Maryland Law Review

Volume 75 | Issue 4 Article 2

Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry

David W. Opderbeck

MARYLAND LAW REVIEW

VOLUME 75 2016 NUMBER 4

SEVENTY-FIFTH ANNIVERSARY EDITION

Articles: Focus on Cyberlaw

CYBERSECURITY, DATA BREACHES, AND THE ECONOMIC LOSS DOCTRINE IN THE PAYMENT CARD INDUSTRY

DAVID W. OPDERBECK*

ABSTRACT

Data breaches are pervasive and costly. Recent civil data breach cases have centered on the consumer credit card payment chain in the retail industry. An important issue in such cases is whether the economic loss doctrine should bar negligence claims for purely pecuniary losses suffered by a non-negligent party, such as an issuing bank or a federal credit union that must incur costs to reimburse cardholders for the fraudulent use of stolen card numbers.

The economic loss doctrine should not bar these claims. Large-scale data networks, such as consumer credit card networks, often entail significant network externalities. These include externalities relating to market concentration as well as to the "weakest link" nature of security in these networks. Although the primary players in these networks are tied together in a complex web of contractual relationships, there are significant transaction costs involved with any effort to change or monitor another party's security measures. Moreover, "outside" entities such as

* Professor of Law, Seton Hall University Law School, and Director of the Gibbons Institute of Law, Science, & Technology.

Thanks to Nathan Sales and Vincent Johnson for helpful comments on earlier drafts of this Paper, and to John Burns for his helpful research assistance.

third-party payment processors, which are not in contractual privity with all other parties in the network, have become ubiquitous. Under these circumstances, a negligence rule should help improve cybersecurity hygiene and promote a more robust cyber risk insurance market.

I. INTRODUCTION

It is not a question of if you will suffer a data breach; it is a question of when. That is the warning cybersecurity experts regularly provide to enterprises of every sort in every segment of the economy.[1] This warning is more than an effort by high-priced consultants to spread FUD[2] in the hope that their clients will purchase expensive cybersecurity services. It is a reality of the digital age. Your cybersecurity may be good, but the hackers are better. Your data security policies may be comprehensive, but it takes only one tired, lazy, stupid, or malicious employee to release your native data irretrievably into the wild.[3]

Most analysts agree that the cost of data breaches are significant. The most recent Verizon Data Breach Report suggests that the average cost to breached entities is 58¢ per record, while the most recent Ponemon Institute report suggests an average cost of over $200 per record.[4] A breach involving a major retailer may encompass tens of millions of individual records.[5] A recent study suggests that data breaches will cost the U.S. economy $2 trillion by 2019.[6]

1. *See, e.g.*, Kate Vinton, *How Companies Can Rebuild Trust After a Security Breach*, FORBES (July 1, 2014), http://www.forbes.com/sites/katevinton/2014/07/01/how-companies-can-rebuild-trust-after-a-security-breach/.

2. FUD is an acronym for "fear, uncertainty, and doubt," originally coined as a term for an IBM comparative sales technique. *Fud*, *Fud in Technology*, DICTIONARY.COM, http://dictionary.reference.com/browse/fud (last visited Mar. 10, 2016).

3. *See, e.g.*, *Defending the Digital Frontier*, ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals.

4. VERIZON ENTERPRISE SOLUTIONS, 2015 DATA BREACH INVESTIGATIONS REPORT 28 (2015), http://www.verizonenterprise.com/DBIR/2015/; PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: UNITED STATES 1 (2015), http://www-03.ibm.com/security/data-breach/. A "record" is a piece of information, such as a payment card number, personally identifying information or medical record. *See* VERIZON ENTERPRISE SOLUTIONS, *supra*, at 28.

5. *See, e.g*, Brian Krebs, *In Home Depot Breach, Investigation Focuses on Self-Checkout Lanes*, KREBS ON SECURITY (Sept. 18, 2014), http://krebsonsecurity.com/tag/target-data-breach/ (noting that Target data breach exposed over 40 million records, and that the Home Depot breach was probably larger).

6. JUNIPER RESEARCH, CYBERCRIME AND THE INTERNET OF THREATS 5 (2015), https://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats.

The size and scale of these estimates suggests that the data breach problem is not only poorly contained—it is out of control. The enormous disparity between the cost to the breached entity (which already is sizable) and the overall economic costs (which could represent a meaningful percentage of GDP) suggests that the problem entails significant externalities. An externalities problem of this scope ordinarily indicates a need for some kind of governmental regulation.[7] Where the problem entails a need to exercise care against harms that impose externalities, tort law naturally presents itself as an option in the regulatory mix.[8] But even as the U.S. Congress has failed to pass significant cybersecurity legislation, the tort system has proven largely incapable of exercising much discipline over cybersecurity standards.[9]

Claims in civil data breach cases have fallen into two broad categories: (1) claims by consumers of the breached entity—usually a retailer, bank, or consumer service provider—whose credit card information, social security numbers, or other personally identifying information has been disclosed; and (2) claims by entities in the financial services chain who have incurred reimbursement, remediation, and other costs as a result of a data breach suffered by another party in the chain—again, usually a retailer, bank or consumer service provider.[10]

Most of these cases have failed at the pleading stage.[11] On the consumer side, the problem is that any direct losses usually are reimbursed by the credit card issuer and any potential future losses are speculative.[12] Tort claims in most consumer cases are resolved, or can be resolved, through Article III standing requirements.[13] On the business side, however, plaintiffs often are able to prove unreimbursed economic damages caused by the data breach.[14] The issue in these cases is that the direct losses are

7. *See* HOWELL E. JACKSON, ET. AL., ANALYTICAL METHODS FOR LAWYERS (2004), *reprinted in* STEVEN SHAVELL, ECONOMIC ANALYSIS OF LAW 19–21 (Foundation Press, 2004) (explaining the benefits of resolving externality problems through tort liability).

8. *Id.*

9. *See* David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 801–11 (2012) [hereinafter Opderbeck, *Cybersecurity*] (summarizing proposed cybersecurity legislation); David W. Opderbeck, *Current Developments in Data Breach Litigation: Article III Standing After Clapper*, 67 S. CAR. L. REV. ___ (2016) (forthcoming) (discussing issues with tort and other actions arising from data breaches); Jennifer Steinhauer, *House Passes Cybersecurity Bill After Companies Fall Victim to Data Breaches*, N.Y. TIMES (Apr. 22, 2015), http://nyti.ms/1JsSzGl (noting failed efforts to pass cybersecurity reform).

10. *See* David W. Opderbeck, *Civil Litigation and Data Breaches in the Consumer Financial Services Industry*, *in* PLI, THINK LIKE A LAWYER, TALK LIKE A GEEK 2014 (Nov. 2014).

11. *See id.*

12. *See id.*

13. *See id.*

14. *See id.*

solely economic, and it is often unclear whether, or to what extent, there might be a contractual remedy for those losses.[15] In business-to-business data breach cases, in other words, the deeper question is whether tort claims are barred by the "economic loss doctrine."[16]

The economic loss doctrine, or, more accurately, the complex of principles that relate to tort claims for purely economic harms, is hotly contested ground in contemporary tort policy. The American Law Institute released a draft proposal in *Restatement (Third) of Torts for Liability for Economic Harm* in 2012 that has attracted significant debate. As Professor Vincent Johnson has noted, the economic loss doctrine represents a "boundary" question between tort policy and private ordering.[17] Those who believe systemic economic risks are best allocated through contracts, insurance, social norms, and other forms of private ordering will tend to view the economic loss doctrine as an important bulwark against judicial regulation. Those who believe systemic economic risks entail externalities, agency problems, and other distortions that inevitably compromise the efficiency of private ordering will tend to view the economic loss doctrine as an impediment to the salutary risk-spreading and deterrence effects of the tort system.

This disagreement is particularly acute in the data breach context because the economic risks are so pervasive and wide-ranging. Today's global economy cannot function without the Internet, the "cloud," email, networked computer automation, and other components of "cyberspace," including the global consumer credit card payment networks. When everything is connected, a breach at one node of the network potentially affects all nodes, or a multiplicity of nodes, in unpredictable, non-linear ways. Can tort law play any principled role in managing this risk? Or is it more likely that tort claims will provide windfalls to lawyers and some individual plaintiffs without improving the system over private ordering—or worse, while making the system more rigid and vulnerable?

