University of Florida Journal of Law & Public Policy

Volume 19 | Issue 1 Article 6

2008

Strength in Numbers: An Examination Into the Liability of Corporate Entities for Consumer and Employee Data Breaches

Joshua R. Levenson

NOTES

STRENGTH IN NUMBERS: AN EXAMINATION INTO THE LIABILITY OF CORPORATE ENTITIES FOR CONSUMER AND EMPLOYEE DATA BREACHES*

*Joshua R. Levenson***

---

* Editor's Note: This Note received the *Barbara W. Makar Writing Award* for Outstanding Note in Fall 2007.

** J.D. expected May 2008, University of Florida Fredric G. Levin College of Law. I dedicate this Note to my parents: Wendy Levenson and Richard Levenson. Their love, wisdom, and guidance allow me to dream no small dreams. Also, a special thanks to Professor Andrea Matwyshyn for her friendship and guidance in selecting this topic.

I. INTRODUCTION

Everyday, millions of people go to work to support themselves, their families, and their friends. In order to work, people must turn over multiple pieces of personally identifiable information to a corporation. A corporation may use this information for data processing, accountability, or even monitoring. No matter how a corporation uses the personally identifiable information, however, such information is susceptible to being stolen and maliciously used for identity theft purposes. Who do we blame? The identity thief? The corporation? Both?

Because it is difficult to find an identity thief, the person in the best position to prevent a breach is the corporation, which is deemed a legal person. Although corporations are currently regulated by data breach notification statutes, there is no private cause of action against a corporation for losing a person's aggregated information. Thus, there is little incentive for a corporation to reallocate its resources to combat information security breaches.

This Note outlines, within Part II, the current state of damages within contract law and specifically details what is necessary to prove special damages for the loss of an income-producing asset. Part II then surveys current case law where plaintiffs have pursued a breach of contract claim against a corporation for losing their personally identifiable information. Most cases never survive summary judgment.

Part III reviews important themes within economics to highlight the overall benefits that will result if corporations begin to account for the negative production externality of consumer identity theft. After reviewing economic theory, Part III then discusses control-share premiums to emphasize which current legal doctrines recognize latent value in the aggregation of intangibles, such as names, social security numbers, and addresses. This concept of latent value in aggregation is used within this

Note's proposal for determining damages for an information security breach.

Part IV departs from analyzing legal doctrines and examines the reality of identity theft to stress the urgency of this Note's proposal. After reviewing the seminal article *The Right to Privacy*, Part IV then reveals startling statistics of current information security breaches, followed by statistics of identity theft prepared by the Federal Trade Commission. Part IV concludes by presenting possible sources of an information security breach on the corporate level.

Part V unites all the previous sections. Because courts have refused to recognize damages in the information security breach context, this Note proposes to take the concept of control-share premiums from the law of corporations and apply it to the aggregation of personally identifiable information to recognize the latent value in aggregation. Part V then proposes a method of calculating the value of an income-producing asset. The Federal Trade Commission would monitor this valuation method, which pegs corporate liability for data breaches based on a combination of the amount of information aggregated and the length of time the information is held.

After finding an identifiable source of measuring the market value of lost data at the time of breach by fusing contracts law with the law of corporations, Part V then proposes several ways of establishing causation for the information security breach. Mainly, causation may be provided by either allowing class action lawsuits or by shifting the burden of proof to the corporation that lost the aggregated personally identifiable information.

Finally, Part VI concludes this Note with an alternate path of addressing the problem of information security breaches outside legal concepts. Part VI reveals the growing market for identity theft insurance.

For all the reasons explained in this Note, it is possible to find a legal cause of action for a breach of contract against a corporation that aggregates personally identifiable information. Such a cause of action requires a fusion of contracts law with the law of corporations. Because corporations law can be viewed as a series of contracts,[1] this fusion is not combining two wholly unrelated areas of law. Moreover, once a private cause of action exists for data breaches, economic theory suggests that corporations will begin to reallocate their resources that will result in an overall market equilibrium for all market players: the corporations and the employees.

1. Henry N. Butler, *The Contractual Theory of the Corporation*, 11 GEO. MASON L. REV. 99, 100 (1989).

Because identity theft is one of the fastest rising crimes, it is time to hold more than just an identity thief accountable. This Note walks through all the necessary areas of the law to recognize a new era of accountability. Simply stated, when corporations begin to aggregate information, they will realize the strength in numbers.

II. THE CURRENT STATE OF CONTRACT LAW

A contract is "a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty."[2] In order to prevail on a breach of contract claim, a plaintiff must generally prove (1) the existence of a valid contract, (2) performance or tendered performance by the plaintiff, (3) breach of the contract by the defendant, and (4) damages sustained by the plaintiff as a result of the breach.[3]

Contract law is state oriented. When a contract claim enters federal court under 28 U.S.C. § 1332 diversity jurisdiction,[4] the federal court will apply the law of the applicable state in evaluating damages for a breach of contract.[5] "Every contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement."[6] The Uniform Commercial Code defines "good faith" as, "honesty in fact and the observance of reasonable commercial standards of fair dealing."[7]

Section A of Part II explains the different forms of damages within contract law. Section B of Part II then compares the current forms of contract damages to actual cases involving identity theft as a result of information security breaches. This comparison highlights how current contract doctrine cannot independently address problems of information security breaches.

A. *Damages in Contract Law*

As a threshold matter, there are two distinct categories of remedies available for a breach of contract: general damages and special damages.

2. RESTATEMENT (SECOND) OF CONTRACTS § 1 (1981); *see also* 1 SAMUEL WILLISTON & RICHARD A. LORD, A TREATISE ON THE LAW OF CONTRACTS § 1:1 (4th ed. 2007).

3. Werline v. E. Tex. Salt Water Disposal Co., 209 S.W.3d 888, 898 (Tex. App. 2006).

4. The rationale behind federal diversity jurisdiction is not to displace substantive state law; rather, to apply the proper law in a neutral federal forum.

5. U.S. Valves, Inc. v. Dray, 212 F.3d 1368, 1373 (Fed. Cir. 2000) (citing Gjerlov v. Schuyler Labs., Inc., 131 F.3d 1016, 1017 (Fed. Cir. 1997)).

6. RESTATEMENT (SECOND) OF CONTRACTS § 205 (1981).

7. U.C.C. § 1-201(20) (2007).

General damages[8] flow naturally from a breach of contract.[9] Special damages[10] compensate a plaintiff for additional losses that are incurred as a result of a defendant's breach but do not include the value of the promised performance.[11] The classic example of a special damage is lost profits because lost profits do not necessarily result from a breach of a contract but may be recoverable if the lost profits were both proximately caused by the alleged breach and reasonably foreseeable at the time the parties entered into the contract.[12] Whether or not damages exist is a question of fact for a jury.[13]

If damages are difficult to establish, the amount of damages does not need to be established with absolute certainty; rather, reasonable certainty will suffice.[14] To reach reasonable certainty, a plaintiff must provide a basis upon which damages may be estimated.[15] For instance, permissible methods of estimating lost profits in connection with a breach of contract claim include either providing evidence of past performance of an established business or demonstrating profits earned by others.[16] However, a plaintiff cannot act under the guise of "reasonable certainty" when calculating damages with a formula that is speculative, vague, or contingent upon some unknown factor.[17]

---

8. General damages have been given various names depending upon the jurisdiction hearing the matter. *Compare* 24 SAMUEL WILLISTON & RICHARD A. LORD, A TREATISE ON THE LAW OF CONTRACTS § 64:12 (4th ed. 2002) (stating general damages are sometimes called "loss of bargain" damages, because "they reflect a failure on the part of a defendant to live up to the bargain it made"), *with* Schonfeld v. Hilliard, 218 F.3d 164, 175-76 (2d Cir. 2000) (stating general damages are sometimes called "market" damages because "such damages are measured by the difference between the contract price and the market value of the goods at the time of breach").

