Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 5 | Issue 1 Article 3

2010

Warranting Data Security

Juliet E. Moringiello

WARRANTING DATA SECURITY

Juliet M. Moringiello[*]

INTRODUCTION

Massive data security breaches have grabbed headlines in the past few years. The data thieves responsible for these breaches have stolen the credit and debit card data of customers of retailers such as TJ Maxx,[1] DSW Shoe Warehouse,[2] BJ's Wholesale Club,[3] and the Hannaford grocery store chain.[4] A thief in control of payment card data, which can include debit and credit card numbers, expiration dates, security codes, and personal identification numbers,[5] has the ability to open new credit accounts and make charges on existing consumer accounts. These data breaches leave individuals fearful that their personal information will be used in ways that will disrupt their financial transactions and damage their credit.[6]

The legal protection of privacy in the United States is far from comprehensive.[7] The level of privacy protection provided to individuals depends on the sector of the economy in which they are participating.[8] One sector of the economy in which privacy legislation exists is the financial sector, but the protection provided by such legislation is not comprehensive.[9] Although individuals may think that they have some protected right to financial privacy because of the Gramm-Leach-Bliley Act, that statute—which requires financial institutions to disclose their privacy policies to consumers—does nothing to protect the consumer when

---

[*] Professor, Widener University School of Law. I thank Ted Janger for organizing the Symposium at which this paper was presented, and all the participants, especially James Grimmelmann and Sarah Jane Hughes, for their very helpful comments on an early draft. Matthew Banks provided terrific research assistance for this Article.

1. Ross Kerber, *Banks in Region Set to Sue TJX Over Breach; Group Says Its Plan Reflects Ire Over Lax Security by Retailers*, BOS. GLOBE, Apr. 25, 2007, at C1; Joseph Pereira, Jennifer Levitz & Jeremy Singer-Vine, *U.S. Indicts 11 in Global Credit-Card Scheme*, WALL ST. J., Aug. 6, 2008, at A1.

2. Bill Husted & David Markiewicz, *Info Theft Slams Chain; 1.4 Million Card Numbers Stolen*, ATLANTA J.-CONST., Apr. 20, 2005, at A1.

3. Todd Mason, *Philadelphia-Based Sovereign Bank to Replace 83,000 Compromised Debit Cards*, KNIGHT RIDDER TRIB. BUS. NEWS (Washington), June 4, 2004, at 1.

4. Mark Albright, *Grocer Credit Data is Swiped*, ST. PETERSBURG TIMES, Mar. 18, 2008, at D1.

5. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 116 (D. Me. 2009).

6. *Identity Theft: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. 28 (2005) (statement of Deborah Platt Majoras, Chairman, Fed. Trade Comm'n).

7. *See, e.g.*, MARGARET JANE RADIN, JOHN A. ROTHCHILD, R. ANTHONY REESE & GREGORY M. SILVERMAN, INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORK 390–92 (2nd ed. 2006).

8. *Id.*

9. *Id.* at 391.

her financial information is stolen from the payment system.[10] Despite the fact that almost all states have provided a measure of protection to consumers by enacting data breach notification statutes, these statutes merely require companies that hold consumer data to notify consumers of a breach so that the consumers can protect themselves.[11] Data breach notification statutes do not grant a private right of action to consumers to recover their losses.[12] A comprehensive statutory and regulatory scheme allocates losses in the credit and debit card systems, and this scheme tends to pass fraud losses on to the banks that issue the cards.[13] While this scheme insulates the individual cardholders from most of the major financial losses resulting from a data breach, it does nothing to compensate the cardholders for the time and money they must spend to monitor their credit, obtain replacement cards, cancel and reinstate recurring automatic payments, and repair their credit in cases in which the data was used to open new fraudulent accounts.

Consumers affected by data breaches understandably feel exposed to serious financial harm, even in the absence of liability for fraudulent charges. A consumer's credit score affects her ability to finance important purchases, and the events that occur in the aftermath of a data breach can negatively affect that score.[14] Because their losses are not addressed by existing privacy and payment system statutes, consumers have attempted to recover them using various common law theories; such theories, however, have uniformly failed to provide them any meaningful recovery for these losses.[15] In this Article, I will discuss cases in which consumers have been denied recovery for losses arising out of data breaches. I then focus on a novel argument made by the plaintiffs in the *Hannaford* case. The *Hannaford* plaintiffs argued that Article 2 of the Uniform Commercial

---

10. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

11. *See, e.g.*, IND. CODE §§ 24-4.9-1-1–9-5-1 (West 2009); MASS. GEN. LAWS ANN. ch. 93H, §§ 1–6 (West 2010); N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2010). As of April 2010, "46 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands had enacted legislation requiring notice to individuals of security breaches involving personal information." *See* State Security Breach Notification Laws, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last visited Sept. 21, 2010). Several attempts to pass a federal data breach notification law have failed. *See* Donald G. Aplin, *Network Security: Carper, Bennett Reintroduce Bipartisan Financial Data Security, Breach Notice Bill*, BNA: ELECTRONIC COMM. & L. REP., July 21, 2010, http://news.bna.com/epln (search "Donald G. Aplin"; then follow "7/19/2010" hyperlink).

12. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007) (stressing that the Indiana data breach notification statute grants enforcement authority only to the Attorney General).

13. *See generally* Truth in Lending Act of 1968 §§ 102–87, 15 U.S.C. §§ 1601–1667f (2006); Electronic Fund Transfer Act of 1978 § 902, 15 U.S.C. §§ 1693–1693r (2006).

14. Gail Hillebrand, *After the FACTA: State Power to Prevent Identity Theft*, 17 LOY. CONSUMER L. REV. 53, 55–57 (2004).

15. *See* discussion *infra* Part II.

Code (UCC) should provide a remedy to individuals harmed by a data breach because every time a retailer accepts a payment card from a buyer, it warrants that its payment system is secure.[16]

While a warranty of data security might be a good idea, Article 2 is not the best place for it because of its limitation to sales of goods. Instead, courts could impose a common law warranty of data security, under which all sellers would warrant that their chosen payment system is secure. In this Article, I will propose a non-waivable common-law warranty of data security that is drawn from both Article 2 warranties and the warranties provided in Articles 3 and 4 of the UCC which apply to negotiable instruments and the check collection system.[17] I will then compare the problem of ensuring safe data transactions today to the problem of ensuring the habitability of rental housing in the mid-20th century, which judges addressed by imposing an implied warranty of habitability in leases for residential real property.[18] The story of that warranty can add to the discussion about how best to ensure the safety of personal financial data.[19]

To develop my argument, in Part I, I will describe the mechanics of a data breach. In Part II, I will focus on the case law to discuss the difficulties that consumers face in recovering their data breach losses. I discuss various UCC warranties in Part III, and in Part IV, I analogize today's data security problems to the problems of scarce habitable rental housing in the mid-twentieth century and suggest that today's courts should protect personal financial data by imposing a warranty modeled in part on the warranty of habitability developed by courts in the 1970s. I conclude by calling on courts to develop a common-law warranty to compensate individuals harmed by data breaches.