Part II of this Article reviews recent trends in civil litigation over data breaches, with particular attention to how the economic loss doctrine is applied to tort claims in such cases. As Part II discusses, most large-scale civil data breach litigation has arisen in the context of theft of consumer credit card data from large retailers. This means that the common law in this area has developed in relation to a unique economic infrastructure resource, the global consumer credit card network, which will be examined

15. *See id.*

16. *See id.*

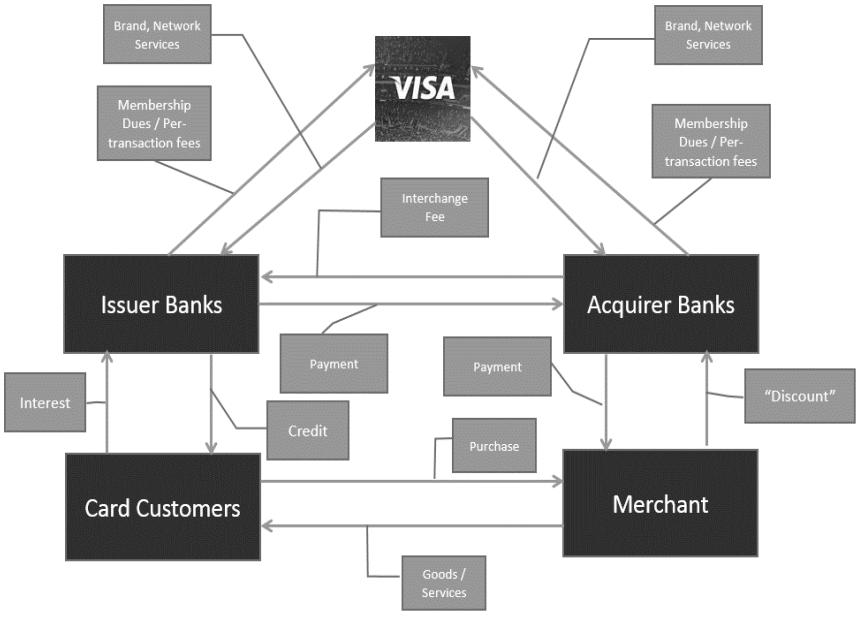
17. Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523, 546–49 (2009). By a "boundary" question Professor Johnson means something that marks the difference between one area of law and another area. *See id.*

in some detail. Part III examines the policy behind the economic loss doctrine and its application to data breach cases, particularly in credit card data theft cases where substantial network externalities are present. The discussion in Part III considers two factors that so far remain unexamined in the case law and scholarly literature: the role of third-party payment processors in the consumer credit card chain, and the availability of cyber risk insurance. Part IV evaluates whether the tort system can help correct market failures relating to data breaches even when the losses are purely economic. Part IV reviews the arguments of other scholars who suggest that the tort system should play little or no role in promoting cybersecurity, and suggests that in circumstances where significant network externalities are present tort remedies may help improve cybersecurity. Part V concludes.

II. TORT CLAIMS FOR DATA BREACHES

A. Consumer Credit Card Networks

The question of civil remedies for data breaches has been complicated by the fact that most civil litigation to date has arisen as the result of credit card information theft. A basic model of the web of relationships in consumer credit networks includes the credit card brand, the issuer bank, the consumer, the acquirer bank, and the merchant.[18] The relationships between and among each of these parties are governed by contracts with corresponding economic interests:



An individual card customer acquires a branded card (such as a Visa card) from an issuer bank.[19] Merchants are set up to receive credit card payments for goods and services by acquirer banks.[20] The issuer and acquirer banks each have contractual relationships with the card network.[21] The card network supplies to the banks the right to use the brand and access to the networks payment processing services.[22] The banks each pay membership dues and per-transaction fees to the networks.[23] When a cardholder makes a purchase using his or her card, the merchant transmits the purchase information to the acquirer bank, which, through the card brand network, inquires about the cardholder's credit status at the issuer bank.[24] If the cardholder possesses adequate credit, the approval of the transaction is communicated from the issuer bank to the acquirer bank through the card network.[25] The acquirer bank reimburses the merchant for the purchase price of the goods or services supplied to the customer, like a "discount fee," which is a percentage of the transaction price.[26] The issuer bank reimburses the acquirer bank for the purchase price, less an "interchange" fee.[27] The customer is responsible to repay the purchase amount to the issuer bank, usually with interest, if the amount is not paid in full within the first billing cycle.[28]

The largest networks worldwide are Visa and Mastercard.[29] The Visa and Mastercard networks are "four-party" networks, which involve an issuer bank, the cardholder, an acquirer bank, and the merchant.[30] Other substantial networks include American Express, Discover Card, and Diners

19. For sources relating to this general description, see, *e.g.*, *NaBanco*, 779 F.2d at 594; United States v. Am. Express Co., 88 F. Supp. 3d 143, 152–56 (E.D.N.Y. 2015); United States v. Visa U.S.A. Inc., 163 F. Supp. 2d 322, 331–34 (S.D.N.Y. 2001); Mark MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 1, 3–4; *How a Visa Transaction Works*, VISA, https://usa.visa.com/content_library/modal/how-visa-transaction-works.html (last visited Mar. 10, 2016); *Payments 101: Credit and Debit Card Payments*, FIRST DATA 6–9 (Oct. 2010), http://www.firstdata.com/downloads/thought-leadership/payments101wp.pdf.

20. *See generally supra* note 19.

21. *See generally supra* note 19.

22. *See generally supra* note 19.

23. *See generally supra* note 19.

24. *See generally supra* note 19.

25. *See generally supra* note 19.

26. *See generally supra* note 19.

27. *See generally supra* note 19.

28. *See generally supra* note 19.

29. U.S. OFFICE OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK: MERCHANT PROCESSING 2 (2014), http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/pub-ch-merchant-processing.pdf.

30. *Id.*; Sovereign Bank v. BJ's Wholesale Club, 533 F.3d 162, 164–65 (3d Cir. 2008).

Club.[31] These are three-party networks in which the issuer bank is the same as the acquirer bank.[32]

Both three- and four-party networks require the issuer and acquirer banks to agree to detailed sets of policies that govern the parties' relationships.[33] These policies typically include data security provisions. The VISA Core Rules, for example, state that all Visa network members must "[m]aintain all materials or records in any form that contains account or Transaction Information in a safe and secure manner with access limited to authorized personnel, as specified in the Payment Card Industry Data Security Standard ("PCI DSS")" and further must "[e]nsure that all agents and Merchants with access to account or Transaction Information comply with the . . . PCI DSS."[34] The VISA Core Rules also require members to ensure that agents and merchants do not store certain information, including the "[f]ull contents of any data taken from the Magnetic Stripe," subsequent to a transaction authorization.[35]

The Fair Credit Billing Act ("FCBA") limits the cardholder's liability for unauthorized use of his or her credit card to $50 and provides for zero liability if the card number was stolen without the physical card.[36] The Electronic Fund Transfer Act ("EFTA") limits the card holder's liability for unauthorized use of his or her card to $50 if the loss is reported within two business days after it is discovered or to $500 if the loss is reported between two business days and sixty calendar days after it is discovered.[37]

In practice, the major card networks have adopted "zero liability" policies in cases of data theft.[38] Under the VISA Core Rules, for example, an issuer is required to credit the cardholder's account for any electronic commerce transaction that involves fraud where the card was physically

31. COMPTROLLER'S HANDBOOK, *supra* note 29, at 2.

32. *Id.*

33. *See, e.g.*, VISA CORE RULES AND VISA PRODUCT AND SERVICE RULES § 1.1.1.1 (2015), https://usa.visa.com/dam/VCOM/download/about-visa/15-April-2015-Visa-Rules-Public.pdf ("All participants in the Visa system are subject to and bound by the Visa Charter Documents and the Visa Rules, as applicable based on the nature of their participation and geography."). The Visa Core Rules and Visa Service Rules are more than 800 pages long. *See id.* The Visa Interlink Network, Inc. Operating Regulations for participation in the Visa Interlink Network, which relates to electronic funds transfer ("debit") cards, is 180 pages long. *See* VISA, INTERLINK NETWORK, INC. OPERATING REGULATIONS (2014), https://usa.visa.com/dam/VCOM/download/about-visa/interlink-operating-regulations.pdf.

34. VISA CORE RULES, *supra* note 33, § 1.10.4.1.

35. *Id.*

36. 15 U.S.C. § 1666 (2012); 12 C.F.R. § 226.12(b) (2015); FEDERAL TRADE COMMISSION, LOST OR STOLEN CREDIT, ATM AND DEBIT CARDS 2–3 (2012), http://www.consumer.ftc.gov/articles/pdf-0075-lost-or-stolen-credit-atm-and-debit-cards.pdf.