9. WILLISTON & LORD, *supra* note 8, § 64:12. Stated differently, general damages would also include damages that follow any breach of similar character in the usual course of events. *Id.*

10. Special damages are also known as "consequential damages." *Schonfeld*, 218 F.3d at 176.

11. *Id.*

12. *Id.*; *see also* WILLISTON & LORD, *supra* note 8, § 64:12.

13. 23 SAMUEL WILLISTON & RICHARD A. LORD, A TREATISE ON THE LAW OF CONTRACTS § 63:5 (4th ed. 2002).

14. U.S. Valves, Inc. v. Dray, 212 F.3d 1368, 1374 (Fed. Cir. 2000).

15. Mercer Mgmt. Consulting, Inc. v. Wilde, 920 F. Supp. 219, 238 (D.D.C. 1996) (citing Garcia v. Llerena, 599 A.2d 1138, 1142 (D.C. Cir. 1991)); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 352 (1981) (stating "[d]amages are not recoverable for loss beyond an amount that the evidence permits to be established with reasonable certainty").

16. *Wilde*, 920 F. Supp. at 238. However, "evidence of lost profits from a new business venture receives greater scrutiny because there is no track record upon which to base an estimate." *Schonfeld*, 218 F.3d at 172.

17. ATACS Corp. v. Trans World Commc'ns, Inc., 155 F.3d 659, 669 (3d Cir. 1998).

Turning specifically towards special damages, *Schonfeld v. Hilliard*[18] articulated a distinction between "lost profits" and "lost assets." Reese Schonfeld,[19] a shareholder of a closely held cable corporation, brought both a derivative action and personal claims against another principal shareholder arguing, amongst other things, that the other shareholder breached their oral agreement.[20] Schonfeld sought damages under lost profits, lost asset damages, and punitive damages because the alleged breach of the oral contract resulted in the corporation losing its exclusive license to air BBC international news within the United States.[21] The district court granted defendant's motion for summary judgment on all claims.[22]

Although the claims for both lost profits and punitive damages were not revived on appeal, the appellate court reversed summary judgment on the special damages claim for lost assets.[23] Specifically, the appellate court stated that the defendant's alleged breach of contract may also cause a plaintiff to lose "an *income-producing* asset" that was in its possession prior to the breach.[24] While lost profits and lost income-producing assets are both types of special damages, they are separate and distinct categories of special damages with specific rules relating to proof.[25] A ruling on either lost profits or the loss of an income-producing asset will not affect the validity of the other claim.[26] What is common to all claims for special damages, lost profits or lost assets, is that a plaintiff must prove that liability for the loss of the asset was within the contemplation of the parties at the time the contract was made and that the asset's value was proven with reasonable certainty.[27]

The most accurate measure of damages resulting from the loss of an income-producing asset is the market value of an asset at the time of breach, rather than the lost profits that the asset could have produced in the

18. *Schonfeld*, 218 F.3d at 164.

19. Reese Schonfeld is the founder and former President of Cable News Network, better known by the initialism "CNN." *Id.* at 168.

20. *Id.* at 170.

21. *Id.* at 170-72.

22. *Id.* at 171-72.

23. *Schonfeld*, 218 F.3d at 184.

24. *Id.* at 176. The circuit court also noted that damages for the loss of an income-producing asset have also sometimes been referred to as "hybrid" damages. *Id.*

25. *Id.* What lost profits and the loss of an income-producing asset do have in common is that they are both one step removed from the promised performance of the defendant and both their existence and extent are largely driven by the individual circumstances of the plaintiff. *Id.* at 177.

26. *Id.* at 176.

27. *Id.* at 177.

future.[28] As long as the asset has a determinable market value, a plaintiff may seek to recover that value whether the asset is tangible or intangible.[29] One test announced in *Schonfeld* for determining the market value of an intangible is, "the price at which the property would change hands between a willing buyer and a willing seller, neither being under any compulsion to buy or to sell and both having reasonable knowledge of relevant facts."[30] Unlike other forms of special damages, experts may give their opinion of the asset's value if no prior sales history is available.[31] Or, if a plaintiff himself is qualified to testify on the asset's market value, he may testify.[32]

Although damages are a part of the prima facie case when pursuing a breach of contract claim, some jurisdictions find an action for breach of contract even where a plaintiff has suffered no actual damages.[33] In situations where no actual damages are proven, an injured party is entitled to at least nominal damages.[34] When pursuing a breach of contract, "damages are not recoverable for loss that the injured party could have avoided [without] undue risk, burden, or humiliation."[35] However, damages are recoverable in full if an injured party made reasonable, albeit unsuccessful, attempts to mitigate damages.[36]

---

28. *Schonfeld*, 218 F.3d at 176. The circuit court also stated that because damages from the loss of an income-producing asset are measured at a single point in time, they are inherently less speculative than lost profits. *Id.* at 177.

29. *Id.*

30. *Id.* at 178.

31. *Id.*

32. *Id.*

33. RLI Ins. Co. v. MLK Ave. Redevelopment Corp., 925 So. 2d 914, 918 (Ala. 2005) (citing Avis Rent A Car Sys., Inc. v. Heilman, 876 So. 2d 1111, 1120 (Ala. 2003)); *but see* Penny/Ohlmann/Nieman, Inc. v. Miami Valley Pension Corp., 399 F.3d 692, 704 (6th Cir. 2005) (holding a claimant seeking to recover for breach of contract must show damage as a result of the breach). In Avis Rent A Car Sys., Inc. v. Heilman, the plaintiff had standing to sue under a breach of contract claim even though the plaintiff had already been reimbursed for the damages from her employer. *Heilman*, 876 So. 2d at 1120.

34. *RLI Ins. Co.*, 925 So. 2d at 918; *see also* WILLISTON & LORD, *supra* note 8, § 64:8.

35. Ziggity Sys., Inc. v. Val Watering Sys., 769 F. Supp. 752, 836 (E.D. Pa. 1990) (citing RESTATEMENT (SECOND) OF CONTRACTS § 350(1) (1981)). In American Railway Express Co. v. Judd, the *Judd* court found that it would have been unreasonable to expect the owner of a shipment of damaged trees to plant the trees in order to see whether some of them would grow. Am. Ry. Express Co. v. Judd, 104 So. 418, 419 (1925).

36. RESTATEMENT (SECOND) OF CONTRACTS § 350(2) (1981).

B. *Information Security Breach Cases*

In a recent string of data security breach cases,[37] plaintiffs whose information was collected by a corporation and later stolen have sought legal action against the corporation under a variety of legal theories.[38] The victims tend not to seek a remedy against the actual identity thief because locating and bringing a lawsuit against the actual identity thief is more difficult. With respect to a data security breach, the two most difficult issues to resolve are causation[39] and damages.[40] The following case law analysis is limited to breach of contract claims sought against a corporation for losing aggregated personally identifiable information.

In *Jones v. Commerce Bancorp, Inc. (Commerce I)*,[41] Jones used certain personally identifiable information to open a business checking account where she was the sole authorized signor.[42] Jones learned that Bancorp authorized fraudulent withdrawals from her account and that a

37. Although the discussion of this Note targets only cases dealing with breach of contract claims and other cases discussing the difficulty of determining damages, many cases regarding information security breaches have been heard. *See generally* Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007); Garcia v. Unionbancal Corp., No. C 06-03762 CRB, 2006 U.S. Dist. LEXIS 67896 (N.D. Cal. Sept. 12, 2006); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006); Daly v. Metro. Life Ins. Co., 782 N.Y.S.2d 530 (N.Y. Sup. Ct. 2004); Huggins v. Citibank, N.A., 585 S.E.2d 275 (S.C. 2003); Am. Express Travel Related Servs., Co. v. Symbiont Software Group, Inc., 837 So. 2d 434 (Fla. 3d DCA 2002); Darcangelo v. Verizon Commc'ns, Inc., 292 F.3d. 181 (4th Cir. 2002); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007); Jones v. Commerce Bank, N.A., No. 06 Civ. 835 (HB), 2007 U.S. Dist. LEXIS 15343 (S.D.N.Y. Mar. 6, 2007); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007); Giordano v. Wachovia Sec., LLC, No. Civ. 06-476 (JBS), 2006 WL 2177036 (D.N.J. July 31, 2006); Sovereign Bank v. BJ's Wholesale Club, Inc., No. Civ. 1:CV-05-1150, 2006 WL 1722398 (M.D. Pa. July 16, 2006); Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006); Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005); Kuhn v. Capital One Fin. Corp., No. 01-5177, 2004 Mass. Super. LEXIS 514 (Mass. Super. Ct. Nov. 30, 2004); Foster v. Hillcrest Baptist Medical Center, No. Civ. No. 10-02-143-CV, 2004 WL 254713 (Tex. App. Feb. 11, 2004).