I. ANATOMY OF A DATA BREACH

A payment card transaction involves four parties—the card issuer, the customer, the merchant, and the merchant bank—each of which is in control of payment data at some point in the transaction.[20] The role of merchant bank is complicated because a merchant bank may itself act as acquirer or processor, or it may sponsor access to the payment card network

16. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 118 (D. Me. 2009).

17. U.C.C. §§ 3-416, 3-417, 4-207, 4-208 (2002).

18. *See* discussion *infra* Part IV.

19. Modern data collection practices provide legal scholars with an excellent opportunity to analogize privacy regulation to the regulations of past social problems. *See generally* James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793 (2010). One possible analogy is to product safety regulation. *Id.* at 813.

20. Julia S. Cheney, *Heartland Payment Systems: Lessons Learned from a Data Breach* 1 (Payments Cards Center, Fed. Reserve Bank of Phila., Discussion Paper No. 10-1, 2010), *available at* http://ssrn.com/abstract=1540143.

for its partner transaction processor.[21] Some data breaches, such as the TJ Maxx data breach, involved data in the merchant's control.[22] Others, such as the Heartland Payment Systems (Heartland) breach, involved data in the processor's control.[23] In some cases, it is difficult to determine the identity of the party at fault for the breach, and as a result, the retailer and its payment processor are often both named as defendants in data breach suits.[24]

The TJ Maxx breach, which was discovered by the company in December 2006, involved customer data held in the company's computer systems.[25] In a Securities and Exchange Commission filing, the company claimed that the data thieves, using software they placed in the company's systems without authorization, captured both unencrypted and encrypted data.[26] The company reported in its filing that it believed that the hackers had access to the decryption tool for the encryption software used by TJ Maxx.[27] According to one news report on the breach, this decryption tool could have been acquired by an insider who participated in the data theft or by a successful entry into the TJ Maxx database where the decryption keys were held.[28]

The Heartland and Hannaford breaches were different from prior attacks in that the hackers focused not on data stored in a consumer database, but on data as it moved from the stores to the credit card processors.[29] In late 2007, fraudsters breached Heartland's system by a method known as SQL injection,[30] which allowed them to exploit a

---

21. *Id.* at 1–2.

22. *See* TJX Co., Annual Report (Form 10-K), at 7 (Mar. 28, 2007), *available at* http://ir.10kwizard.com/files.php?source=487&page=14&ext=1 (reporting that TJX had suffered "an unauthorized intrusion into portions of [its] computer system").

23. Cheney, *supra* note 20, at 3.

24. *See, e.g.*, Amerifirst Bank v. TJX Co., Inc., 564 F.3d 489, 491–92 (1st Cir. 2009) (naming both the retailer and its processing bank as defendants, alleging that they both "failed to follow security protocols prescribed by Visa and MasterCard").

25. *See* TJX Co., Annual Report, *supra* note 22, at 7.

26. *Id*. at 9.

27. *See id*.

28. Larry Greenemeier, *T.J. Maxx Parent Company Data Theft is the Worst Ever*, INFORMATIONWEEK.COM (Mar. 29, 2007), http://www.informationweek.com/news/security/showArticle.jhtml?articleID=198701100.

29. *See* Linda McGlasson, *Hannaford Data Breach May Be 'Tip of Iceberg'*, BANK INFO SECURITY (Apr. 4, 2008), http://www.bankinfosecurity.com/articles.php?art_id=810 (quoting a security expert who described the Hannaford incident as "highly significant because it represents the first publicly-acknowledged theft of sensitive card authorization data in transit"); *see also* Cheney, *supra* note 20, at 3.

30. SQL stands for "structured query language," which is defined as "a standardized language for defining and manipulating data in a relational database." IBM, SQL REFERENCE VOLUME 1, 1 (2006), *available at* ftp://public.dhe.ibm.com/ps/products/db2/info/vr9/pdf/letter/en_US/db2s1e90.pdf. For a good explanation of how SQL works and a detailed description of some of the high-profile data breaches mentioned in this article, see generally James Verini, *The Hacker Who Went Into the Cold*, N.Y. TIMES MAG., Nov. 14, 2010, at 44.

vulnerability in Heartland's corporate and payment processing networks.[31] They then installed software that captured payment card data as it moved through Heartland's system.[32] In early 2008, Hannaford discovered that hackers had placed malicious software on their servers to capture payment card information.[33] The software picked up credit card numbers and expiration dates as they traveled through the system and sent that information to overseas servers.[34]

It is important to note that the Payment Cards Industry Standards Council, founded by the five payment card networks, manages a set of security standards (known collectively as the Payment Card Industry Data Security Standard, or PCI DSS)[35] with which all merchants and processors must comply in order to participate in the card payment systems.[36] While TJ Maxx had not fully complied with the PCI DSS standards,[37] Heartland had been certified as compliant at the time its system was breached.[38] PCI DSS is not seen as the "gold standard" in data security, however, and most companies do more to protect their data than is required by PCI DSS.[39]

The amount of data compromised in these breaches can be staggering. The Hannaford data breach resulted in the theft of 4.2 million credit and debit card numbers and related information such as PIN codes.[40] The DSW Shoe Warehouse breach involved more than 1.4 million credit and debit card numbers and almost 100,000 checking account numbers and driver's license numbers.[41] The BJ's Wholesale Club breach allowed "unauthorized parties [to gain] access to magnetic stripe data from 9.2 million credit cards."[42] The TJ Maxx breach was one of the largest, with 94 million compromised records, according to one estimate.[43] The largest breach to date was the Heartland breach, which affected about 130 million credit and

---

31. Cheney, *supra* note 20, at 3.

32. *Id.*

33. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 116 (D. Me. 2009).

34. McGlasson, *supra* note 29.

35. *About the PCI Data Security Standard (PCI DSS)*, PCI SECURITY STANDARDS COUNCIL, http://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited Oct. 26, 2010).

36. *Id.*

37. Bill Brenner, *TJX Security Breach Tied to Wi-Fi Exploits*, COMPUTERWEEKLY.COM (May 8, 2007), http://www.computerweekly.com/Articles/2008/08/08/223672/TJX-security-breach-tied-to-Wi-Fi-exploits.htm.

38. *See* Cheney, *supra* note 20, at 4.

39. *See id.* (discussing the observations of Bob Carr, the CEO of Heartland Payment Systems).

40. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 116 (D. Me. 2009).

41. Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 777 (W.D. Mich. 2006).

42. Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E.2d 36, 39 (Mass. 2009).

43. *See Data Security Breaches Reach a Record in 2007*, WALL ST. J., Dec. 31, 2007, at B5 (reporting that while the company acknowledged that 46 million records were compromised, Visa and MasterCard estimated that 94 million TJ Maxx records were compromised).

debit cards.[44] These breaches have exposed the personal financial data of millions of individuals, giving unauthorized parties the ability to enter into fraudulent payment card transactions. The data thief is often hard to find, so the data breach victims seek recovery from the company to whom they entrusted their information by making a payment.[45] Although consumers are protected from liability for the fraudulent transactions themselves, they have had almost no success recovering other costs arising from these breaches.[46]

II. THWARTED ATTEMPTS TO RECOVER FOR DATA THEFT

Rules governing both credit cards and debit cards protect consumers from most of the liability for fraudulent charges. The Truth in Lending Act limits the liability of a consumer for unauthorized use of her credit card to $50[47] and many credit card issuers promise no liability to cardholders if the cardholder notifies the issuer immediately after the card was lost or stolen.[48] The Electronic Funds Transfer Act contains a $50 liability limitation for the unauthorized use of a debit card, but the consumer can be liable for a greater amount if she fails to report the loss of her card within a prescribed amount of time.[49] Yet data breaches cause consumers to suffer a wide range of other financial and non-financial harms.