37. 15 U.S.C. § 1693(g); FEDERAL TRADE COMMISSION, *supra n*ote 36, at 3.

38. *See, e.g.*, VISA, *Security + Support, Resolve Issues*, http://usa.visa.com/personal/security/zero-liability.jsp (last visited Dec. 16, 2015).

absent.[39] Further, in the U.S., "an [i]ssuer must limit the [c]ardholder's liability to zero upon receipt of notification from its [c]ardholder of an unauthorized Visa Consumer Card or Visa Business Card Transaction."[40] The VISA Core Rules further purport to "assign liability" between the issuer and acquirer for certain counterfeit transactions and provide an arbitration and compliance mechanism for disputes between members.[41]

The "presentation" and "card not present" rules represent some of the most important components of this mechanism. In a brick-and-mortar transaction, the customer must present the physical credit or debit card at the point of sale, and the merchant must take certain steps to authenticate the card.[42] It is, of course, possible for data thieves to manufacture counterfeit cards, purchase goods in brick-and-mortar retailers, and fence the goods online or elsewhere. The presentation rules for in-person purchases, however, at least create some additional transaction costs and provide some checks that might reduce the overall incidence of fraud. If the retailer complies with the card presentation rules, the risk of loss of fraud is borne entirely by the issuing bank.[43]

In the e-commerce context, the "card not present" rules do not apply because the transaction, by definition, is not conducted in person.[44] In this context, the e-commerce retailer ultimately bears the risk of loss of fraud.

B. Consumer Claims for Credit Card Information Theft

As noted above, cardholder information stolen in a data breach is fully reimbursed for any charges or debits made as a result of the theft. For this reason, most courts have found that consumers lack standing to sue and/or have no ascertainable damages under various common law theories.[45]

Some consumers have sought to recover costs of future credit monitoring, akin to claims for medical monitoring expenses in personal injury cases.[46] Prior to the Supreme Court's decision in *Clapper v. Amnesty*

39. VISA CORE RULES, *supra* note 33, § 1.11.1.2.

40. *Id.* § 4.1.13.3.

41. *Id.* §§ 1.10.7.1, 1.11.2.

42. *Id.* § 1.7.4

43. *Id.*; *see also Visa Optimizes Dispute Rules*, VISA, https://usa.visa.com/dam/VCOM/download/merchants/visa-optimizes-dispute-rules-new-avenues-for-card-not-present-mechants.pdf (last visited Mar. 10, 2016) (discussing authentication requirements in effect as of October 17, 2015); *Global Visa Card-Not-Present Merchant Guide to Greater Fraud Control*, VISA, https://www.visa-asia.com/ap/sg/merchants/include/Global_Card_Absent_GuideTo_Fraud_Control.pdf (last visited Mar. 10, 2016).

44. *See* MacCarthy, *supra* note 19, at 9–10.

45. *See* Opderbeck, *Cybersecurity*, *supra* note 10.

46. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631, 639 (7th Cir. 2007).

International USA,[47] there was a circuit split concerning whether such claims satisfy Article III standing requirements.[48] In *Clapper*, a case involving the NSA's surveillance programs authorized by the FISA Court, the Supreme Court held that Article III standing requires at least "certainly impending" or "substantial" risk of future harm.[49] It is unclear whether *Clapper* implicitly abrogates the holdings in cases that had previously allowed future credit monitoring claims to proceed in data breach cases.[50]

Consumers have also filed claims under state consumer fraud and data breach reporting statutes, with varying degrees of success depending on the particular standing and out-of-pocket loss requirements of the statutes.[51] These cases generally do not implicate the economic loss doctrine because they are statutory and not common law tort claims.

C. Business Claims for Recovery of Expenses Related to Data Theft

The second broad category of data breach cases is comprised of claims by commercial entities for losses caused by breaches of other commercial entities. These cases involve quantifiable, unreimbursed out-of-pocket losses, so they do not usually fail on threshold Article III standing grounds.

An important question that arises in connection with this web of relationships is why civil litigation would ever ensue in the first place. The card networks and banks obviously are engaged in a highly lucrative enterprise that is designed to be self-policing. Indeed, as discussed in Part III.C *infra*, some courts and regulators have found that aspects of the credit card networks can violate the antitrust laws. It would seem exceedingly strange for an issuing or acquiring bank that has suffered some loss as the result of a credit card data breach to air this dirty laundry in court. The answer to this question may lie in several existing and emerging aspects of consumer credit and data security.

First, many of the high-profile commercial cases have been filed by credit unions associated with pension funds and labor unions.[52] The credit unions often issue Visa or MasterCard credit and debit cards to their members, but the credit unions usually do not function as issuing or

47. 133 S. Ct. 1138 (2013).

48. *Cf.* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (Article III standing not satisfied); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (Article III standing satisfied); *Pisciotta*, 499 F.3d 629, 634 (Article III standing satisfied).

49. *Clapper*, 133 S. Ct. at 1147–48, n.5.

50. For a discussion of this question, see Peters v. St. Joseph Serv's Corp., 74 F. Supp. 3d 847, 856, n.10 (S.D. Tex. 2015); Antman v. Uber Tech's, Inc., No. 3:15-cv-01175-LB, 2015 WL 6123054, at *10 (N.D. Cal. Oct. 19, 2015).

51. *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1165–66 (D. Minn. 2014).

52. *See, e.g.*, Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 164 (3d Cir. 2008).

acquiring banks because they are not regulated as banks. Nevertheless, the credit unions may be charged by the credit card network or the issuing bank with the costs of reimbursing cardholders for losses after a data breach. If the party that was breached was the acquiring bank or the merchant, the credit union may not have any leverage or recourse under the card network agreements.

Second, recent high-profile commercial cases have involved enormously influential national retailers such as BJ's and Target.[53] The size and influence of these "big box" retail chains might skew the dynamics of a system designed when the retail industry was far more local or regional, and banks correspondingly had more ability to control risk.

Finally, at least one of the recent cases involves a third-party payment processor.[54] As discussed in Part III.D *infra*, third-party payment processors have become a ubiquitous part of the consumer credit chain, but they are not banks and are not otherwise direct members of the credit card networks. Parts II.B.1–3 discuss several of these recent important cases in which courts applied the economic loss doctrine.

1. The BJ's Data Breach Litigation (2008)

The litigation resulting from one of the first major retail data breaches, involving BJ's Wholesale Club,[55] provides an excellent example of the economic loss doctrine as applied in a data breach case. In *Sovereign Bank v. BJ's*, plaintiffs alleged that BJ's had stored electronic credit card information in violation of the Visa Operating Regulations and that Fifth Third Bank, the merchant bank that processed the BJ's transactions, failed to ensure BJ's compliance with the Regulations.[56] One of the plaintiffs, Sovereign Bank, was an issuer bank that was required to reimburse its cardholders for losses incurred as a result of the breach in accordance with the Visa cardholder agreement.[57] The other plaintiff, Pennsylvania State Employees Credit Union ("PSECU"), also functioned as an issuer of Visa cards to its members and claimed that it had incurred approximately $98,000 in out-of-pocket expenses when it canceled and reissued its members' cards that were compromised by the breach.[58]

53. *See id.*; *In re Target*, 66 F. Supp. 3d at 1154.

54. *See In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566 (S.D. Tex. 2011), *rev'd in part sub nom.*, Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013).

55. Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162 (3d Cir. 2008).

56. *Id.* at 166–67.

57. *Id.*

58. *Id.*

Both Fifth Third and PSECU suffered direct, ascertainable losses as a result of the breach. Nevertheless, the Court of Appeals for the Third Circuit, applying Pennsylvania law, held that the plaintiffs' negligence claims were barred under the economic loss doctrine.[59] According to the Third Circuit, Pennsylvania had adopted a relatively straightforward version of the economic loss doctrine: "The Economic Loss Doctrine provides that no cause of action exists for negligence that results solely in economic damages unaccompanied by physical or property damage."[60]

The court rejected Sovereign Bank's argument that Pennsylvania law in fact was more nuanced than this bald rule statement suggests.[61] The Third Circuit quoted at length from a Pennsylvania Superior Court decision: "To allow a cause of action for negligent cause of purely economic loss would be to open the door to every person or business to bring a cause of action. Such an outstanding burden is clearly inappropriate and a danger to our economic system."[62]

Similarly, the Third Circuit rejected PSECU's argument that Pennsylvania had modified its economic loss doctrine in later case law.[63] In addition, the court waived off PSECU's argument that there was, in fact, physical property damage because its consumers' compromised credit cards were canceled.[64] According to the court, "PSECU deemed the cards useless not because they were damaged, but because PSECU was exposed to liability for unauthorized charges."[65]

The BJ's data breach also spawned litigation that reached the Massachusetts Supreme Judicial Court in *Cumis Insurance Society v. BJ's Wholesale Club, Inc.*[66] In *Cumis*, claims were asserted against Fifth Third and BJ's by a group of credit unions that had issued MasterCard and Visa cards to their members and by an insurer of the credit unions that had reimbursed credit union card members for fraudulent charges.[67] The court rejected the plaintiffs' negligence claims under the economic loss doctrine.[68] Like the court in *Sovereign Bank*, the Massachusetts high court stated the economic loss doctrine, under Massachusetts law, in stark terms:

59. *Id.* at 175–80.