38. Most theories are either a contract claim or a tort claim.

39. Courts usually apply causation elements of tort law to determine whether the breach of the contract itself resulted in the damages the plaintiff seeks. Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906, at *5 (D. Ariz. Sept. 6, 2005).

40. *See generally Stollenwerk*, 2005 WL 2465906, at *7 (granting summary judgment for the defendant because plaintiffs were unable to prove causation or actual damages resulting from burglary of computer hard drives containing plaintiff's personal information).

41. Jones v. Commerce Bancorp, Inc., No. 06 Civ. 835 (HB), 2006 U.S. Dist. LEXIS 32067 (S.D.N.Y. May 23, 2006).

42. *Id.* at *2. This information included her social security number and date of birth. *Id.*

separate fraudulent account had been opened in Jones's name.[43] After the breach was discovered, Bancorp credited the fraudulently withdrawn funds to Jones's bank account, which was $1,860.00.[44] Jones brought a breach of contract claim against Bancorp, and Bancorp replied with a motion to dismiss claiming that because the money was credited, Jones could not prove any damages flowing from the supposed breach.[45]

The district court denied Bancorp's motion to dismiss because Jones adequately pled a breach of contract claim.[46] The district court believed that Jones might, by using the tools of discovery, show some damages stemming from her inability to access her funds during the weeks before it was credited back.[47] As the proceedings moved forward, in *Commerce II*,[48] Bancorp then moved for summary judgment on the breach of contract claim.[49] Although the district court's opinion did not expressly address the breach of contract claim in its analysis,[50] it was able to analyze the negligence claim to determine if the damages element of the breach of contract claim still held merit.[51] Regarding causation, Jones was not able to provide sufficient evidence linking Bancorp to the theft, nor was Jones able to demonstrate that she suffered any compensable injury stemming from the loss.[52] A motion to reconsider *Commerce II* was denied.[53]

In another breach of contract claim for negligent information security, plaintiff in *Forbes v. Wells Fargo Bank*[54] brought a breach of contract claim against Wells Fargo after computers were stolen from a service

---

43. *Id.* at *3.

44. *Id.*

45. *Id.* at *12.

46. *Jones*, 2006 U.S. Dist. LEXIS 32067, at *12-13. Crucial to the district court's opinion was that Jones was appearing *pro se*. *Id.*

47. *Id.* at *12-13.

48. Jones v. Commerce Bank, N.A., No. 06 Civ. 835, 2006 U.S. Dist. LEXIS 65630 (S.D.N.Y. Sept. 15, 2006) is also known as *Commerce II*.

49. *Id.* at *1.

50. The district court made a general statement regarding the prima facie case for negligence, then analyzed both the causation and damages elements of negligence before stating, "because plaintiff has produced no evidence that [Bancorp] proximately caused any compensable injury to her, [Bancorp]'s motion for summary judgment is granted." *Id.* at *9. It is reasonable to assume that the district court here, as most other courts also do, applied tort causation elements to analyze the damages components universal to both contract and tort claims.

51. *Id.* at *6-8.

52. *Id.*

53. Jones v. Commerce Bank, N.A., No. 06 Civ. 835, 2007 U.S. Dist. LEXIS 15343, at *1 (S.D.N.Y. Mar. 6, 2007).

54. 420 F. Supp. 2d 1018 (D. Minn. 2006).

provider Wells Fargo hired.[55] Information on the computers included names, addresses, social security numbers, and account numbers.[56] After Forbes was notified of the breach, she brought various claims against Wells Fargo, including a breach of contract claim.[57] Wells Fargo moved for summary judgment on all claims, citing that Forbes failed to prove any damages.[58]

To survive summary judgment, Forbes set forth two theories of damages resulting from the breach of contract.[59] First, Forbes claimed that the money she spent monitoring her credit services could be used to calculate damages.[60] Second, Forbes claimed that she was entitled to use the statutory definitions found in the Identity Theft and Assumption Deterrence Act[61] to provide a basis for damages.[62]

The district court dismissed the first theory claiming:

> [Plaintiffs] overlook the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized. . . . Plaintiffs have shown no present injury or reasonably certain future injury to support damages for any alleged increased risk of harm.[63]

The second claim also did not survive summary judgment because Forbes did not provide any legal basis as to why the district court should apply a criminal statute to a civil claim.[64]

---

55. Wells Fargo Bank subsidiaries hired Regulus Integrated Solutions to print monthly statements for home equity mortgage and student loan customers. *Forbes*, 420 F. Supp. 2d at 1019-20.

56. *Id.* at 1019.

57. *Id.* at 1020.

58. *Id.* Proving damages is essential to any contract claim. *Id.* at 1021.

59. *Id.* at 1020-21.

60. *Forbes*, 420 F. Supp. 2d at 1020-21.

61. Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028), *available at* http://www.ftc.gov/os/statutes/itada/itadact.pdf (last visited Feb. 24, 2008).

62. *Forbes*, 420 F. Supp. 2d at 1021.

63. *Id.* at 1021. This relates to the legal principle in contract law that a plaintiff cannot act under the guise of "reasonable certainty" when calculating damages when the formula employed is too speculative, vague, or contingent upon some unknown factor. *See* ATACS Corp. v. Trans World Commc'ns, Inc., 155 F.3d 659, 669 (3d Cir. 1998).

64. *Forbes*, 420 F. Supp. 2d at 1021. In dicta, the district court also reasoned that even if the district court were allowed to apply the Identity Theft and Assumption Deterrence Act to a state law claim, the plaintiffs would not be able to prove the intent requirement of 18 U.S.C. § 1028(a)(7). *Id.*

Two negligent information security cases decided before and after *Forbes* also highlight the difficulties in proving causation and damages.[65] In *Stollenwerk v. Tri-West Healthcare Alliance*,[66] a security breach resulted in names, addresses, birth dates, and social security numbers of the various healthcare beneficiaries being compromised.[67] Although the breach of contract claim did not survive a motion to dismiss, a negligence claim was reviewed on summary judgment, which allowed the district court to analyze both causation and damages.[68] One of the plaintiffs in *Stollenwerk*, Mark Brandt, produced evidence that after the information security breach there were six attempts to open credit accounts in his name, with two successful attempts generating more than $7,000 in unauthorized charges.[69] Despite Brandt's personal assertions,[70] the only evidence before the district court was temporal evidence showing that the accounts were opened after the breach, which Brandt claimed was the result of the breach.[71]

Absent additional information to prove causation, the district court stated this was an example of *post hoc ergo propter hoc*,[72] which does not allow a reasonable jury to infer that the burglary caused the incidents of identity fraud.[73] Summary judgment for the defendant was granted on all

65. The two cases alluded to are Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005) and Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006).

66. *Stollenwerk*, 2005 WL 2465906.

67. *Id.* at *1. Unauthorized personnel broke into defendant's facilities and removed computer hard drives containing the plaintiffs' personal information. *Id.*

68. *Id.* at *2. In a unique claim, plaintiffs here also compared the loss of their data to a toxic tort claim, in large part claiming that the loss of the data had "infected" them and the harm was likely to occur in the future. *Id.* The district court stated, to win on a toxic tort analogy of identity theft, the plaintiffs would be "required to establish, at a minimum: (1) significant exposure of sensitive personal information; (2) a significantly increased risk of identity fraud as a result of that exposure; and (3) the necessity and effectiveness of credit monitoring in detecting, treating, and/or preventing identity fraud." *Id.* at *4. However, the district court stated that because the plaintiffs were unable to bring forth enough evidence showing that their own personal information was compromised on the laptops and exposed to the thieves, this toxic tort identity theft analogy fails. *Id.* at *5.