Consumer plaintiffs in data breach cases have alleged a variety of harms. Although they ultimately incur little to no liability for unauthorized charges, consumer victims of a data breach spend time and money to address and resolve their financial disruptions.[50] For example, an individual whose personal information has been compromised as a result of a data breach often feels the need to pay to monitor her credit[51] because an unauthorized party might use the stolen data to assume the affected individual's identity and obtain credit or other benefits fraudulently in that

---

44. Linda McGlasson, *Heartland Breach: Consumer Settlement Proposed*, BANK INFO SECURITY (May 6, 2010), http://www.bankinfosecurity.com/articles.php?art_id=2498.

45. *See, e.g.*, *In re Hannaford Bros. Co.*, 613 F. Supp. 2d at 114; *Hendricks*, 444 F. Supp. 2d at 776; Settlement Agreement, *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig. (S. D. Tex. 2009) (No. 4:09-MD-2-46), *available at* http://www.hpscardholdersettlement.com/Documents/Settlement%20Agreement.pdf [hereinafter Heartland Settlement Agreement].

46. *See* discussion *infra* Part II.

47. Truth in Lending Act of 1968 § 133, 15 U.S.C. § 1643 (a) (1) (2006).

48. *See* Mastercard Zero Liability: Zero Liability Protection for Lost & Stolen Cards, MASTERCARD, http://www.mastercard.com/us/personal/en/cardholderservices/zeroliability.html (last visited Aug. 27, 2010); Visa Zero Liability, VISA, http://usa.visa.com/personal/security/visa_security_program/zero_liability.html (last visited Aug. 27, 2010).

49. Electronic Fund Transfer Act of 1978 § 909, 15 U.S.C. § 1693g (2006).

50. *In re Hannaford Bros. Co.,* 613 F. Supp. 2d at 116.

51. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631 (7th Cir. 2007); *In re Hannaford Bros. Co.*, 613 F. Supp. 2d at 116; Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 777 (W.D. Mich. 2006); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1019 (D. Minn. 2006).

person's name.[52] If that individual finds unauthorized payments or charges on her bank and credit card statements, she must take the time to contest the fraudulent charges. As a result, many victims of a data breach seek compensation for credit monitoring costs.[53] The *Hannaford* plaintiffs alleged a comprehensive list of harms, which covered almost everything that can happen when the security of a credit or debit card is compromised.[54] Some customers were deprived of the use of their cards because their bank accounts were overdrawn and their credit limits were exceeded.[55] Customers also lost bonus points on their cards for the period of time when their cards were cancelled.[56] Some banks required customers to pay for replacement cards.[57] Customers were also forced to spend time dealing with pre-authorized charges because they had to give new credit card numbers to the payees to whom the pre-authorized payments were made.[58] When a consumer's pre-authorized payments cannot be made because the credit card on file is not valid, the consumer incurs additional charges such as late fees. Therefore, the *Hannaford* plaintiffs also claimed damages for the disruption of their pre-authorized charge relationships.[59]

Courts have rejected consumer attempts to recover these costs. Most courts have found that the harms caused by the exposure of personal financial information are too speculative to form the basis for a claim for damages in either contract or tort law.[60] In *Pisciotta v. Old National Bancorp,* the plaintiffs sought compensation, under a negligence theory, for both the credit monitoring services they were forced to obtain and for the emotional distress that they suffered after their personal financial information was taken from the defendant bank's Web site.[61] In order to recover on their negligence claim, the plaintiffs were required to show that they suffered "a compensable injury proximately caused by [the bank's] breach of duty."[62] To show that they had suffered a compensable harm, the plaintiffs pointed to the Indiana data breach notification statute, arguing that the Indiana legislature, by enacting such a statute, agreed that consumers suffer compensable harm at the moment their personal financial information

---

52. *See* Heartland Settlement Agreement, *supra* note 45, at 12–13.

53. *See, e.g.*, *Pisciotta*, 499 F.3d at 631; *In re Hannaford Bros. Co.*, 613 F. Supp. 2d at 116; *Forbes*, 420 F. Supp. 2d at 1020.

54. *In re Hannaford Bros. Co*., 613 F. Supp. 2d at 116.

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 779–81 (W.D. Mich. 2006).

61. *Pisciotta*, 499 F.3d at 631–32.

62. *Id.* at 635 (emphasis omitted) (quoting Bader v. Johnson, 732 N.E.2d 1212, 1216–17 (Ind. 2000)).

is compromised by a data breach.[63] The court rejected this argument, noting the absence of any statement by the legislature that it intended to allow such a recovery.[64]

The plaintiffs in *Forbes v. Wells Fargo* were also denied recovery for credit monitoring costs.[65] In that case, the plaintiffs sued Wells Fargo for both negligence and breach of contract when their financial information was stolen from a Wells Fargo service provider.[66] The court rejected the plaintiffs' arguments, holding that credit monitoring expenses were not incurred because of any present injury, but were rather incurred to prevent future injury, stressing that the plaintiffs' injuries were "solely the result of a perceived risk of future harm."[67] The court denied the plaintiffs' breach of contract claims in *Hendricks v. DSW Shoe Warehouse* because the plaintiff did not prove that her personal information had been used in any way and therefore had suffered no cognizable loss.[68] The court characterized the plaintiffs' claim for credit monitoring costs as "damages to buy peace of mind."[69]

Although several plaintiffs have attempted to recover for their losses on a breach of contract theory, the *Hannaford* plaintiffs made a particularly novel contract argument. They argued that every time Hannaford accepted a payment card, it impliedly warranted that its payment system "was fit for its intended purpose, namely the safe and secure processing of credit and debit card payment transactions," and that this warranty was breached because the system "allowed wrongdoers to steal the customers' confidential personal and financial data."[70] This resembles the implied warranty of fitness for a particular purpose from Article 2 of the UCC.[71] The plaintiffs argued not that the Article 2 warranty applies by its terms to payment processing transactions, but that Article 2 "provides an 'analogue' on which [the] . . . court should draw in crafting a common law implied warranty to fit their situation."[72]

The court refused to imply such a warranty for several reasons, focusing on the requirements of Article 2.[73] In order for a warranty of fitness for a particular purpose to be implied in a contract of sale, the seller must have reason to know of two facts: the particular purpose for which the