60. *Id.* at 175 (quoting Adams v. Copper Beach Townhome Cmtys., L.P., 816 A.2d 301, 305 (Pa. Super. Ct. 2003)).

61. *Id.* at 176–77.

62. *Id.* at 176 (quoting Aikens v. Balt. & Ohio R.R. Co., 501 A.2d 277, 279 (Pa. Super. Ct. 1985)).

63. *Id.* at 180.

64. *Id.* at 179–80.

65. *Id.* at 180.

66. 918 N.E.2d 36 (Mass. 2009).

67. *Id.* at 39.

68. *Id.* at 46–47.

"In addition, the economic loss doctrine bars recovery unless the plaintiffs can establish that the injuries they suffered due to the defendants' negligence involved physical harm or property damage, and not solely economic loss."[69]

The court in *Cumis* was even less sanguine than the Third Circuit, however, about third-party beneficiary claims. The Massachusetts court noted that the agreement between BJ's and Fifth Third contained a clause expressly disclaiming any intent to benefit third-parties.[70] The court further concluded that the security provisions in the Visa and MasterCard operating regulations did not override this express disclaimer of third-party liability.[71] Rather, the court said, "nothing in the Visa and MasterCard operating regulations prohibits [the merchant bank and the merchant from] entering into agreements that explicitly exclude enforcement by third parties."[72] Unlike the Third Circuit, the Massachusetts Supreme Judicial Court had no qualms about foreclosing the sort of contract remedy that could provide an alternative to a tort claim for economic losses.[73]

2. The Target Data Breach Litigation (2014)

The breach of another major national retailer, Target, also spawned a large-scale civil class action litigation filed by consumer credit card holders.[74] The Federal Target cases were consolidated in the District of Minnesota by the Judicial Panel on Multidistrict Litigation. That court subsequently heard a motion to dismiss on the pleadings.[75] A portion of the court's opinion considered the plaintiffs' tort claims under the economic loss doctrine.[76] Judge Magnuson evaluated these claims under the law of each state in which Target asserted that the economic loss doctrine should

69. *Id.* at 46 (citing Aldrich v. ADD Inc., 770 N.E.2d 447 (Mass. 2002)).

70. *Id.* at 43–44 (quoting agreement as follows: "This Agreement is for the benefit of, and may be enforced only by, [Fifth Third] and [BJ's] and their respective successors and permitted transferees and assignees, and is not for the benefit of, and may not be enforced by, any third-party.").

71. *Id.* at 45.

72. *Id.*

73. The court's holdings in *Cumis* subsequently were applied by the First Circuit in the TJX data breach litigation. Amerifirst Bank v. TJX Cos. (*In re* TJX Cos. Retail Sec. Breach Litig.), 564 F.3d 489, 495 (1st Cir. 2009).

74. *See In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, (D. Minn. 2014).

75. *Id.*

76. *Id.* at 1171–76.

bar the claims.[77] Accordingly, the court evaluated the economic loss doctrine as applied to data breaches under the law of eleven jurisdictions.[78]

Judge Magnuson seems to have adopted two basic principles: (1) if a state court or a local federal court applying state law previously held that the economic loss doctrine barred a data breach claim, then the motion to dismiss concerning that jurisdiction would be granted; but (2) absent such authority on point, if the relevant state law allowed tort claims for economic loss based on a "special relationship," the tort-based allegations would survive dismissal.[79] This approach seems to reflect a strained notion of stare decisis because most of the authorities the court relied upon were federal district or circuit court decisions applying or predicting state law, not state law itself, except for cases from Idaho, Iowa, and New Hampshire state courts.[80] In any event, Judge Magnuson held that the economic loss doctrine in Alaska, California, Illinois, Iowa, and Massachusetts barred plaintiffs' tort claims but that negligence claims under other state law could proceed.[81]

3. The Heartland Breach (2011)

The breach of a major third-party payment processor, Heartland Payment systems, resulted in claims against Heartland by credit card customers and issuer banks in the Southern District of Texas.[82] The district court applied New Jersey law, holding that the economic loss doctrine prohibited plaintiffs' negligence claims.[83] In addition to its analysis of New Jersey precedent, the district court noted that, under New Jersey public policy, "allocation of risks in accordance with [a voluntary] agreement better serves the public interest than an allocation achieved as a matter of

77. *Id.*

78. *Id.* The jurisdictions were Alaska, California, the District of Columbia, Georgia, Idaho, Illinois, Iowa, Massachusetts, New Hampshire, New York, and Pennsylvania. *Id.*

79. *See id.*

80. *See id.* at 1173–75. In Idaho, a state Supreme Court opinion suggested a "special relationship" exception to the economic loss doctrine. Aardema v. U.S. Dairy Sys., Inc., 215 P.3d 505 (Idaho 2009). In Iowa, a state Supreme Court opinion refused to adopt a "special relationship" exception. St. Malachy Roman Catholic Congregation of Geneseo, Ill. v. Ingram, 841 N.W.2d 338 (Iowa 2013). In New Hampshire, in which a state Supreme Court opinion seemed to adopt an independent duty/special relationship exception to the doctrine. Plourde Sand & Gravel Co. v. JGI E. Inc., 917 A.2d 1250 (N.H. 2007).

81. *Id.* at 1176.

82. *See In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566 (S.D. Tex. 2011), *rev'd in part sub nom.*, Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013).

83. *Id.* at 585–90.

policy without reference to that agreement."[84] The district court stated that this view "is consistent with the approach of the federal government and most states, which generally have avoided regulating risk allocations in the payment-card industry except to cap consumers' liability."[85] According to the district court, federal and state law, including New Jersey law, regulates credit card consumer privacy but not security, suggesting that the allocation of risks relating to security should be left to private bargaining.[86] The district court, therefore, dismissed plaintiffs' negligence claim.[87]

The Court of Appeals for the Fifth Circuit, however, reversed.[88] The appellate court agreed that New Jersey law encoded a broad public policy favoring contract principles and private bargaining for the allocation of purely economic risk.[89] However, the court also noted that New Jersey law suspends the economic loss doctrine and imposes a "duty of care to take reasonable measures to avoid the risk of causing economic damages, aside from physical injury, to particular plaintiffs or plaintiffs comprising an identifiable class with respect to whom [the] defendant knows or has reason to know are likely to suffer such damages from its conduct . . . ."[90] The Fifth Circuit further recited the principles for determining whether a class of plaintiffs is "identifiable" under New Jersey law: the class "must be particularly foreseeable in terms of the type of persons or entities comprising the class, the certainty or predictability of their presence, the approximate numbers of those in the class, as well as the type of economic expectations disrupted."[91] Where application of these factors is unclear, the court should "draw upon notions of fairness, common sense and morality to fix the line limiting liability as a matter of public policy, rather than an uncritical application of the principle of particular foreseeability."[92]

84. *Id.* at 589 (quoting Spring Motors Distribs., Inc. v. Ford Motor Co., 489 A.2d 660, 671 (N.J. 1985)).

85. *Id.*

86. *Id.*

87. *Id.* at 590.

88. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 422 (5th Cir. 2013).

89. *Id.* at 423–24. The Fifth Circuit also quoted *Spring Motors*, as follows:

> Generally speaking, tort principles, such as negligence, are better suited for resolving claims involving unanticipated physical injury, particularly those arising out of an accident. Contract principles, on the other hand, are generally more appropriate for determining claims for consequential damage that the parties have, or could have, addressed in their agreement.

Id. at 424 (quoting *Spring Motors*, 489 A.2d at 672).