69. *Id.* at *1.

70. Brandt claimed that the fraudulent accounts must have been a result of the information security breach because he never transmitted his personal information over the Internet and shredded all mail relating to credit card offers. *Id.* at *6. However, Brandt did also concede he provided his personal information to organizations other than the defendant. *Id.*

71. *Stollenwerk*, 2005 WL 2465906, at *7.

72. "After this, therefore because of this." *Post hoc ergo propter hoc* is a logical fallacy that mistakes causation with temporal circumstances. *Id.*

73. *Id.*

claims.[74] On appeal, however, summary judgment on Brandt's claim was reversed.[75] The appellate court stated that a plaintiff need only show that the Tri-West burglary was a substantial factor in bringing about the result and a factor "without which the injury would not have occurred."[76] Brandt did not need to prove the burglary was the sole cause.[77] Because Brandt put forth enough circumstantial evidence to create a jury question on the issue of causation, the issue was remanded.[78]

In *Guin v. Brazos Higher Education Service Corporation*,[79] Brazos was a nonprofit corporation that originated and serviced student loans.[80] Brazos employed a financial analyst, John Wright, to analyze loan portfolios for a number of transactions, including purchasing portfolios from other lending organizations and selling bonds financed by student loan interest payments.[81] To perform this task, Wright was issued a laptop from Brazos, which contained personally identifiable information of various customers and employees.[82] Wright's home was burglarized and the laptop was stolen; Brazos and Wright did not know what personal information was stored on Wright's laptop.[83] Because Brazos's efforts to determine which borrowers and employees were potentially affected by this breach were unsuccessful, and pursuant to the state's breach-notification statute, Brazos sent a notification letter to approximately 550,000 customers.[84]

---

74. *Id.*

75. Stollenwerk v. Tri-West Health Care Alliance, No. 05-16990, 2007 WL 4116068, at *4 (9th Cir. Nov. 20, 2007).

76. *Id.* at *3

77. *Id.*

78. *Id.* at *4. The circuit court stated:

> Here . . . proximate cause is supported not only by the temporal, but also by the *logical*, relationship between the two events. . . . If as a matter of ordinary experience a particular act or omission might be expected, under the circumstances, to produce a particular result, and that result in fact has followed, the conclusion may be permissible that the causal relation exists. Circumstantial evidence, expert testimony, or common knowledge may provide a basis from which the causal sequence may be inferred.

Id. at *3.

79. No. Civ. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006).

80. *Id.* at *1.

81. *Id.*

82. *Id.*

83. *Id.*

84. *Guin*, 2006 WL 288483, at *2.

Stacy Guin received one of these notification letters.[85] Guin sued Brazos for, amongst other things, negligence.[86] In the damages analysis, the district court stated that a plaintiff must suffer some actual loss or damage and that the threat of harm does not meet this requirement.[87] Guin was unable to prove any actual damages after the negligent security breach.[88] The district court cited to the proposition set forth in *Stollenwerk*'s district court opinion[89] and granted summary judgment for the defendant.[90]

III. ANALYSIS OF ECONOMIC MODELS IMPACTING CORPORATIONS AND CORPORATIONS LAW

A. *Economic Models Impacting Corporations*

When Adam Smith wrote *The Wealth of Nations*, he gave birth to the modern study of economics. In his book, Smith argued that when a person makes the best possible economic choice, that choice leads to the best outcome for society as a whole. This "invisible hand" theory is extracted from the following quote from Smith:

> By preferring the support of domestic to that of foreign industry, he intends only his own security; and by directing that industry in such a manner as its produce may be of the greatest value, he intends only his own gain, and he is in this, as in many other cases, led by an *invisible hand* to promote an end which was no part of his intention. Nor is it always the worse for the society that it was not part of it. By pursuing his own interest he frequently promotes that of the society more effectually than when he really intends to promote it.[91]

Although the quote was addressing the choice of domestic–versus–foreign goods, the underlying principles of division of labor and

85. *Id.* Guin acquired a student loan through Brazos. *Id.*

86. *Id.* Guin, originally, also brought a breach of contract claim that was later dropped. *Id.* Because the damage analysis is similar to the contract damage analysis, this case was included.

87. *Id.* at *5

88. *Id.* at *6.

89. *See* Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906, at *7 (D. Ariz. Sept. 6, 2005).

90. *Guin*, 2006 WL 288483, at *7.

91. ADAM SMITH, THE WEALTH OF NATIONS, bk. IV, ch. 2, *available at* http://www.bibliomania.com/2/1/65/112/frameset.html (last visited Feb. 24, 2008) (emphasis added).

free markets have been applied in several areas of economics, including market equilibrium. Market equilibrium is a situation where the opposing market forces of supply and demand balance each other.[92]

One economic factor that does not impact the market equilibrium model equally for certain market players is negative externalities.[93] An externality is a cost or benefit that arises from production and falls on someone other than a producer.[94] Pollution is a commonly used example of a negative production externality for didactic purposes. Suppose a factory is adjacent to a housing community. When the factory produces goods, the pollution generated from factory production that floods the air and adjacent waters is a negative production externality. Because of the pollution, the amount of money a person is willing to pay to live in the housing community decreases because he or she is taking into account that he or she will have to live with the pollution. The pollution, however, does not impact the market for the goods the factory produces, thus providing little incentive for the factory to combat the pollution. The overall market outcome and allocation of resources is inefficient in light of the market equilibrium because in this scenario, although the marginal cost[95] equals the marginal benefit,[96] marginal benefit does not equal the marginal social cost.[97]

One way to place a market with negative externalities back into equilibrium, and thereby ensure an efficient allocation of resources, is to create property rights in the externality.[98] In the factory-housing community example, if the factory owned the housing community, it would have a new incentive to decrease the amount of pollution it generates, because reduced pollution in the housing community allows the factory to charge more for housing. That is of course assuming the amount of profit from the housing community exceeds the cost of eliminating the waste.

---

92. MICHAEL PARKIN, MICROECONOMICS 68 (6th ed., Addison Wesley 2003). Market equilibrium can be expressed in a variety of ways, including when supply equals demand, or when the marginal cost equals the marginal benefit.

93. *Id.* at 410.

94. *Id.*

95. Marginal cost is the cost to the factory of producing the pollution-creating goods.

96. Marginal benefit is the cost a private person is willing to pay for the pollution-creating goods.

97. Marginal social cost is calculated when the factory in this example takes into account both the private production of the good, and the external cost of the pollution.

98. PARKIN, *supra* note 92, at 414. A property right is a legally established title to the ownership, use and disposal of factors of production and goods and services that are enforceable in the courts. *Id.*

Properly applied, these same economic principles create financial incentives for companies to reduce their susceptibility to information security breaches. Currently, corporations that aggregate personal information are only regulated by various data breach notification statutes.[99] Although the aggregation of data makes a corporation more efficient in several respects, it also creates a negative production externality by making the information more susceptible to an identity thief. Because a corporation does not bear the cost of identity theft, it is a negative production externality examined relative to the corporation. If the law begins to recognize damages that corporations must bear for data breaches, economics suggest that a corporation will take these costs into account when assessing its practice of aggregating personally identifiable information. Furthermore, if corporations begin to internalize the cost of data breach, the market equilibrium model suggests this will result in a more efficient allocation of resources for everyone in the market. In order to have this market impact, however, the law must recognize a scheme for assessing damages for data breaches. Also, just like the factory-housing community example, the cost a company must bear for any data breach must exceed the cost of better protecting the information in order for this market equilibrium to occur.