---

63. *Id.* at 637.
64. *Id.*
65. *See* Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006).
66. *Id.* at 1020.
67. *Id.* at 1021.
68. Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 779–81 (W.D. Mich. 2006).
69. *Id.* at 780.
70. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 119–20 (D. Me. 2009) (quotations omitted).
71. U.C.C. § 2-315 (2002).
72. *In re Hannaford Bros. Co.*, 613 F. Supp. 2d at 120.
73. *Id.*

buyer requires the goods, and that the buyer is relying on the seller's skill or judgment in selecting or furnishing such goods.[74] The court emphasized that the warranty applies to goods sold, and the definition of goods does not include the payment system used to process the payment for the goods.[75] In addition, the implied warranty of fitness for a particular purpose is implied not when a buyer seeks goods for their ordinary purpose, but only when a buyer seeks goods for a purpose that is particular to that buyer's needs.[76] The court correctly observed that the buyers did not use the payment system for a particular purpose;[77] instead, they relied on it to process credit and debit card payments in the same way as did all other grocery purchasers.[78]

However, while Article 2 may not be the best place to locate a warranty or provide the best analogy, implying a warranty of data security in consumer payment transactions is a good idea. A better analogy might be the non-waivable implied warranty of habitability developed by courts in the early 1970s to respond to the societal changes wrought by urbanization.[79] As I will discuss in Part IV, some of the same concerns that drove the courts of forty years ago to protect consumers of urban rental housing exist today in the area of payment data security.[80]

An implied warranty of data security would allow consumers to recover their losses without overly straining established legal doctrines. Today, there are two major impediments to recovery for the losses that individuals incur as a result of a data breach. The first, applicable to both contract and tort actions, is that the damages are seen as too speculative.[81] Second, purely economic losses that are not coupled with personal injury or physical property damage are not recoverable in tort.[82] One justification for this doctrine is to allow parties to allocate their economic losses by contract.[83] In the consumer context, however, reliance on freedom of contract often fails to protect consumer welfare.[84] Because of this preference for freedom of contract, consumers appear doomed to absorb some costs of data breaches themselves. In order for an implied warranty of data security to truly protect

---

74. U.C.C. § 2-315 (2002).

75. *In re Hannaford Bros. Co.*, 613 F. Supp. 2d at 120.

76. U.C.C. § 2-315, cmt. 2.

77. *In re Hannaford Bros. Co*., 613 F. Supp. 2d at 120.

78. *Id.*

79. *See, e.g.*, Javins v. First Nat'l Realty Corp., 428 F.2d 1071, 1078 (D.C. Cir. 1970).

80. *See* discussion *infra* Part IV.

81. *See* cases cited *supra* note 60.

82. *In re Hannaford Bros. Co.*, 613 F. Supp. 2d at 127; JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE § 11-5, at 538–39 (6th ed. 2010); Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 470 (2008).

83. *See* WHITE & SUMMERS, *supra* note 82, § 11-5, at 541.

84. *See* Oren Bar-Gill & Elizabeth Warren, *Making Credit Safer*, 157 U. PA. L. REV. 1, 7–8 (2008) (arguing that markets for consumer credit function only when consumers are rational and informed).

consumers, it would have to be non-waivable. There is precedent for non-waivable warranties both in the UCC and the common law.[85] The remainder of this Article will discuss the various warranties that are implied in commercial transactions, and will propose that an implied warranty of data security be imposed on retailers.

III. EXISTING UCC WARRANTIES: CAN WE EXPAND THEM TO PROTECT DATA?

The proposed warranty of data security would be implied in all contracts between a seller accepting a payment card and the buyer using that card. The seller is the best person to give such a warranty because the seller is the party who deals with the consumer and is also the party that the consumer trusts to handle her payments safely. The seller would be warranting the safety of a transaction, not a product. Nevertheless, elements of several UCC warranties can be incorporated into an implied warranty of data security.

The UCC implies several warranties under Article 2, which governs sales of goods, and Articles 3 and 4, which govern some aspects of the payment system.[86] The persons giving these warranties represent that a product,[87] a transaction,[88] or both[89] meet certain quality and reliability requirements. Parties to a transaction can waive some,[90] but not all,[91] of these warranties. Although a payment card transaction falls strictly outside of the UCC's scope—and therefore a warranty protecting it could not find a home in the UCC—an implied warranty of data security could draw on and combine elements of several of these warranties. In the remainder of this section, I will discuss the elements of the UCC warranties that should be included in a warranty of data security and argue that a warranty approach to the data breach problem has several advantages over a tort approach.

A. UCC PRODUCT WARRANTIES

Under the implied warranties of merchantability[92] and fitness for a particular purpose,[93] a seller in a transaction governed by Article 2 promises that goods sold meet some standard of quality (in the case of

85. *See*, *e.g.*, Javins v. First Nat'l Realty Corp., 428 F.2d 1071, 1081–82 (D.C. Cir. 1970) (holding that the implied warranty of habitability is non-waivable); U.C.C. § 3-417(e) (2003) (providing that the Article 3 presentment warranty cannot be waived with respect to checks).

86. *See generally* U.C.C. §§ 2-312–317, 2-321, 3-318, 3-415–416, 4-207–209 (2002).

87. *See infra* notes 93–123 and accompanying text.

88. *See infra* notes 125–134 and accompanying text.

89. *See infra* notes 135–137 and accompanying text.

90. U.C.C. § 2-316 (2002) (setting forth the requirements for Article 2 warranty disclaimers).

91. *See, e.g.*, U.C.C. § 3-417(e) (2003) (providing that the Article 3 presentment warranty cannot be disclaimed with respect to checks).

92. U.C.C. § 2-314 (2002).

93. *Id.* § 2-315.

merchantability) or of suitability (in the case of fitness for a particular purpose). A seller in a payment card transaction is providing two different things: the product or service sold, and the system that processes the payment.

A discussion of an argument that the *Hannaford* plaintiffs could have but failed to make illustrates some of the advantages and disadvantages in using Article 2 of the UCC to protect payment card data. Rather than asking the court to apply the Article 2 warranties by analogy, the *Hannaford* plaintiffs could have argued that the payment system software itself breached the warranty of merchantability that is implied, unless excluded, in all contracts covered by Article 2.[94] Most courts have held that the transfer of software is a sale of goods for the purpose of Article 2.[95] However, the software warranty in a payment card transaction would first run from the payment software vendor to the retailer, leaving the plaintiffs with a privity barrier, one that I will explain below.

An examination of this hypothetical argument highlights some of the benefits that an implied warranty might give consumers in payment card transactions and also illustrates the impediments that consumers would face in relying on existing warranties. First, the warranty of merchantability is implied in all contracts for the sale of goods in which the seller is a merchant.[96] The UCC defines a merchant as "a person who deals in goods of the kind or otherwise by his occupation holds himself out as having knowledge or skill peculiar to the practices or goods involved in the transaction."[97] All merchants give this warranty because they, as merchant sellers, hold themselves out as having special knowledge with respect to the products sold.[98] A buyer need not show that he relied on any representations made by the seller in order to recover for breach of warranty.[99] Because the warranty of merchantability is implied, unless excluded, in all transactions in which goods are sold by a merchant, it is curious that the *Hannaford* plaintiffs did not try to claim damages for its breach.[100]

The application to all merchant seller transactions is one element of the warranty of merchantability that should be incorporated into a warranty of data security. For this purpose, a merchant can be defined as anyone who

94. *Id.*

95. Scott, *supra* note 82, at 436 (discussing judicial classification of software).

96. U.C.C. § 2-314.

97. *Id.* § 2-104(1).