90. *Id.* at 424 (quoting People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 116 (N.J. 1985)).

91. *Id.* (quoting *People Express*, 495 A.2d at 116).

92. *Id.*

Applying these principles to the issuer banks' claims, the Fifth Circuit stated that "[t]he identities, nature, and number of the victims are easily foreseeable, as the Issuer Banks are the very entities to which Heartland sends payment card information."[93] The court further stated that "in the absence of a tort remedy, the Issuer Banks would be left with no remedy for Heartland's alleged negligence, defying 'notions of fairness, common sense and morality.'"[94] The court thought it "unclear" whether the payment processor, Heartland, was a contractual participant in the Visa and MasterCard networks or whether the Issuer Banks had any bargaining power in relation to Heartland.[95] Therefore, the court concluded, "it is not clear that the allocation of risk 'could have been the subject of . . . negotiations' between the Issuer Banks and Heartland by way of contracts with Visa and MasterCard."[96] The appellate court, therefore, reversed the dismissal of plaintiffs' negligence claim on the pleadings.[97]

The trial and appellate court opinions in the *Heartland* litigation are interesting on the doctrinal, policy, and factual levels. Doctrinally, these opinions raise questions, and provide conflicting answers, about the availability and applicability of a "special relationship" exception to the economic loss doctrine. Concerning public policy, they raise questions, and provide conflicting answers, about bargaining power and risk allocation among various entities in the consumer credit chain. At the factual level, the trial and appellate courts seem to have held different perceptions about what kind of entity Heartland was, which may have colored their different approaches to doctrine and policy.

93. *Id.* at 426 (citing *People Express*, 495 A.2d at 116).

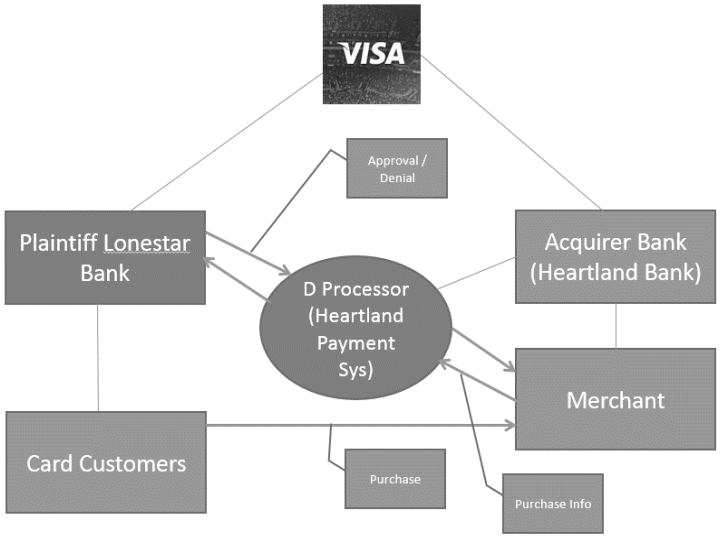
94. *Id.* (first quoting *People Express*, 495 A.2d at 116; and then citing Carter Lincoln-Mercury, Inc. v. EMAR Grp., Inc., 638 A.2d 1288, 1294 (N.J. 1994)).

95. *Id.*

96. *Id.* (quoting Travelers Indem. Co. v. Dammann & Co., 594 F.3d 238, 248 (3d Cir. 2010)).

97. *Id.* at 427.

As noted in Part II.A *supra*, the "typical" credit card network is a four-party or three-party network. In *Heartland*, however, another entity, with an unclear relationship to the acquirer bank, stood between the issuer bank and the merchant:



At first blush, it appears that the "payment processor," Heartland Payment Systems, is related to the acquirer bank, Heartland Bank, but the Fifth Circuit apparently was unwilling to delve into this factual question in connection with a motion to dismiss on the pleadings. In fact, Heartland Payment Systems is an independent payment processor and was not related to Heartland Bank, which has since been acquired by another bank. Moreover, the presence of an independent payment processor in the consumer credit card chain is not unusual. As discussed in Part III *infra*, the details of the credit card payment system, including the role of independent payments processors, should have significant consequences for how courts apply the economic loss doctrine in data breach cases.

III. THE POLICY AND ECONOMICS OF THE ECONOMIC LOSS DOCTRINE APPLIED TO DATA BREACHES

A. The Policy and Economics of the Economic Loss Doctrine

1. Economic Loss, Boundaries, and Foreseeability

The economic loss doctrine is traditionally invoked to define the boundary between tort and contract law.[98] The effort to draw this line has been justified by the belief that risks and benefits are allocated more efficiently through private ordering than by public legal regulation.[99] One important economic rationale for this boundary function is that it places the risk of loss on the party best able to insure against the risk.[100] However, courts often apply the economic loss doctrine as a boundary marker in favor of private ordering even when the insurance rationale does not apply.[101] In such cases, perhaps in most cases, the doctrine may simply reflect a policy or ideological judgment against governmental regulation.[102] Stated more positively, the economic loss doctrine may help negotiate whether a given set of social relationships is better suited to a contract, tort, property, or negligence law "paradigm."[103]

The *Kinsman* cases are a classic pair of cases used by torts professors to introduce the economic loss doctrine in relation to general tort concepts of foreseeability.[104] Those cases resulted when a barge broke loose from its improperly secured moorings on the icy Buffalo River and crashed into a second barge, which also broke its moorings.[105] The two barges were swept downriver until they collided with the Michigan Avenue Bridge in Buffalo.[106] The resulting pileup of barges and ice cased the river to overflow and flood private property surrounding the bridge.[107] The court had little problem finding that the flooding was a foreseeable result of the first barge-owner's negligence in improperly securing its moorings and awarded tort damages to the property owners.[108]

98. *See* Johnson, *supra* note 17, at 546.

99. Jay M. Feinman, *The Economic Loss Rule and Private Ordering*, 48 ARIZ. L. REV. 813, 817 (2006).

100. *See* Johnson, *supra* note 17, at 544–45.

101. *Id.* at 544–59.

102. Feinman, *supra* note 99, at 825–26.

103. William Powers, Jr., *Border Wars*, 72 TEX. L. REV. 1209, 1210–11 (1994).

104. *In re* Kinsman Transit Co. (*Kinsman I*), 338 F.2d 708 (2d Cir. 1964); *In re* Kinsman Transit Co. (*Kinsman II*), 388 F.2d 821 (2d Cir. 1968).

105. *Kinsman I*, 338 F.2d at 711–14.

106. *Id.*

107. *Id.*

108. *Id.* at 714

The ships meant to deliver wheat to a grain elevator downstream from the bridge, however, did not fare as well in court.[109] The mess at the bridge impeded river traffic for two months and delayed grain shipments to the elevator, resulting in economic losses to the plaintiffs.[110] Here the court drew a line: the purely economic losses, although surely within the chain of actual causation resulting from the first barge owner's negligence, were not reasonably foreseeable for the purposes of proximate causation.[111] The court stated that, "we hesitate to accept the 'negligent interference with contract' doctrine in the absence of satisfactory reasons for differentiating contractual rights from other interests which the law protects."[112] However, applying ordinary tort principles of foreseeability, the court held that the economic losses were too speculative or remote to permit recovery.[113]

The *Kinsman* cases are wonderfully illustrative because they literally involve a *stream*—actually a large river—of causality. Negligence happens "upstream" and causes results "downstream." How far "downstream" does liability in tort extend? All the way to the harbor? Out the harbor and across the sea? No: the Michigan Avenue Bridge itself literally supplies the "bridge" between torts and private ordering. Once that bridge is crossed, there is no tort remedy. But how can we determine when we are about to cross the bridge? It may only reflect, as Justice Andrews stated in his famous *Palsgraf* dissent in relation to proximate cause, a matter "of convenience, of public policy, of a rough sense of justice" through which "the law arbitrarily declines to trace a series of events beyond a certain point."[114]

It is interesting that the court in *Kinsman II* eschewed a bald formulation of an economic loss doctrine (which it called the "negligent interference with contract" principle) in favor of general foreseeability principles. This tension illustrates that courts as well as commentators have had difficulty articulating exactly what the economic loss doctrine is and precisely what function it serves in tort law beyond the general concept of foreseeability.

109. *Kinsman II*, 338 F.2d 821.

110. *Id.* at 823–24.