B. *Control-Share Premiums in Corporations Law*

Black's Law Dictionary defines "control premium" as, "[a] premium paid for shares carrying the power to control a corporation. The control premium is often computed by comparing the aggregate value of the controlling block of shares with the cost that would be incurred if the shares could be acquired at the going market price per share."[100] However, some courts provide alternate valuation theories for a control premium.[101] Ultimately, the control premium is determined on a case-by-case basis. In *Doft & Co. v. Travelocity.com, Inc.*,[102] the *Doft* court applied a 30% control premium using a combination of factors including EBITDA[103] and

99. For an excellent and well-researched analysis of data breach notification laws, see Brandon Faulkner, Note, *Hacking Into Data Breach Notification Laws*, 59 U. FLA. L. REV. 1097 (2007).

100. BLACK'S LAW DICTIONARY 1219 (8th ed. 2004).

101. *See generally* Martin v. Marlin, 529 So. 2d 1174, 1176 (Fla. 3d DCA 1988) (stating the control-share premium will be some percentage of the anticipated increase in value once the transfer of control is effectuated).

102. No. Civ.A. 19734, 2004 WL 1366994 (Del. Ch. June 10, 2004).

103. EBITDA («ee-bit-dah» or «ee-bit-dee-eh») is an acronym for earnings before interest, taxes, depreciation, and amortization. Therefore it measures operating cash flow in an organization.

EPS.[104] Whereas in *PNB Holding Co. Shareholders Litigation*,[105] the defendant's expert found a 7.37% control premium and the plaintiff's expert found a 10% control premium based on the same set of facts.[106]

The control premium is recognition that buyers of stock are willing to pay more on a per-share basis than if the shares were not part of the controlling block.[107] In essence, the premium is a "payment for power rather than stock."[108] Power in the control premium context refers to the ability of the buyer to install his own management team, reduce costs, and increase corporate profitability.[109] Various courts have recognized, in line with a free market theory, that "the economy is best served by allowing control premiums to be retained by sellers."[110]

IV. THE CURRENT STATE OF IDENTITY THEFT AND REMEDIAL MEASURES

A. *A Call For a Right of Privacy*

Companies traditionally collect an eclectic amount of personally identifiable information on their employees and customers for security, credit, accountability, or marketing purposes. The collection of personally identifiable information is not limited to one industry. Rather, business, service, medical, and even educational entities will aggregate personally identifiable information. Although the technology currently used to aggregate large amounts of data raises several privacy concerns, the principles underlying a right to privacy are not a recent development.

In 1890, Samuel Warren and Louis Brandeis wrote *The Right to Privacy*, where both essentially called for a right to be left alone.[111] At the time of this article's publication, privacy concerns were raised with the creation of a snap camera that was inexpensive, portable, and capable of taking instantaneous photographs of people.[112] Warren and Brandeis feared that this technology "invaded the sacred precincts of private and domestic

104. EPS is an initialism for "earnings per share," which represents the earnings returned on the initial investment amount.

105. No. Civ.A. 28-N, 2006 WL 2403999 (Del. Ch. Aug. 18, 2006).

106. *PNB Holding Co.*, 2006 WL 2403999, at *23-25.

107. Alfred Hill, *The Sale of Controlling Shares*, 70 HARV. L. REV. 986, 986 (1957).

108. *Id.* at 987.

109. Frank H. Easterbrook & Daniel R. Fischel, *Corporate Control Transactions*, 91 YALE L.J. 698, 705 (1982).

110. Martin v. Marlin, 529 So. 2d 1174, 1176 n.5 (Fla. 3d DCA 1988).

111. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

112. *Id.*

life"[113] and that the law should "afford some remedy for the unauthorized circulation of portraits for private persons."[114] Although the Supreme Court found a constitutional right of privacy in the penumbras of the Bill of Rights,[115] this right had less recognition in the areas of contract, property, and tort law when claims involved personally identifiable information.[116]

Nevertheless, there is a distinction between a person who maliciously uses personal information for identity theft[117] purposes and a corporation that originally collected and housed the information that is later used by an identity thief. In October 1998, with identity theft rising,[118] Congress enacted the Identity Theft and Assumption Deterrence Act[119] to make identity theft a federal crime. Six years later, President Bush signed the Identity Theft Penalty Enhancement Act,[120] creating a mandatory two-year-minimum sentence to be served by convicted defendants in addition to their aggravated identity theft sentence.[121] President Bush stated, "[The Identity Theft Penalty Enforcement Act] reflects our government's resolve to answer serious offenses with serious penalties."[122]

What about a corporation that aggregated personally identifiable information that was used by an identity thief? Should the corporation also be held accountable for the costs associated with repairing a stolen

---

113. *Id.*

114. *Id.*

115. *See* Griswold v. Connecticut, 381 U.S. 479, 483, 485 (1965).

116. Vera Bergelson discussed the treatment of personal information in a property and tort context, finding that neither property nor tort theory recognizes individuals' rights in their personally identifiable information. Vera Bergelson, *It's Personal, But is it Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 403 (2003); *see also* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).

117. "Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes." Federal Trade Commission, About Identity Theft, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Feb. 24, 2008).

118. Robert O'Harrow believes identity theft has risen because "we are awash in information about ourselves. Twenty-four hours a day, every day of the year, the credit bureaus, information services, groceries, pharmacies, toll collectors, banks, and other institutions gather information about [citizens]." ROBERT O'HARROW JR., NO PLACE TO HIDE 83 (2005).

119. Pub. L. No. 105-318, *supra* note 61.

120. Pub. L. No. 108-275, 118 Stat. 831 (2004), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf (last visited Jan. 12, 2008).

121. 18 U.S.C.A. § 1028A (West 2004).

122. President George W. Bush, Remarks by the President at Signing of Identity Theft Penalty Enhancement Act (July 15, 2004), *available at* http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html.

identity? Based on the rampant mishandling of information outlined below, the answer is a resounding yes.

B. *Fueling the Litigation Fire: Information Security Mishandlings and Startling Identity Theft Statistics*

Companies have a history of failing to adequately secure collected information.[123] For example, in 2003, Acxiom experienced a breach where a hacker decrypted various passwords of the company, and then began downloading the names, credit card numbers, social security numbers, addresses and various other detailed information of approximately twenty million people.[124] Between 2003 and 2005, ChoicePoint suffered a major security breach, where the private information of over 145,000 people was improperly accessed, ultimately leading to over 700 cases of identity theft.[125] In 2007, information from 45.7 million credit and debit cards was stolen from TJ Maxx,[126] and a compact disc containing Medicaid information of 2.9 million Georgians was lost while being shipped from Atlanta to Maryland.[127]

In 2003, the Federal Trade Commission released an Identity Theft Survey Report.[128] The report highlights the nightmare of identity theft by presenting a series of startling statistics. After examining all forms of identity theft, the report concluded that identity theft affects 4.6% of the population, which equated to approximately ten-million people during the study.[129] The average loss of money and goods obtained by an identity thief was $4,800; whereas, the average loss to a victim, including the

123. For a continuously updated list of data security breach cases, see Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, *available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 24, 2008).

124. O'HARROW JR., *supra* note 118, at 71.

125. DANIEL J. SOLOVE ET AL., PRIVACY, INFORMATION, AND TECHNOLOGY 255 (2006); *see also ChoicePoint: More ID Theft Warnings*, CNN, Feb. 17, 2005, http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/.

126. *Corporate Owner of T.J. Maxx, Marshall's Says Information for 45.7 Million Cardholders Stolen*, FOX NEWS, Mar. 29, 2007, http://www.foxnews.com/story/0,2933,262300,00.html.

127. *Disk With Data on 2.9M Georgians Lost*, ABC NEWS, Apr. 10, 2007, http://abcnews.go.com/US/wireStory?id=3026319; a copy of the official public notice is *available at* http://dch.georgia.gov/vgn/images/portal/cit_1210/19/38/80010015Public_Notice-Missing_Personal_Data.pdf (last visited Feb. 24, 2008).

128. FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT (2003) [hereinafter Identity Theft Survey Report], *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited Feb. 24, 2008).