98. WHITE & SUMMERS, *supra* note 82, § 10-11, at 482 (tracing the logic behind the warranty of merchantability to the pre-Code warranty implied in transactions with manufacturers).

99. *Id.*

100. According to the two leading commentators on the UCC, a key reason that a transferee might seek to classify its transaction as a purchase of goods is to receive the benefit of Article 2's warranty of merchantability. *See* WHITE & SUMMERS, *supra* note 82, § 10-2, at 449.

accepts a payment card for goods or services.[101] Merchant sellers choose the persons responsible for handling the data that they collect,[102] so imposing a warranty on these sellers would force them to choose their payment processors carefully and to negotiate indemnification clauses with those processors.

To satisfy the implied warranty of merchantability, the seller must provide goods that "are fit for the ordinary purposes for which [they] are used"[103] and that "pass without objection in the trade under the contract description."[104] A merchant who provides customers with the convenience of using a card payment system should be deemed to represent that its payment system is fit for the ordinary purpose for which a payment system is used—the safe and secure processing of a purchaser's payment data. One of the reasons the plaintiffs' warranty argument failed in the *Hannaford* case was that the plaintiffs had chosen to argue for a warranty of fitness for a particular purpose despite the fact that the payment system was actually being used for its ordinary purpose.[105] An argument that the payment system in the transaction was not fit for its *ordinary* purposes might have fared better.

There are two major intertwined problems with arguing that an individual victim of a data breach can recover from the provider of payment software under the implied warranty of merchantability. First, the implied warranty of merchantability can be disclaimed in the contract between the buyer and seller.[106] Sellers of goods tend not to disclaim this warranty altogether, choosing instead to limit the damages recoverable because concerns for future business force attention to quality.[107]

One reason that suing the payment system software vendors is undesirable is that the problem of warranty disclaimers is magnified when the product transferred is software. The tumultuous drafting history of Article 2B of the UCC (which became the Uniform Computer Information

---

101. Individuals making isolated sales could be exempted from this definition. U.C.C. § 2-314 cmt. 3 (2002) (exempting a person making an isolated sale from the Article 2 implied warranty of merchantability). These individuals do not participate in the payment system by choosing from a variety of payment processors; if they do accept payment cards, they do so through person-to-person payment systems such as PayPal. *See* PAYPAL, https://www.paypal.com (select "personal" tab; then select "get paid" from top bar; then select "accept credit cards" from drop-down list) (last visited Oct. 9, 2010) (explaining how individuals can accept payment cards through PayPal from persons who do not have PayPal accounts).

102. Businesses can choose among many payment processing service companies. *See, e.g.*, ACH PAYMENTS, http://www.ach-payments.com (last visited Dec. 18, 2010); ELIOT MANAGEMENT GROUP, http://www.e-mg.com (last visited Dec. 18, 2010); HEARTLAND PAYMENT SYSTEMS, http://www.heartlandpaymentsystems.com (last visited Dec. 18, 2010).

103. U.C.C. § 2-314(2)(c).

104. *Id.* § 2-314(2)(a).

105. *See In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 120 (D. Me. 2009).

106. *See* U.C.C. § 2-316(2) (2002).

107. DANIEL KEATING, SALES: A SYSTEMS APPROACH 151 (4th ed. 2009).

Transactions Act after the American Law Institute withdrew from the project) shows how averse software vendors are to Article 2 warranty liability.[108] Software vendors almost universally disclaim the warranty of merchantability because vendors contend that "[c]omputer software has peculiar qualities" that render a comparison among software programs senseless.[109] Such a comparison is necessary in order to determine that software would "pass without objection in the trade under the contract description," for the purpose of the warranty of merchantability.[110]

Second, even in the unlikely absence of a disclaimer, the aggrieved individuals would have difficulty recovering for a breach of warranty because they never buy or take a transfer of the payment processing software.[111] Because warranty liability is based on contract law, the general rule is that a warrantor is directly liable only to the person with whom it has a contract.[112] The harsh effects of this general rule have been ameliorated in the sale of goods area, and today, most manufacturer warranties run to the ultimate buyer for two reasons. First, most states have eliminated the vertical privity requirement by common law when a consumer is personally injured by a manufacturer's product.[113] Second, most manufacturers, for reasons of reputation, treat their warranties as though they run to the ultimate purchaser.[114]

This erosion of the privity barrier would not assist a consumer harmed by a data breach, however. Although Article 2 of the UCC allows non-buyers affected by a product to sue for breach of warranty, most states, in their versions of Article 2, deny a cause of action to a third party non-buyer in the absence of personal injury.[115] A person whose payment card data has been stolen has not suffered any personal injury. In states that have adopted the third alternative to § 2-318, a third party has a cause of action against

---

108. *See generally* Peter A. Alces, *W(h)ither Warranty: The B(l)oom of Products Liability Theory in Cases of Deficient Software Design*, 87 CALIF. L. REV. 269 (1999) (discussing the Article 2B drafting process).

109. Robert Gomulkiewicz, *The Implied Warranty of Merchantability in Software Contracts: A Warranty No One Dares to Give and How to Change That*, 16 J. MARSHALL J. COMPUTER & INFO. L. 393, 398–99 (1997); Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1150 (2009) (quoting Scott, *supra* note 82, at 426) (explaining that "software vendors have traditionally . . . used various risk allocation provisions of [the U.C.C.] to shift the risk of insecure software to the licensee").

110. *See* U.C.C. § 2-314 (2) (2002); Gomulkiewicz, *supra* note 109 (explaining that, as essentially diverse collections of ideas that cannot reasonably be compared to one another, attempts to identify minimum quality standards for software products would be difficult and unfair).

111. *See In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 121 (D. Me. 2009); *see also* Cheney, *supra* note 20, at 1–2 (describing a credit card transaction).

112. *See* U.C.C. §§ 2-313–315 (2000); *see also* Metro. Coal Co. v. Howard, 155 F.2d 780, 784 (2d Cir. 1946) ("A warranty is an assurance by one party to a contract of the existence of a fact upon which the other party may rely.").

113. KEATING, *supra* note 107, at 178–79.

114. *Id.* at 178.

