled by the defendant; the class is comprised solely of individuals whose information the company stores. *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255, 296-99 (2005). Lastly, individual losses from identity theft are generally fixed to the time and money spent in repairing their credit. Although these costs may be difficult for a court to determine, the losses or harm are not entirely speculative. *See* Anita Ramasastry, *Data Insecurity: What Remedy Should Consumers Have When Companies Do Not Keep Their Data Safe?*, FindLaw's Writ, March 06, 2006, http://writ.news.findlaw.com/ramasastry/20060306.html.

71. W. Page Keeton et al., Prosser and Keeton on The Law of Torts 458 (5th ed. 1984).

72. The doctrine has been used in a variety of circumstances. From reducing damage awards based on a plaintiff's refusal to lose weight, (*See* Danny Veilleux, Annotation, *Failure to lose weight as basis for reduction of damages in personal injury action*, 24 A.L.R. 5th 174 (2006)) to avoiding damage awards in wrongful conception cases (*See* Norman M. Block, Note, *Wrongful Birth: The Avoidance of Consequences Doctrine in Mitigation of Damages*, 53 Fordham L. Rev. 1107 (1985)). For general information on the doctrine of avoidable consequences, *see* 25 C.J.S. *Damages* §§ 46-52 (2008); 22 Am. Jur. 2d *Damages* §§ 340-82 (2008).

73. Credit freeze laws are of relatively recent vintage. At the start of 2005, only 4 states had enacted a security freeze law of any kind. By 2007, 27 states had adopted a credit freeze law, and 17 more states were considering credit freeze laws. *See State PIRG Summary of State Security Freeze and Security Breach Notification Laws*, State Public Interest Research Groups, July 18, 2006, http://www.pirg.org/consumer/credit/statelaws.htm; *State Security Freeze Laws*, Consumers Union, October 30, 2007, http://www.consumersunion.org/campaigns/learn_more/003484indiv.html; *Freeze Identity Thieves Out of Consumers' Credit Files: State ID Theft Protection Bills That Give Consumers the Option to Place Security Freezes on their Credit Files, 2007 Session*, Consumers Union, http://www.consumersunion.org/campaigns/financialprivacynow/2006/10/current_state_security_freeze_1.html

(last visited Marcb 29, 2008).

74. Anita Ramasastry, *We Should Warm Up to Credit Freeze*, Seattle Post-Intelligencer, February 15, 2006 at B7, *available at* http://seattlepi.nwsource.com/opinion/259463_creditfreeze.html.

75. *See* California Law SB 168 (Debra Bowen) Identity Theft Prevention, Fight Identity Theft, http://www.fightidentitytheft.com/legislation_california_sb168.html (last visited March 29, 2008).

76. Statement of the Electronic Privacy Information Center to Maryland Attorney General Identity Theft Forum, Chris Jay Hoofnagle, Senior Counsel, Electronic Privacy Information Center West Coast Office (November 21, 2005), *available at* http://www.epic.org/privacy/idtheft/mdstate11.21.05.html.