129. *Id.* at 7.

money spent to remedy the identity theft was approximately $500.[130] An individual spends, on average, thirty hours resolving an identity theft;[131] identity theft is discovered 26% of the time with corporate notice and 52% of the time by a person simply monitoring his or her accounts.[132] In 2007, the Federal Trade Commission released its annual report entitled, "Identity Theft Victim Complaint Data."[133] The report detailed identity theft complaints by victim age. Persons between the ages of 18 and 29 comprised 29% of all identity theft complaints, with the subsequent, older age groups, all gradually declining to smaller percentages.[134]

The monetary losses from identity theft affect people in various ways. The ramifications of identity theft include, but are not limited to: credit card problems, harassment by debt collectors, loan rejection, banking problems, insurance rejection, utilities being turned off, civil litigation, and criminal investigation.[135]

By juxtaposing the recent examples of information security breaches with identity theft statistics, the need for a legal remedy against corporations is apparent. Reviewing the previous incidents and statistics begs the question of how these incidents occur. Corporate vulnerability, surprisingly, usually occurs in plain sight.

C. *Corporate Vulnerability*

Too often corporations, and people, believe the key to preventing identity theft is shredding personal documents, installing the latest technology designed to combat identity theft, or not visiting certain web sites. However, for corporations, Kevin Mitnick argued that the weakest link is the human element.[136] In his book, *The Art of Deception*, Mitnick relayed dozens of social-engineering schemes that expose the human element of security. Depending upon the nature of an attack—conversing with an employee on the phone or in person—Mitnick relayed several tactics for successfully stealing valuable information by essentially having

130. *Id.*

131. *Id.*

132. *Id.* at 39.

133. FEDERAL TRADE COMMISSION, IDENTITY THEFT VICTIM COMPLAINT DATA (2007), *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf (last visited Feb. 24, 2008).

134. *Id.* at 7.

135. For a more detailed account of identity theft, its problems, and how to combat it on a personal level the Federal Trade Commission has created the following web site, http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html (last visited Feb. 24, 2008).

136. KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 3 (Carl Long ed., Wiley Publishing 2002).

a company's own employees work against the company.[137] No matter which method of attack a person employs, the common warning signs within all attacks include: use of corporate lingo, claims of authority, name dropping, stress of urgency, flirting, out-of-ordinary request, and a refusal to give a callback number.[138]

Mitnick's assertion of social engineering casts employees of the corporation as an innocent victim of an attack. However, identity theft also arises when employees steal a company's information. In *Identity Theft, Inc.*, Glenn Hastings relays that he accomplished his first major identity theft scheme by using credit card information he observed in his normal course of business as a hotel front-desk employee to make grandiose purchases, such as Navajo rugs.[139] However, various identity theft schemes Hastings described in his book are far more complex than social engineering or simply copying information from a credit card.[140]

In light of both Mitnick and Hasting's showing that identity theft can arise from people either inside or outside a corporation, who should be held accountable for information security breaches—the employee, the corporation, or both? This Note suggests that a corporation is in the best position to implement the necessary training to prevent these data breaches, making it the more ideal candidate to bear the loss. Also, holding a corporation liable for data breach loss lessens the risk of a judgment-proof defendant.

V. FINDING A BREACH OF CONTRACT CLAIM FOR INFORMATION SECURITY BREACHES

A proposal for a breach of contract remedy for information security breaches is not without critics. Identity theft is not just a claim that affects individual citizens. Rather, "[i]dentity theft can spell disaster for any

137. *Id.* at 332-33. Although the book provides a detailed series of examples and explanations of the cons, Mitnick provides a concise summary at the end of the book where he states several common social-engineering methods including, but not limited to: posing as a fellow employee; posing as someone in authority; offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call them for help; or pretending to be from a remote office and asking for e-mail access locally. *Id.* at 332.

138. *Id.* at 333.

139. GLENN HASTINGS & RICHARD MACRUS, IDENTITY THEFT, INC. 19-40 (2006).

140. Hastings provides another example, in addition to his major scheme of applying for multiple credit cards at once, where he was able to call the Social Security Administration and obtain social security numbers over the phone by providing information that was available in the volumes of *Who's Who* in the local library. *Id.* at 45-55.

business, from a one-person operation to a Fortune 500 company."[141] Identity theft risk management specialist John Gardner, Jr. claims that "[l]itigation brought by employees or customers over identity theft can doom a business."[142] Simply stated, "[i]dentity theft is a problem that could cost businesses hundreds of thousands of dollars."[143]

Despite the looming liability that a corporation faces from identity theft, if a corporation is forced to recognize the damages and causation proposals below, it will reallocate its resources more efficiently for society and achieve market equilibrium.[144] Because data breaches from a corporate standpoint are still largely a negative production externality,[145] it is crucial that a private breach of contract action exist in order to provide the necessary incentive for a corporation to adjust its data-handling practices. When juxtaposing the statistics of identity theft with information security breach incidents, it becomes clear that under current practices the data breach notification statutes are not forcing corporations to allocate resources efficiently. Hence, a new proposal is in order.

A. *Calculating Damages for Breach of Contract*

In most of the cases discussed, the breach of contract theory for information security breaches never made it beyond the summary judgment phase of civil litigation because the plaintiff failed to provide evidence of either causation or damages.[146] However, by fusing contract law together with the law of corporations, damages become evident in information security breach scenarios. The proposal below is not calling for an expansion of any one area of law; rather, the proposal is a recognition of multiple areas of law that should not be treated separately.

1. Control-Share Premium Applied to Personally Identifiable Information

As stated, the law of corporations recognizes a control-share premium for the aggregation of a certain amount of shares that provide the shareholder with the ability to always control a vote placed to the

141. Ben Heath, *The Dangers of Identity Theft*, ADVOCATE-CT, Dec. 14, 2006, *available at* 2006 WLNR 21548271.

142. *Id.*

143. Jeff Postelwait, *Identity Theft Poses Liability For Businesses*, TULSA WORLD, Dec. 6, 2006, *available at* 2006 WLNR 21136370.

144. *See supra* notes 91-98 and accompanying text.

145. *See supra* text accompanying note 93.

146. *See supra* text accompanying notes 41–90.

shareholders.[147] It is not that the shares themselves are any different from non-controlling shares; but rather, there is value in aggregation. In today's world, a person is more than a living, breathing organism. In the realm of identity theft, a person is a full name, social security number, temporary address, permanent address, date of birth, bank account number, and telephone number. If contracts law and the law of corporations apply the same concept of a control-share premium to information security breaches, then the law would recognize that there is latent value in the aggregation of personally identifiable information. A name and social security number independent of one another have little to no monetary value. The aggregation and linkage of these two independently valueless pieces of information, however, give rise to value in the form of identity theft. Simply stated, the aggregation of personally identifiable information gives rise to a human clone—strength in numbers.

Once personally identifiable information is aggregated, an identity thief can begin applying for credit cards, or even mortgages. By way of example, a person may apply for an American Express credit card online with no human interaction.[148] In order to apply for "Blue from American Express Card," a user only needs a series of informational data that is commonly aggregated by corporations.[149] Perhaps the two more difficult pieces of information to collect about a person in order to complete the American Express credit card application would be both the "annual household income" and the "income source." In the information security breach context, because the breach is occurring at the employment level, this information can either be guessed with reasonable certainty based on a person's job title or stolen along with the other information. If the credit card application also asked for information about a person's mortgage or

147. *See supra* text accompanying notes 100-10.

148. At American Express's web site, a user can either apply directly for a card he or she wants, or complete a questionnaire that allows the web site to indicate which card is best suited to fulfill the user's needs, *available at* http://www201.americanexpress.com/apply/Fmacfservlet?csi=0/20/b/0&us_nu=subtab (last visited Feb. 24, 2008). Besides American Express, other credit cards can be obtained simply by completing various fields online. In order to obtain a Visa credit card from Bank of America, you need a person's first name, last name, address, city, state, zip code, number of years at a physical address, monthly housing payments, social security number, date of birth, mother's maiden name, and an e-mail address, *available at* https://www2.bankofamerica.com/creditcards/application/index.cfm?requesttimeout=500&offer_id=ECOMM090BAWI0040 0800122126EN004&requestTimeout=120&newapp=y&state=undefined (last visited Feb. 24, 2008).