115. *See* WHITE & SUMMERS, *supra* note 82, § 12-3, at 546.

the seller if it is "injured" by the breach of warranty.[116] This alternative would seem to allow someone harmed by payment processing software to recover. In these states, however, a seller can disclaim the warranty as to third parties who did not suffer personal injury as a result of the breach of warranty.[117]

The foregoing discussion illustrates the hurdles that a consumer would face in attempting to recover damages from a payment software vendor for breach of the Article 2 implied warranty of merchantability. Although imposition of the Article 2 implied warranty of merchantability to payment transactions is not feasible, the policies underlying the warranty are particularly salient to today's electronic payment transactions. Before the mass production of goods, buyers were bound by *caveat emptor* and no warranties were implied.[118] The old law was based on a system in which traders were neighbors.[119] *Caveat emptor* was considered just in face-to-face transactions in which the seller and buyer had roughly equal commercial experience and the buyer had ample opportunity to inspect the goods he was buying.[120] Over the course of the last century, courts and legislatures have chipped away at the doctrine, recognizing the inequality of knowledge and bargaining power between buyers and sellers.[121] As mass production of goods proliferated, warranties were imposed on professional sellers.[122] The move away from *caveat emptor* was slower in real estate law, as mass production of housing did not emerge until after World War II.[123]

Caveat emptor has no place in card payment transactions. Payment processing transactions are completely invisible to consumers. The clerk at my local grocery store will ask me whether I want to use my Visa debit card (which is not a credit card) as a "debit or credit" card, having no idea that she is asking me which payment network (the Visa network or the PIN-based debit card network) I want to use.[124]

B. UCC TRANSACTION WARRANTIES

The discussion above analogizes a warranty of data security to a warranty of product quality. The UCC imposes transaction warranties as well,[125] and a data security warranty might be better analogized to such a

116. U.C.C. § 2-318 (2003).
117. *Id.* § 2-318 cmt. 2.
118. *See* Timothy J. Sullivan, *Innovation in the Law of Warranty: The Burden of Reform*, 32 HASTINGS L.J. 341, 356 (1980).
119. *See* Allison Dunham, *Vendor's Obligation as to Fitness of Land for a Particular Purpose*, 37 MINN. L. REV. 108, 110 (1952).
120. *See* Sullivan, *supra* note 118, at 356.
121. *Id.*
122. *See id.* at 356–57.
123. *See* Dunham, *supra* note 119, at 111.
124. I would not know that either had I not taught Payment Systems for a number of years.
125. *See, e.g.*, U.C.C. § 2-312 (2002).

warranty. These transaction warranties also contain elements that a court could incorporate in an implied warranty of data security. Unlike the warranty of merchantability, the implied warranty of title helps to ensure the quality of the transaction in which the goods are transferred.[126] Therefore, a seller giving a warranty of title promises that the transaction is reliable.[127] Under Article 2, all sellers give a warranty that title to the goods "shall be good and its transfer rightful."[128] This warranty has nothing to do with the quality of the product, rather it relates to the transactions in which the goods reach the seller. If there is a thief in the chain of title, the seller breaches the warranty.[129] The UCC permits a seller to disclaim this warranty, but any disclaimer must clearly indicate that the seller claims no title in the goods sold.[130]

The purpose behind this warranty is to ensure that the buyer will not be exposed to litigation in order to protect its title to the goods because of defects in purchase transactions in his chain of title.[131] Although the implied warranty of title looks backwards, holding the seller liable for the wrongdoing of persons in the past, its basic purpose, to protect the buyer from transaction defects, could be used as a basis for an implied warranty of data security. A data security warranty would necessarily be forward-looking, but it would also serve to guarantee the quality of a chain of transactions, rather than a product. A warranty of data security can ensure that someone who uses a payment card will not be forced to incur costs to protect her personal information from misuse in the chain of transfers comprising a payment transaction.

The warranty of title imposes strict liability on the seller.[132] Under UCC § 2-312, a seller is not protected from liability on the warranty of title by his lack of knowledge that the title conveyed is not good.[133] A thief of goods breaks the chain of title, so the warranty of title functions to pass the risk that the transaction is not good to the person who dealt most closely with the thief.[134] The result is to place the loss on the person best situated to avoid it. Using the same logic, a seller who takes a payment card is best situated to guard against unsafe payment transactions, and if it enters into an unsafe payment transaction with a consumer, it should bear the loss regardless of its knowledge that the transaction may be unsafe.

In the payment system, as in the sales system, warranties play an important loss allocation function. Payment warranties pass the risk of fraud

126. *Id.*
127. *Id.* § 2-312(1)(a).
128. *Id.* § 2-312.
129. *See* West v. Roberts, 143 P.3d 1037, 1045 (Colo. 2006).
130. U.C.C. § 2-312(3).
131. *Id.* § 2-312(1) cmt. 1.
132. *Id.* § 2-312.
133. KEATING, *supra* note 107, at 279.
134. *See id.* at 279–80.

to the person closest to the fraud. When a bank pays the wrong person by honoring a check bearing a forged endorsement, it must re-credit its customer's account.[135] The warranties under Article 4 of the UCC then allow the bank to seek compensation from persons up the collection stream.[136] However, unlike most warrantors in the sales system, those giving payment warranties vouch for both the transaction and the product. The warrantor of a negotiable instrument vouches for the product (the negotiable instrument) in that it warrants that "the instrument has not been altered" and that "all signatures . . . are authentic and authorized," but it also vouches for the transaction in that it warrants that it is "entitled to enforce the instrument" and that "the instrument is not subject to a defense or claim in recoupment by any party."[137]

In order to effectively protect personal financial information, the implied warranty of data security should be non-waivable. There is precedent in the UCC for a non-waivable warranty. The warranties in Articles 3 and 4 of the UCC cannot be disclaimed with respect to checks.[138] This prohibition of disclaimers protects the checking system; checks are collected and paid by automated means, so banks rely on the warranties for their protection.[139]

Warranty is a good theory on which to give a remedy to injured consumers. Privity remains an issue in imposing a warranty of data security on data controllers. Privity is not a problem when the merchant itself is responsible for the breach, because that merchant will always have a contract with the aggrieved purchaser. Lack of privity, however, should not bar recovery from the payment processors. All consumers entering the payment system through a merchant, however, have a contract with that merchant.[140] Therefore, imposing a warranty on that merchant makes sense; that merchant must then either make sure that it protects the data, or negotiate an agreement with its processor that the processor will protect the data and indemnify the merchant from any losses as a result of a data breach. The retailer is in the best position to know whether its processor

---

135. *See* WHITE & SUMMERS, *supra* note 82, § 16-3, at 754.

136. *See id.*

137. U.C.C. § 3-416 (2002) (setting forth transfer warranties); *id.* § 3-417 (setting forth presentment warranties, which do not include a warranty that there are no defenses or claims in recoupment to the instrument); *id.* § 4-207 (setting forth transfer warranties in the check collection system); *id.* § 4-208 (setting forth presentment warranties in the check collection system, which also do not include the warranty that there are no defenses or claims in recoupment).

138. *See id.* §§ 3-416(c), 3-417(e), 4-207(d), 4-208(e).

139. *See id.* § 3-417 cmt. 7.

140. Consumers use the payment system for several reasons: to purchase goods, services, and information, and to make loan payments. In all of these transactions, there is some contract between the consumer and the merchant. *See, e.g.*, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 118 (D. Me. 2009) ("Both sides agree that at the point of sale—the cash register—there is a contract for the sale of groceries.").

handles data safely, and can choose to use a more secure system if the processor will not cover losses from data breaches.

Contract law, unlike tort law, allows recovery for purely economic loss. A buyer aggrieved by a breach of the warranty of merchantability can recover the difference in value between the goods accepted and the goods as warranted.[141] This difference can be measured by the cost of repair.[142] The damages claimed by consumer plaintiffs in data breach cases are in essence claims for the cost of repair to their credit profile, because a consumer who must pay for card replacement or credit monitoring is trying to restore the data to the condition it was in before the breach. Recognizing this type of remedy would eliminate one of the major hurdles to protecting data security through tort law—the limitations on economic loss damages.