111. *Id.* at 825. The court quoted Judge Andrews' formulation of the proximate cause rule from the *Palsgraf* case: "It is all a question of expediency. . . . of fair judgment, always keeping in mind the fact that we endeavor to make a rule in each case that will be practical and in keeping with the general understanding of mankind." *Id.* (quoting Palsgraf v. Long Island R.R., 162 N.E. 99, 104 (N.Y. 1928) (Andrews, J., dissenting)).

112. *Id.* at 823.

113. *Id.* at 823–24.

114. *Palsgraf*, 162 N.E. at 103 (Andrews, J., dissenting).

2. Economic Loss and Externalities

A more robust *economic* explanation for the economic loss doctrine relates to the concept of externalities.[115] Tort-based liability rules can be viewed as a mechanism for correcting market failures.[116] If an activity imposes costs only on its producer and confers benefits only on its consumer, then the producer and consumer can agree on an appropriate market exchange. If the activity also imposes costs or confers benefits on third parties other than the producer and consumer, there is an "externality" or "spillover."[117] Externalities do not necessarily result in net economic inefficiency. For example, the price of the original transaction might be adjusted by the market to reflect the costs or benefits of the externality, or markets may arise in which the right to impose externalities can be bought and sold.[118]

But in many cases, such market corrections are impossible, often because transactions costs are excessive.[119] The tort system then serves as a replacement for an externalities market.[120] The cost of tort liability forces the party imposing negative externalities to internalize those costs. This economic efficiency function thereby feeds into tort law deterrence and risk-spreading rationales. If a party imposing negative externalities knows that it is liable for those costs, it will take reasonable precautions and/or obtain insurance, and the costs of those precautions and/or insurance will be reflected in the exchange between the producer and consumer.[121]

Many cases of private economic loss do not reflect a net cost to society and therefore do not represent externalities.[122] Consider, for example, the following prototypical case: A negligent driver crashes into another car on a highway, injuring the driver of the second car and closing the highway until the debris is cleared. Because the highway is closed, a truck carrying bananas is unable to reach the local food store, and as a result, a customer who comes to the store looking to purchase bananas finds the store's banana display empty. The driver of the second car could recover damages relating to his physical injuries against the negligent driver of the first car. But the economic loss doctrine would prohibit the store from recovering these lost banana sales from the negligent driver, even though actual causation could be established.

115. *See generally* W. Bishop, *Economic Loss in Tort*, 2 OXFORD J. LEGAL STUD. 1 (1982).
116. *Id.* at 3–4.
117. *See id.* at 3.
118. *See id.* at 4.
119. *See id.*
120. *See id.*
121. *See id.*
122. *Id.*

One economic rationale for this result is that the store's individual economic losses probably do not represent a *social* cost. The customer presumably could purchase her bananas at a different store, in which case the overall market would remain in equilibrium: the consumer would still have her bananas and the revenue would simply have shifted from the first store to the second.[123] In other words, the market efficiently soaks up potential externalities.

It is possible to imagine cases in which the market cannot efficiently soak up potential externalities. Even the simple example given above does not account for the customer's increased transaction costs in finding and traveling to a new store with bananas in stock. If those costs were significant, the customer's desire to obtain bananas might be frustrated, and the loss of this transaction might represent a social cost. In such a case, there is an economic argument in favor of allowing a tort claim by the first store against the negligent driver to recover its lost revenue. Of course, litigation over the cost of a few bananas would be prohibitively expensive, so we need not fear an inefficient litigation explosion over trivial cases. But where the stakes are high enough, a tort remedy might provide the most efficient result, particularly over the long term as repeated tort cases encourage greater care and risk spreading through insurance.

Transaction costs are likely to increase in relation to the extent the frustrated expectations of the original parties were unique or special. In the example of the bananas, the customer does not have any sort of unique or special relationship with the trucking company or the grocer. Bananas are essentially a commodity, and the customer can easily find a replacement if her expectation of purchasing bananas at the first grocer are frustrated. There is nothing unique or special about the customer's relationship to the grocer, the trucking company, or the negligent driver. The possibility of a "special" relationship that might produce an exception to the economic loss doctrine leads to the next Part.

B. "Exceptions" to the Economic Loss Doctrine

The word "exceptions" is in quotation marks in this Part's heading because the economic loss doctrine is not really a "rule" with "exceptions." Some courts and commentators refer to it as the economic loss *rule*, but this Article has avoided that terminology on purpose. It is better thought of as a general principle that may or may not apply in light of other applicable principles.

123. *See id.* at 4–6.

Many of these principles were recognized in the proposed *Restatement (Third) of Torts: Liability for Economic Harm*.[124] This proposed *Restatement* has proven controversial, although portions of it have been approved by the ALI membership.[125] The proposed *Restatement*, in Section 1, recognizes that, "[a]n actor has no general duty to avoid the unintentional infliction of economic loss on another," but specifies circumstances under which such a duty could arise.[126] Comment c. to Section 1 acknowledges that a general duty to avoid economic losses could lead to indeterminate and disproportionate liability and that courts should usually defer to contractual arrangements because "[r]isks of economic loss tend to be especially well suited to allocation by contract."[127]

In particular, Comment c. to Section 1 suggests that a person entering into a transaction "has a full chance to consider how to manage the risks involved, whether by inspecting the item or investment, obtaining insurance against the risk of disappointment, or making a contract that assigns the risk of loss to someone else."[128] Further, Comment c. recognizes that if insurance benefits, indemnity payments, or other agreed upon monetary payments are allocated pursuant to an agreement, the injured party is made whole.[129] Finally, Comment c. notes that the parties are usually in a better position ex ante to determine an appropriate allocation of risks and responsibilities than a court would be ex post, and an ex post judicial determination also involves additional social costs of adjudication.[130] Nevertheless, Comment e. suggests that "[a] court should not labor under a presumption against liability when the rationales for restricting it are absent."[131]

Consistent with Section 1 and its Comments c. and e., Section 3 of the proposed *Restatement* states that, "[e]xcept as provided elsewhere in this Restatement, there is no liability in tort for economic loss caused by negligence in the performance or negotiation of a contract between the

124. RESTATEMENT OF THE LAW (THIRD) TORTS: LIAB. FOR ECON. HARM (AM. LAW INST., Tentative Draft No. 1, 2012) [hereinafter PROPOSED RESTATEMENT DRAFT NO. 1].

125. *See* Vincent R. Johnson, *The Vast Domain of the* Restatement (Third) of Torts, 1 WAKE FOREST L. REV. FORUM 29 (2010); *Restatement of the Law, Third, Torts: Liability for Economic Harm*, AM. LAW INST., https://www.ali.org/projects/show/torts-liability-economic-harm-3rd/.

126. PROPOSED RESTATEMENT DRAFT NO. 1, *supra* note 124, §§ 1(a)–(b). The Comment to this Section notes that, "[s]ubsection (a) states a more limited principle [than the economic loss rule]: not that liability for economic loss is generally precluded, but that duties of care with respect to economic loss are not general in character; they are recognized in specific circumstances." *Id.* § 1 cmt. b.

127. *Id.* § 1 cmt. c.

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.* § 1 cmt. e.

parties."[132] One of the provisos is relatively uncontroversial because it is already embedded in substantial existing case law: professional negligence (Section 4).[133] A proviso on negligent misrepresentation (Section 5) is more controversial because it takes a position on a disputed body of case law.[134] A third proviso is even more controversial: "negligent performance of services" (Section 6).[135] The proviso for negligent performance of services states that,

> [o]ne who, in the course of his business, profession, or employment, or in any other transaction in which he has a pecuniary interest, performs a service for the benefit of others, is subject to liability for pecuniary loss caused to them by their reliance upon the service, if he fails to exercise reasonable care in performing it.[136]

Liability would be limited to loss suffered by "the person or one of a limited group of persons for whose benefit the actor performs the service" and "through reliance upon it in a transaction that the actor intends to influence."[137] The illustrations to this first draft of Section 6 are interesting for our discussion of data breach cases.[138]

Illustration 1 involves an accountant hired by a limited partnership to provide auditing services, which are performed negligently.[139] The limited partners individually rely on the services.[140] The accountant would be liable to the limited partners because they relied on the representations and expertise of the accountant.[141]

Illustration 5 involves a mechanic who negligently services a machine.[142] The machine's owner then sells it to a buyer, who subsequently learns it must be repaired. If the mechanic was hired by the original owner for his own benefit, the mechanic would not be liable in negligence to the buyer. If the mechanic was hired by the original owner as a condition of the sale, however, the mechanic would be liable to the buyer in negligence because the buyer relied on the mechanic's work.[143]

---

132. *Id.* § 3.
133. *Id.* § 4.
134. *Id.* § 5.
135. *Id.* § 6.
136. *Id.*
137. *Id.*
138. *Id.* § 6 illus. 1–6.
139. *Id.* § 6 illus. 1.
140. *Id.*
141. *Id.* The reporter's note states that this illustration is based on *White v. Guarente*, 372 N.E.2d 315 (N.Y. 1977). *Id.* § 6 reporter's note a.
142. *Id.* § 6 illus. 5.
143. *Id.* The reporter's note states that this illustration is based on *Ramerth v. Hart*, 983 P.2d 848 (Idaho 1999). *Id.* § 6 reporter's note a.