149. Specifically, to apply for a Blue from American Express online, the only "required" pieces of information include: first name, last name, date of birth, social security number, home address, city, state, zip code, annual household income, and income source, *available at* https://www201.americanexpress.com/cards/Applyfservlet?csi=38/23000/b/10/0/0/0/n&from=2 (last visited Feb. 24, 2008).

monthly mortgage payments on a home, that information is also obtainable through the public domain by simply visiting the appropriate county property appraiser's web site.

Credit card applications are just the beginning. They represent a principle that contracts law should adopt from the law of corporations: there is latent value in aggregating personally identifiable information, just like a control-share premium. If contract law applies the control-share premium concept to personally identifiable information, the issue then becomes how to actually measure the damages.

2. Information Security Breach As a Lost Income-Producing Asset

In contracts law, the losses arising from information security breaches should be treated as a special damage because the losses occur as a result of the defendant's breach, but do not include the value of the promised performance.[150] If a data breach is treated as a special damage,[151] in light of *Schonfeld v. Hilliard*,[152] the aggregation of personally identifiable information should be treated as an "income-producing asset," which includes intangible property.[153] If personally identifiable information is treated as an income-producing asset, then the issue still becomes how to assess the market value of the income-producing asset at the time of the breach. Contract law provides a source.

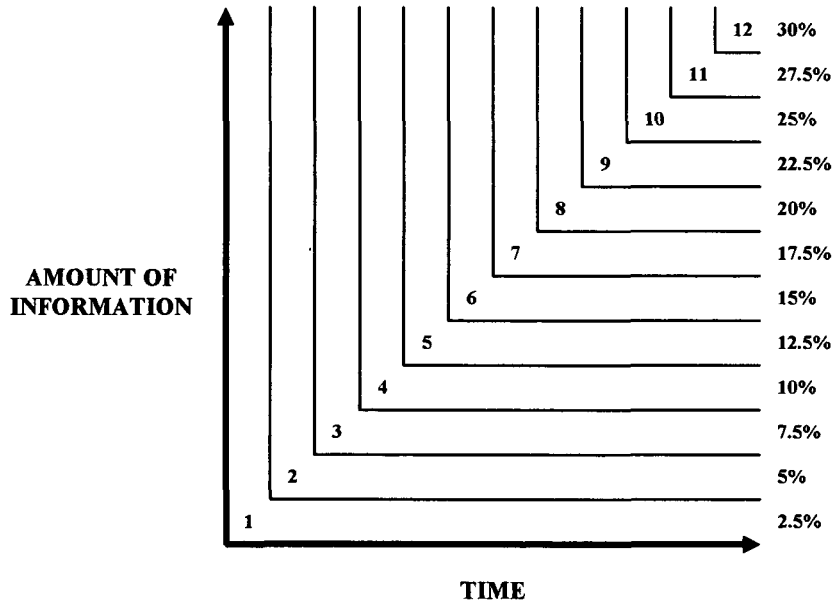
In *Eastern Air Lines, Inc. v. Gulf Oil Corporation*,[154] Gulf Oil entered into a contract to sell jet fuel to Eastern Air Lines.[155] In the contract, both parties acknowledged the constant fluctuation of oil prices due to external factors, so both agreed that the price of oil would be based upon an indicator: West Texas Sour.[156] The West Texas Sour was an independent party that calculated the price of oil, which in turn was physically posted at a public location to reflect the current price that an oil company will pay for a given barrel of crude oil.[157] This same act of pegging a price of oil can be applied to the information security breach cases.

The appropriate party to establish a measurement system to peg damages to claims is the Federal Trade Commission, because it already provides multiple services for identity theft victims. Figure A (below) provides a system of calculating the market value of an income-producing

150. *See* Schonfeld v. Hilliard, 218 F.3d 164, 176 (2d Cir. 2000).
151. *Supra* text accompanying note 10.
152. *Schonfeld*, 218 F.3d at 164.
153. *Id.* at 177.
154. 415 F. Supp. 429 (S.D. Fla. 1975).
155. *Eastern Air Lines*, 415 F. Supp. at 432.
156. *Id.* at 432-33.
157. *Id.* at 433.

asset that should arise from an information security breach at the time of breach. The X-axis indicates the length of time a corporation holds information, with time increasing as you move further to the right away from the point (0,0). The Y-axis is the amount of information collected by a corporation. Ascension on the Y-axis is linked directly with the amount of information a corporation aggregates. The more personally identifiable information aggregated, the higher a corporation rises on the Y-axis. There are a variety of ways the Federal Trade Commission can calculate the value of the Y-axis, but the principle is easily understood without getting into the arithmetic, which can be calculated by the Federal Trade Commission.[158]

Figure A. Data Breach Percentage Points



Unlike a traditional (X,Y) chart, Figure A has been designed into a leveled structure. If a company's Y-axis value is extremely low because it only aggregated a person's name and telephone number, no matter how

158. Any system of calculating the value on the Y-axis should consider adding weight to certain variables. For example, consider the situation where company A collects a person's name and social security number, whereas company B only collects a person's name and telephone number. Company A's data breach percentage point should be plotted higher on the Y-axis because a person's social security number has more value than a person's telephone number for identity theft purposes.

long it retains that information, it will always remain in level one, because the risk of identity theft from aggregating those pieces of information is extremely low. However, once a company aggregates more information, it moves higher on the Y-axis, and depending upon how long it retains the information, the company will begin to move horizontally right into different percentage levels over time. The policy reasoning behind this leveled structure is that a company that aggregates such a minimal amount of information is less likely to be susceptible to identity theft and should not be penalized in the same manner as a company that aggregates the requisite information to apply for credit cards. Moreover the graph provides an economic incentive to both aggregate a minimal amount of information, and not to keep it for a lengthy period of time.

On the right side of Figure A are corresponding "percentage points" that correspond to a level a company falls within based on the (X,Y) value. Similar to the West Texas Sour price indicator for oil,[159] the Federal Trade Commission could use Figure A to assess a market value of an income-producing asset at the time of breach for an information security breach. Depending upon which level a corporation falls within, the percentage point could be multiplied against either the corporation's total profits for the previous six or twelve months, or perhaps even the total assets of the corporation.[160] The resulting number would then be divided by the number of affected employees. The quotient is the measure of damages per person.

For example, assume Company-A has 100 employees. If Company-A aggregated enough information to place itself lateral to level six on the Y-axis of Figure A, and then retained the information about the employees long enough to move horizontally into level six, then Company-A is subject to a 15% penalty at the time of an information security breach. In contract terms, the market value of the income-producing asset at the time of breach is 15%. If the corporation was the unfortunate victim of an information security breach, the corporation would become liable for an amount equaling 15% of either the corporate profits or corporate assets. Assume for this example that the 15% is applied to corporate profits from the previous six months, which hypothetically equals $1,000,000, then the corporation is liable for a total amount of $150,000. The resulting time-stamped figure, $150,000, would then be divided by the number of affected employees. If in this example 100 employees were affected, the

159. *Eastern Air Lines*, 415 F. Supp. at 433.

160. If this standard is adopted, the mathematical formula to calculate the Y-axis and the numeric value to be factored against the percentage points are details that can be resolved at a later time. Principle alone, this pegging system provides the necessary incentive to force corporations into market equilibrium.

result would be a total loss per person of $1,500.[161] Considering the average loss of identity theft when new accounts are established on a per victim basis is approximately $1,180,[162] this example does not appear unreasonable.

A percentage scheme is proposed so that each corporation is affected equally. Considering both small and large corporations aggregate information, providing a preset statutory penalty would hurt small corporations much more than larger corporations. Under a preset statutory penalty system, larger corporations would have no economic incentive to fix its data security practices. In order to reach market equilibrium and have market resources allocated efficiently, it is crucial that each corporation is affected severely enough that the cost to the corporation to provide better data security practices is less than the cost of the resulting penalty of a breach. An affected employee should be able to prevail against summary judgment if the Federal Trade Commission established this pegging system. In the event the (X,Y) value yields an absurdly high result or low result, it can be adjusted later by the jury or court. Nevertheless, this system of pegging damages provides a way to proceed beyond the summary judgment phase of civil litigation.