Some have suggested treating privacy concerns in a manner analogous to product safety.[143] Although both tort law and contract law have a role in ensuring product safety, those who urge a product safety approach to privacy have focused primarily on tort law.[144] Some have proposed a tort action based on strict products liability for data breaches;[145] products liability law, however, does not often grant recovery for economic loss.[146] While some have argued that new technology begs a redefinition of injury,[147] a warranty approach would not force courts to strain existing tort doctrine in that way. Every transaction in which payment data is passed is a contract transaction, either for goods, information, or services. Therefore, a contract will always exist into which a warranty of data security could be implied. The tendency of courts to rule that one party to a contract cannot sue the other party for negligence might make such an implied warranty preferable to a tort action.[148]

There is no doubt that consumers are harmed by unauthorized uses of their personal financial data even in the absence of liability for the

---

141. U.C.C. § 2-714(2) (2002). A buyer can also recover incidental and consequential damages. *Id.* § 2-714(3).

142. *See* WHITE & SUMMERS, *supra* note 82, § 11-2, at 518.

143. *See generally* Grimmelmann, *supra* note 19.

144. *See id.* at 814–17 (discussing several scholars' approaches to protecting personal information using a product safety analogy).

145. *See, e.g.*, Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 296 (2007); Scott, *supra* note 82, at 470 (identifying the economic loss rule as "[t]he most significant impediment to the use of strict product liability law to recover damages caused by insecure software").

146. *See* James J. White, *Reverberations from the Collision of Tort and Warranty*, 53 S.C. L. REV. 1067, 1068 (2002) ("loss that is solely 'economic' may be recovered in warranty but not in tort") (citing Rich Prods. Corp. v. Kemutec Inc., 241 F.3d 915, 918 (7th Cir. 2001); Calloway v. City of Reno, 993 P.2d 1259, 1264 (Nev. 2000); Steiner v. Ford Motor Co., 606 N.W.2d 881, 884 (N.D. 2000)). Courts have rejected this cause of action in data breach cases. *See, e.g.*, Amerifirst Bank v. TJX Co., Inc., 564 F.3d 489, 498 (1st Cir. 2009).

147. *See, e.g.*, Citron, *supra* note 145, at 295–96.

148. *See* Scott, *supra* note 82, at 456 (discussing tendency of courts to deny plaintiffs' negligence claims when those plaintiffs are parties to contracts with their defendants).

fraudulent charges made to their accounts. Although a warranty of data security is desirable, data security does not fit neatly into the existing UCC warranties for several reasons. First, the articles in the UCC are organized by type of transaction. Even if a warranty regarding goods could be stretched to include the payment system used to purchase the goods, many payment transactions do not involve goods. The payment system contains numerous warranties, but these warranties—designed to place the risk of fraud in checking and other negotiable instrument transactions on the person closest to the fraud—do nothing to compensate an individual who is harmed by identity theft. Revising the UCC to include data security within the Article 2 warranties is probably politically unfeasible[149] and in addition, an Article 2 warranty would not give any recovery to those whose data was taken in a sale of services transaction.

IV. THE IMPLIED WARRANTY OF HABITABILITY: A GOOD ANALOGY?

To adequately protect consumers, any warranty of data security should be implied in all payment card transactions between an individual and a merchant and should be non-waivable. The use of payment cards to pay for almost everything has allowed sellers and payment processors to collect tremendous amounts of personal financial information. Havoc ensues when this information falls into the wrong hands. The changes in the conduct of business wrought by the electronic processing of payments beg a judicially-created remedy tailored to the emerging and serious problem of data theft. One can find precedent for such a remedy in landlord-tenant law. In this section, I will apply lessons from landlord-tenant law to the protection of payment card data.

Real property law provides some precedent for judge-made, non-waivable warranties to protect consumers. One that exists today—either by statute or case law in nearly every state and the District of Columbia—is the warranty of habitability implied in leases for residential real property.[150] This warranty that a dwelling be safe, clean, and fit for human habitation cannot be waived in a lease.[151]

---

149. The goal of the UCC's sponsoring bodies, the American Law Institute and the National Conference of Commissioners on Uniform State Laws, is to draft a uniform law that can be enacted in all U.S. jurisdictions**.** *See* Edward J. Janger, *Predicting When the Uniform Law Process Will Fail: Article 9, Capture, and the Race to the Bottom*, 83 IOWA L. REV. 569, 571 n. 8 (1998). For an excellent discussion of political pressures in the uniform law drafting process, see *id.* at 582–93.

150. *See* Michael Madison, *The Real Properties of Contract Law*, 82 B.U. L. REV. 405, 417 (2002).

151. Hilder v. St. Peter, 478 A.2d 202, 208 (Vt. 1984). Another implied real estate warranty is the warranty of workmanlike quality that is given from the builder to the buyer of a newly-constructed home; this is also a consumer-protective warranty. Lempke v. Dagenais, 547 A.2d 290, 294 (N.H. 1988). The warranty of workmanlike quality is given only by builders of new

The initial judicial imposition of this warranty recognized the modernization of the landlord-tenant relationship. When the common law landlord-tenant rules first developed, the typical lessee was more interested in the land than the dwelling and was expected to make repairs to the dwelling himself.[152] The modern urban tenant is interested solely in a habitable dwelling, and has neither the ability nor economic incentive to make repairs to the dwelling because his lease is often for a fairly short term.[153] Courts relied on consumer protection concepts to imply a warranty of habitability in all residential leases because tenants, particularly poor urban tenants, had little leverage to demand better quality housing.[154]

In imposing implied warranties in residential leases and in contracts for the sale of new homes, courts recognized that the *caveat emptor* doctrine did nothing to protect tenants and home buyers.[155] The justification for *caveat emptor* was that a tenant or buyer could "discover and protect himself against defects in [real] property."[156] In addition, traditional landlord-tenant law was developed for an agrarian society in which the land was much more valuable to the tenant than the dwelling.[157] Modern tenants have far less bargaining power than their agrarian predecessors, and unlike those predecessors, the modern tenant does not have the skill to discover defects in a building's complex systems.[158]

Courts avoid rewriting contracts, and the courts that first read an implied warranty of habitability into residential leases recognized this limitation on their power.[159] They justified the warranty by assuming that reasonable people would agree that housing must be "habitable and fit for living" and that therefore, if a landlord and tenant were to negotiate a lease, such a warranty would be included.[160]

As society placed increasing value on safe, affordable rental housing, legislatures and administrative bodies began to enact statutes and regulations aimed at ensuring the availability of such housing.[161] These codes and rules represented "a policy judgment—that it [was] socially (and

---

homes and not by lay sellers of existing homes, recognizing that a vendor-builder has control over the habitability of premises. Stevens v. Bouchard, 532 A.2d 1028, 1030 (Me. 1987).

152. *See* Javins v. First Nat'l Realty Corp., 428 F.2d 1071, 1077 (D.C. Cir. 1970).

153. *Id.* at 1078–79.

154. *See id.*

155. Frona M. Powell & Jane P. Mallor, *The Case for an Implied Warranty of Quality in Sales of Commercial Real Estate*, 68 WASH. U. L.Q. 305, 309–12 (1990).