Illustration 6 involves a builder who negligently constructs a chimney on a home.[144] The homeowner subsequently sells the home to a buyer. After the sale, the chimney damage becomes evident and requires repair. The builder would not be liable to the subsequent buyer because the buyer would have had ample opportunity to conduct any inspections before closing and to adjust the purchase price accordingly and/or to include adjustments for latent defects in the sale contract.

A similar dynamic is reflected in Section 6 of the proposed *Restatement (Third)*.[145] That Section states that there is liability for negligent performance of a service that causes pecuniary loss to others if the loss is "suffered (a) by the person or one of a limited group of persons for whose benefit the actor performs the service; and (b) through reliance upon it in a transaction the actor intends to influence."[146]

This Section would "not recognize liability for negligence in the course of negotiating or performing a contract between the parties."[147] The illustrations include an accountant hired by a limited partnership who makes representations that are relied upon by the limited partners, a lawyer who represents both buyer and seller in a transaction, a realtor who works for the seller but arranges for a home inspection on the buyer's behalf, and the machine mechanic illustration from Section 3.[148]

Comment b. to Section 6 covers "three-cornered construction disputes."[149] The example provided is a construction project owner who hires an architect and a builder, who have no contract with each other.[150] The architect's negligent design causes the builder to suffer pecuniary losses.[151] The proposed *Restatement (Third)* would recognize tort liability under these circumstances.[152] The Comment notes that if the default tort liability rule's "allocation of responsibility is not congenial to the parties, they are free to change it in the contracts that link them."[153]

Data breach cases in the consumer credit card industry seem to fall somewhere between Illustrations 1 and 6 to Section 3 and in some ways

144. *Id.* § 6 illus. 6. The reporter's note states that this illustration is based on *Redarowicz v. Ohlendorf*, 441 N.E.2d 324 (Ill. 1982), although the note indicates there is a division of authority on the question. *See id.* § 6 reporter's note c.

145. RESTATEMENT OF THE LAW THIRD TORTS: LIAB. FOR ECON. HARM § 6 (AM. LAW. INST., Tentative Draft No. 2, 2014).

146. *Id.* §§ 6(2)(a)–(b).

147. *Id.* § 6(4).

148. *Id.* § 6 illus. 1–3, 5.

149. *Id.* § 6 cmt. b.

150. *Id.*

151. *Id.*

152. *Id.*

153. *Id.*

seem to resemble the liability scenario under Illustration 5 to both Sections 3 and 6 of the proposed *Restatement (Third)*. None of the parties in the credit card finance chain are "hired" by the other parties to perform any particular services, but there is a sense in which each party relies on the other to meet minimum network security standards.[154] One of the conditions for any party of entering into a credit card network relationship is the belief that all of the commercial parties involved will take efforts to secure the network from data breaches. If the mechanic who services a machine as a condition of the sale can be liable to the buyer in negligence, a bank, merchant, or card brand that supplies network security as a condition of every other party's participation in the network might be liable in negligence as well.

However, the use of the term "condition" here—a term that does not appear in the illustrations to the proposed *Restatement (Third)* we have been discussing—complicates the analysis. In the mechanic's case (Illustration 5 discussed *supra*), for example, it is unclear why the buyer should not be required to specify the mechanical services as a condition of the sale and obtain a warranty and indemnity or otherwise to agree on a sale price that reflects some degree of uncertainty about the efficacy of the seller's mechanic's work.

If there is an answer to this question, in economic terms, it must relate to the extent to which there are any externalities imposed by the transaction and if so, whether they are effectively internalized by contract. If the negligence would be hard to detect in a timely fashion, or the potential loss hard to account for or insure against efficiently by agreement, negligence law could perhaps fill the gap. Many of the examples noted above are cases in which courts have recognized a "special relationship" of a fiduciary or quasi-fiduciary nature between the tortfeasor and the damaged party.[155] These have included cases involving, for example, auditors, surveyors, inspectors, engineers, attorneys, notaries public, architects, weighers, and telegraph companies.[156] These are circumstances under which ordinary contract principles sometimes do not apply because one party is in a position to have special knowledge or power that the other party does not possess. These kinds of asymmetries in information or power are precisely the sorts of circumstances that are likely to produce externalities.[157]

154. For a discussion of credit card payment systems as "weakest link" networks in terms of security, see *infra*, Part III.B.3.

155. *See* People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107 (N.J. 1985).

156. *See id.* at 117–18 and cases cited therein.

157. *See, e.g.*, Sujit Chakravorti, *Externalities in Payment Card Networks: Theory and Evidence*, FED. RES. BANK OF CHI., POL'Y DISCUSSION PAPER 2009-8, at 3 (Nov. 18, 2009), https://www.chicagofed.org/publications/policy-discussion-papers/2009/pdp-8.

Data breaches involving consumer credit cards can also resemble the three-cornered construction disputes referenced in Comment b. to Section 6 of the proposed *Restatement (Third)* when a third-party payment processor is involved. The third-party payment processor has a contractual relationship with the merchant and/or the acquiring bank but does not have contractual relationships with the issuing bank, the cardholder, or any other party such as a credit union card issuer. Once again, the economic issue is whether any externalities imposed by the payment processor's negligence are internalized by contract. The fact that the injured parties are not in contractual privity with the payment processor suggests a default tort liability rule might be appropriate.

C. The Externalities of Consumer Credit Card Data Breaches

So what are the externalities, if any, of a data breach involving consumer credit card information, and how difficult are they to account for by agreement? As we have seen, most of the recent high profile data breach incidents that have resulted in mass tort litigation arose in the "big box" retail context and involved the theft of consumer credit card data. A growing variety of cyber threats involve types of malware called "RAM scrapers" that are able to capture credit card stripe data housed temporarily in the random access memory of computer systems used by retailers to process payments.[158] This vulnerability made big box retailers who process enormous volumes of credit card transactions attractive targets for cyber criminals.[159]

As we have also seen, consumer credit card networks operate within a web of contractual relationships. These provisions in the Visa Core Rules appear to represent an extensive effort to adjust the risks of data breaches and fraud among all participants in the network. It is hard to imagine a clearer circumstance in which potential externalities are internalized by sophisticated parties. It seems, then, that the economic loss doctrine should bar tort claims between any of the parties for all costs relating to a data breach.

Nevertheless, something seems intuitively unsatisfying about this result. In the not too distant past, instances of identity theft and credit card counterfeiting were confined to discrete cases. Such activity has scaled exponentially with the advent of mass cybercrime. An important reason why is precisely because the credit card networks are *networks*.

158. *See* Brian Riley, *Ram Scraper Malware: Why PCI DSS Can't Fix Retail* (July 23, 2014), INFO. WK. DARK READING, http://www.darkreading.com/attacks-breaches/ram-scraper-malware-why-pci-dss-cant-fix-retail/a/d-id/1297501.

159. *Id.*

1. Network Externalities Generally

The consumer credit card networks, concentrated into two major providers (Visa and MasterCard), and three secondary providers (American Express, Discover, and Diners Club), comprise an essential component of the world's economic infrastructure. There are over two billion issued Visa cards worldwide and over one hundred fifty million transactions are processed over the Visa network every day.[160] As a primer on cyberdefense on Visa's website states, "[i]t is impossible to overstate the threat posed by cyber attacks . . . ."[161] Another video on Visa's website notes that the payment network "has got to be like a light switch—like electricity, like water" and "it's so important when we're talking about money, right, about people's lives."[162] If the consumer credit card system were compromised on a large scale, the negative spillover effects could be enormous.