Because contract law allows for contracts to reference external indicators, it is unlikely this pegging system will fail the damages portion of a lawsuit because the system will not be considered too speculative. However, a person is still obligated to mitigate damages. In this context, a person is required to obtain a credit report and establish a credit alert monitoring system. Moreover, if the pegging system remains a common law remedy and a statutory penalty, due process violations are avoided.[163]

The data breach pegging system is open to criticism because not everyone's information that is stolen through an information security breach is later used by an identity thief. However, in order to force a company to recognize these costs economically, it is essential that a company face the risk of total loss resulting from data breach so it can take the appropriate measures to fix its data handling practices. By establishing this pegging system, it is as if the factory in the factory-housing community pollution example owned the housing community and will achieve greater profits by taking steps to reduce pollution. Or here, take steps to reduce data breaches.

---

161. $150,000 / 100 = $1,500.

162. Identity Theft Survey Report, *supra* note 128.

163. *See* State Farm Mut. Auto. Ins. Co. v. Campbell, 538 U.S. 408, 416 (2003) (stating "[t]he Due Process Clause of the Fourteenth Amendment prohibits the imposition of grossly excessive or arbitrary punishments on a tortfeasor").

B. *Determining Causation for Information Security Breach*

Causation provides an extremely challenging situation for pursuing a breach of contract claim. Because all personally identifiable information is an intangible asset, it can be perfectly replicated in a variety of mediums. This situation gives rise to the question, when a person is subject to identity theft, how does the person know the information from the data breach was the same information that was used in an actual identity theft? Absent biometric data or some other way to pinpoint an actual source, there is really no way of determining absolute causation. Although it is more likely that a corporation subject to a data breach was the cause of a subsequent identity theft, contracts law and economics refuse to recognize temporal relationships for causation.[164] A plaintiff may prevail, however, if he can show the information security breach was a substantial factor in bringing about the identity theft.[165]

1. Class Action Litigation for Information Security Breach

One way to surmount the causation problem is with a class action lawsuit. Federal Rule of Civil Procedure 23 (FRCP 23) governs class actions lawsuits in federal court. Although contract claims are driven by state law, FRCP 23 provides the necessary framework for the following examples. Once one person is actually the victim of identity theft following an information security breach, he or she may bring a breach of contract suit, and will hopefully be able to prove by a preponderance of evidence, that the identity theft resulted from the actual data breach in question.[166] Causation in this context is provable by a showing that the person has not given certain information to other parties, that other parties holding the person's personally identifiable information have not experienced a breach, or that the identity was located and linked to the resulting data breach.

While this initial causation is being established, the named plaintiff can seek to certify a class, which would be narrowly defined to include only those persons whose information was absolutely stolen during a data breach. Defining the class any broader may result in a class decertification or falling victim to a motion of summary judgment.[167] If a class is defined,

---

164. *See supra* text accompanying note 72.

165. *See supra* text accompanying notes 76-78.

166. *See generally supra* text accompanying notes 76-78.

167. *See* Wal-Mart Stores, Inc. v. Bailey, 808 N.E. 2d 1198, 1204 (Ind. Ct. App. 2004) (ruling that a class defined as "[a]ll current and former hourly employees of Wal-Mart Stores, Inc. (including its operating divisions Sam's Club and Wal-Mart Supercenters) in the State of Indiana during the period August 1, 1998 to present" is overbroad because it "includes members who never

it is no longer a matter of determining causation of everyone in the class; rather, just seeing if the person falls within the definition of the class.

As with all class action lawsuits, the claims being aggregated into a class cannot be highly specialized and must share a degree of commonality and typicality. One roadblock between a breach of contract claim and class certification is that courts, "have repeatedly held that breach of contract claims are inappropriate for class certification [because] they involve individualized inquiries to determine liability and damages."[168] However, in the realm of information security breaches, everyone in the class has experienced virtually the same exact injury. Unlike a class certified under a breach of contract theory for unfair treatment or prejudicial treatment in the workplace, there is no individual weighing that needs to occur. Thus, in this limited scenario, certifying a class under a breach of contract theory seems appropriate.

2. Shifting the Burden of Proof

Another way to surmount the difficulties in proving damages from an information security data breach would be to simply shift the burden of proof to the corporation to prove that the resulting identity theft was not caused from the corporation's mishandling. Just like creating property rights to recognize the cost of externalities, shifting the burden of proof is another way to hold corporations liable, and force corporations to calculate the cost of litigation when deciding how many resources it wishes to allocate in order to protect personally identifiable information that has been aggregated. As the market equilibrium model indicates, if a corporation recognizes these costs, then the resulting allocation of resources should be the most efficient allocation possible.

VI. A DEPARTURE FROM LEGAL REMEDIES: INFORMATION SECURITY INSURANCE

Another way for a corporation to protect itself, or for private citizens to protect themselves, against identity theft is with identity theft insurance. Identity theft insurance is a recent phenomenon resulting from the fast rising numbers of identity thefts.[169] The general purpose of identity theft insurance is to "[clean] up the mess left by identity theft, such as clearing

worked off the clock" and therefore "have no interest in the lawsuit").

168. Gilman v. John Hancock Variable Life Ins. Co., No. 02-00051 AB, 2003 WL 23191098, at *15 (Fla. 15th Cir. Oct. 20, 2003).

169. Pamela Yip, *Identity Thefts Generate Protection Trade*, BRADENTON HERALD, Apr. 17, 2007, *available at* 2007 WLNR 7227784.

up false credit card charges and fixing credit ratings."[170] Allstate Insurance has also joined other insurance companies in this field by selling a $40-a-year identity theft insurance policy in Florida that offers customers up to $25,000 in reimbursement for expenses incurred in trying to restore their credit standing.[171] However, most identity theft insurance policies run between $25 and $50 annually.[172]

Identity theft insurance has its critics. Most notably is Frank W. Abagnale.[173] Abagnale claims that identity theft insurance is a ripoff.[174] Because most insurance plans already provide coverage for identity theft, Abagnale claims purchasing identity theft insurance is "giving them two worthless policies."[175]

VII. CONCLUSION

The previous pages have outlined the current hurdles contracts law poses to provide for a legal remedy against corporations that have aggregated personally identifiable information, which was subsequently stolen. Because many plaintiffs have been unable to prove damages or causation from a resulting breach, corporations have had little incentive to increase the durability of data management practices. Only by forcing companies to bear the cost of information security breaches will the market of corporations reach market equilibrium and result in an efficient allocation of resources for both corporations and consumers.

By fusing together contracts law and the law of corporations, it is possible to calculate the necessary damages and causation in order to defeat a motion of summary judgment and place the matter before a jury. With identity theft rapidly rising, policy considerations push the current state of the law towards recognizing these elements. This proposal weaves two realms of law together for an efficient outcome.

---

170. Theresa Agovino, *Identity Theft Insurance Will Help Pay Cost of Clearing Your Name*, BUFF. NEWS, Mar. 26, 2007, *available at* 2007 WLNR 5712050.

171. Thomas S. Brown, *Insuring Your Identity: Firms Offer Financial Privacy Protection*, DAYTONA NEWS J., Apr. 7, 2007, *available at* 2007 WLNR 6720949.

172. *Id.*

173. Frank W. Abagnale is one of the world's most respected authorities on the subjects of forgery, embezzlement, and secure documents. For over thirty years he has lectured to and consulted with hundreds of financial institutions, corporations, and government agencies around the world. Abagnale was the subject of a major motion picture entitled CATCH ME IF YOU CAN (Dreamworks SKG 2002), directed by Steven Spielberg with Leonardo DiCaprio and Tom Hanks.

174. Yip, *supra* note 169.

175. *Id.*