156. *Id.* at 308.

157. *See* Katheryn M. Dutenhaver, *Non-Waiver of the Implied Warranty of Habitability in Residential Leases*, 10 LOY. U. CHI. L.J. 41, 45 (1978).

158. *See Javins,* 428 F.2d at 1078; *see also* Dutenhaver, *supra* note 157, at 51.

159. *See Javins*, 428 F.2d at 1077–78; Marini v. Ireland, 265 A.2d 526, 532 (N.J. 1970); Pines v. Perssion, 111 N.W.2d 409, 412 (Wis. 1961).

160. *Marini*, 265 A.2d at 533–34.

161. Mary Ann Glendon, *The Transformation of American Landlord-Tenant Law*, 23 B.C. L. REV. 503, 503–05 (1982).

politically) desirable to impose [the duty of providing safe housing] on a property owner" and thus abolish the rule of *caveat emptor*.[162] Describing the need for safe housing in the 1960s, one court urged that "[t]he need and social desirability of adequate housing for people in this era of rapid population increases is too important to be rebuffed by that obnoxious legal cliché, *caveat emptor*."[163]

The imposition of an implied warranty of habitability was seen as a move away from classifying a lease as a property conveyance to classifying a lease as a contract.[164] Yet, by making the warranty of habitability non-waivable, the courts veered from a freedom of contract approach. They recognized also that the validity of the distinctions between contract and property rules in landlord-tenant law was primarily historical and that courts have a duty to "reappraise old doctrines in the light of the facts and values of contemporary life."[165] In data security law, there is no such history to discard, and the law can be written on a cleaner slate, with protections pulled from contract, property, and tort law.[166] William Prosser once described the implied warranty as "a freak hybrid born of the illicit intercourse of tort and contract."[167] This illicit intercourse might provide the right remedy for the theft of personal information; by importing contract law concepts, judges can avoid twisting tort law to evade its limitation on recovery for purely economic loss.[168]

One challenge that courts will face in implying a warranty of data security is developing the standards that a payment system must meet in order to satisfy the warranty. Courts imposing an implied warranty of habitability were able to rely on housing codes for standards.[169] In data breach cases, the proper source for the elements of a quality payment system is not as clear. In a case like *DSW Shoe Warehouse*, the plaintiffs could use the fact that the FTC had filed a complaint against the retailer, alleging that it had "fail[ed] to employ reasonable and appropriate security measures to protect personal information and files."[170] The failure to

---

162. *Pines*, 111 N.W.2d at 412–13.

163. *Id.* at 413 (emphasis in the original).

164. *See* Glendon, *supra* note 161, at 503.

165. Javins v. Nat'l Realty Corp., 428 F.2d 1071, 1074 (D.C. Cir. 1970).

166. One could also analogize a data transaction to a bailment. Doing so might strain doctrine even less than imposing a warranty would. When a bailee misdelivers goods, the bailee is strictly liable to the bailor for damages. *See* R.H. Helmholtz, *Bailment Theories and the Liability of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 U. KAN. L. REV. 97, 99 (1992). One can certainly think of a data breach as a misdelivery of personal payment data.

167. William L. Prosser, *The Assault Upon the Citadel (Strict Liability to the Consumer)*, 69 YALE L.J. 1099, 1126 (1960).

168. *See supra* notes 143–148 and accompanying text.

169. *See, e.g.*, *Javins*, 428 F.2d at 1081–82; Berzito v. Gambino, 308 A.2d 17, 22 (N.J. 1973) (listing factors that a court should consider in determining whether a lessor had breached a covenant of habitability).

170. Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 777 (W.D. Mich. 2006) (citations omitted).

comply with PCI DSS would clearly constitute a breach of warranty, but as noted above, PCI DSS is seen as a minimum standard of data security.[171]

The judicially-created implied warranty of habitability was a response to changing social and economic conditions.[172] Courts implied the warranty of habitability at a time when society started to recognize that shelter is a basic human necessity.[173] The federal government recognized this in the Housing Act of 1949, "which committed [the government] to . . . achieving . . . the goal of a . . . suitable living environment for every American family."[174] While data security is not yet ingrained in our culture as a basic human need, lawmakers today are well aware that Americans may not "fully understand and appreciate what information is being collected about them" and may not have the power to stop unsafe practices from taking place.[175] Legislatures that have enacted data breach notification laws likewise recognize that data theft is a significant problem; in fact California, the first state to enact such a law, did so after one of the state's general purpose data centers suffered a security breach.[176] The legislative findings accompanying that law recognized that identity theft was one of California's fastest growing crimes, and that rapid notice of a data breach might help consumers minimize potential harm to them.[177]

In imposing an implied warranty of habitability, courts recognized that when a tenant rents an apartment or a house, that tenant "seek[s] a well known package of goods and services" that includes working utilities and proper maintenance.[178] Likewise, a consumer giving her payment card in a transaction expects that her information will be safeguarded in such a way that she will not be exposed to identity theft. Because she, like the urban tenant, cannot ensure the safety of her data on her own, courts should consider imposing a warranty of data security on sellers who accept payment cards.

CONCLUSION

Like residential tenants and buyers of new homes, the consumer who uses the payment system on a daily basis has little ability to protect herself

---

171. Cheney, *supra* note 20, at 4 (discussing observations of Robert Carr, CEO of Heartland Payment Systems at the time of the 2009 Heartland data breach).

172. *See* cases cited *supra* note 159.

173. *See generally* Glendon, *supra* note 161, at 528–45.

174. *Id.* at 519 (internal quotations omitted).

175. *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. (2010) (unpublished statement of John D. Rockefeller IV, Chairman, S. Comm. on Commerce, Science and Transportation), *available at* http://commerce.senate.gov/public/index.cfm?p=Hearings (follow "July 2010" hyperlink; then follow "Chairman John D. (Jay) Rockefeller IV" hyperlink).

176. Winn, *supra* note 109, at 1142–43.

177. *Id.*

178. Javins v. Nat'l Realty Corp., 428 F.2d 1071, 1074 (D.C. Cir 1970).

from data breaches. Some loss, therefore, should fall on the persons best able to guard against data theft. The real estate warranties are examples of judge-made warranties that respond to modern changes that put the consumer at risk for economic harm. Unsafe electronic payment systems likewise pose significant risks to consumers, particularly of data theft. One of the beauties of the common law is that courts can refine it to respond to modern conditions; indeed, the common law's "continued vitality . . . depends upon its ability to reflect contemporary community values and ethics."[179] Payment cards are a wonderful innovation,[180] but the misuse of the data that is collected from the users of those cards is a significant problem. Judges should recognize that consumers feel less secure in their financial lives when their data is compromised and fashion a warranty to compensate them for their losses.

179. *Id.* (internal quotations omitted).

180. In late 2009, no less an expert than former Federal Reserve Chairman Paul Volcker described the ATM as the most important financial innovation of the last 20 years. *See* Alan Murray, *Paul Volcker: Think More Boldly: The Former Fed Chairman Says the Conference Proposals Don't Go Nearly Far Enough to Accomplish What Needs to be Accomplished*, WALL ST. J., Dec. 14, 2009, at R7.