The concentration of the card payment networks is a form of network externality.[163] A network externality arises when a network is valuable to users based not only on its features and performance, but also on its size.[164] A network externality can lead to lower investment in features and performance, including in the area of security. As Ross Anderson and Tyler Moore note, "[p]ut simply, while a platform vendor is building market dominance, it must appeal to vendors of complementary products as well as to its direct customers; not only does this divert energy that might be spent on securing the platform, but security could get in the way by

160. *See VisaNet: Catalyst for Commerce*, VISA (2013), https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/VisaNet-Network-Processing-Overview.pdf; *A day in the life of VisaNet*, VISA, https://usa.visa.com/about-visa/visanet.html (last visited Feb. 12, 2016); *VisaNet: by the numbers*, VISA https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-fact-sheet.pdf (last visited Feb. 12, 2016); VISA, *VisaNet—An Electronic Payment Processing Network*, YOUTUBE (Aug. 17, 2011), https://youtu.be/XntlmMj-Jyk.

161. Ellen Richey, *Breaking Down Barriers to Cyberdefense Through Congressional Action*, VISA, https://usa.visa.com/visa-everywhere/security/breaking-down-barriers-to-cyberdefense.html.

162. *VisaNet*, VISA, https://usa.visa.com/about-visa/visanet.html#1 (last visited Feb. 12, 2016).

163. *See* Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCI. 610, 611 (2006); Bruce J. Summers, *Fraud Containment*, ECON. PERSP., 1Q/2009, at 17, 18, https://www.chicagofed.org/digital_assets/publications/economic_perspectives/2009/ep_1qtr2009_part3_summers.pdf (stating that "[f]rom the perspective of economic analysis . . . payment systems and markets are thought of as special because they entail something called 'network effects' and 'two-sided' services, which are characteristic of public goods. Payment markets, moreover, may not always function like perfect markets because of the presence of 'externalities . . . .'").

164. *See* Anderson & Moore, *supra* note 163.

making life harder for the complementers."[165] In fact, there has been significant antitrust litigation relating to the credit card networks, which suggests that the system as a whole entails public goods issues.[166]

In the early and mid-1980s, there were two significant private antitrust cases against Visa.[167] In the first case, a third-party payment processor, NaBanco, unsuccessfully challenged Visa's interchange fees.[168] The trial court upheld these fees under the rule of reason, and the judgment was affirmed by the Court of Appeals for the Eleventh Circuit.[169] The second case arose after Sears, Roebuck and Co. began issuing its own card, the Discover Card, while also seeking to offer cards within the Visa network through an affiliate.[170] Visa had adopted a rule that excluded from the Visa network the affiliates of firms that offered cards "deemed competitive" to Visa.[171] A jury found that this restriction violated antitrust law, and the verdict was upheld by the trial court.[172] The Court of Appeals for the Tenth Circuit, however, reversed the verdict, finding that there was insufficient evidence to establish that Visa's exclusionary rule unlawfully precluded entry of new credit card bands into the general credit card market.[173]

The *NaBanco* and *MountainWest* cases, however, were not the last word on antitrust in the credit card industry. The U.S. Department of Justice brought a civil antitrust case against Visa and MasterCard in 2000, and in early 2015 the Justice Department along with the Attorneys General of seventeen states brought another civil antitrust case against Visa, MasterCard, and American Express.[174]

In the 2000 case, the Justice Department alleged that some of Visa and MasterCard's governance rules and exclusionary practices violated section 1 of the Sherman Anti-Trust Act.[175] Most significantly for the purpose of

165. *Id.* Anderson and Moore suggest that "platform vendors commonly ignore security in the beginning, as they are building their market position; later, once they have captured a lucrative market, they add excessive security in order to lock their customers in tightly." *Id.*

166. *See* Dennis W. Carlton & Alan S. Frankel, *The Antitrust Economics of Credit Card Networks*, 63 ANTITRUST L.J. 643, 667 (1995).

167. Nat'l Bancard Corp. (NaBanco) v. VISA U.S.A., Inc., 596 F. Supp. 1231 (S.D. Fla. 1984), *aff'd*, 779 F.2d 592 (11th Cir. 1986); SCFC ILC, Inc., v. VISA U.S.A., Inc., 819 F. Supp. 956 (D. Utah 1993), *aff'd in part, rev'd in part*, 36 F.3d 958 (10th Cir. 1994).

168. *NaBanco*, 596 F. Supp. at 1263.

169. Nat'l Bancard Corp. (NaBanco) v. VISA U.S.A., Inc., 779 F.2d 592, 605 (11th Cir. 1986).

170. SCFC ILC, Inc., v. VISA U.S.A., Inc., 36 F.3d 958, 961 (10th Cir. 1994).

171. *Id.*

172. *SCFC ILC, Inc.*, 819 F. Supp. at 990.

173. *SCFC ILC, Inc.*, 36 F.3d at 963–72.

174. United States v. Visa U.S.A. Inc., 163 F. Supp. 2d 322 (S.D.N.Y. 2001), *aff'd*, 344 F.3d 229 (2d Cir. 2003); United States v. Am. Express Co., 88 F. Supp. 3d 143 (E.D.N.Y. 2015).

175. *U.S. v. Visa*, 163 F. Supp. 2d at 327.

this Article, after a thirty-four day trial, the district court found that there were significant barriers to entry in the relevant product markets and that both Visa and MasterCard possessed market power.[176] The Court of Appeals for the Second Circuit subsequently affirmed these findings.[177]

In the 2015 case, the Justice Department and the States alleged that the card networks' "anti-steering" rules violated section 1 of the Sherman Anti-Trust Act.[178] These rules prohibited merchants from steering customers towards a competitor's cards through advertising, discounts, or otherwise.[179] Visa and MasterCard entered into consent decrees prior to trial, but American Express and a related entity, American Express Travel Related Services Company, elected to litigate.[180] After a lengthy trial, the court found that American Express' "anti-steering" rules violated the Sherman Anti-Trust Act.[181] Again, the most significant part of this decision for the purpose of this Article is the court's treatment of market definition and market power. American Express argued that the separate "network services" and "card" markets defined in the 2000 *Visa* case should be collapsed into a single, larger market.[182] The court rejected this argument and reiterated the approach in the 2000 *Visa* case that card network services is a separate product market.[183] The court further found that, "[d]efendants enjoy significant market share in a highly concentrated market with high barriers to entry and are able to exercise uncommon leverage over their merchant-consumers due to the amplifying effect of cardholder insistence and derived demand."[184] The court noted that the network services market remained highly concentrated with significant entry barriers despite the fifteen years that had passed between the decisions"[185] In particular, the court found, "American Express is one of only four major suppliers of GPCC card network services, and three of the competitors in this market (Visa, American Express, and MasterCard) are significantly larger than the fourth (Discover)."[186] The court further found that new digital payment methods, including PayPal, Square, and Google Wallet had not diluted the

176. *Id.* at 335, 341–42.

177. United States v. Visa U.S.A. Inc., 344 F.3d 229, 238–39 (2d Cir. 2003).

178. *U.S. v. Am. Express*, 88 F. Supp. 3d at 149.

179. *See id.* at 149–50.

180. *Id.* at 149.

181. *Id.* at 150–51.

182. *Id.* at 171–72.

183. *Id.* at 173–74.

184. *Id.* at 188. "Cardholder insistence" is the notion that cardholders insist that merchants accept certain cards, including American Express. *See id.* at 191. In more traditional antitrust economics terms, it is a kind of network effect.

185. *Id.* at 189.

186. *Id.*

major networks' market power, but rather "piggyback on existing methods of payment."[187]

These findings concerning market definition and market power in both the 2000 and 2015 credit card network antitrust cases, of course, were hotly contested. Nevertheless, the consensus in the academic literature concerning credit card network economics is that the industry is highly concentrated and entails high barriers to entry due to network effects.[188]

2. Network Externalities Relating to Fraud and Liability Protection

Sujit Chakravorti, a senior economist with the Federal Reserve Bank of Chicago, has identified multiple kinds of potential externalities in payment card networks, including externalities relating to card adoption and usage, merchant competition, instrument-contingent pricing, network competition, surplus from revolvers, merchant fees and consumer credit, competition among payment instruments, and dynamic efficiency and innovation.[189] Most significantly for our purposes, Chakravorti notes that there are potential externalities relating to "payment fraud and liability" in card networks.[190]

The potential network externalities of fraud and liability shifting, Chakravorti observes, "ha[ve] received little attention in the payment network literature."[191] He briefly identifies two problems: (1) the zero liability policy could result in consumers taking inadequate fraud precautions; and (2) individual merchants and payment processors might not have adequate incentives to take precautions, and "while the cost of not protecting payment information for an individual entity may be small, its impact on the system as a whole may be significant."[192] Chakravorti notes that the proposed solutions to these problems by industry participants have included better enforcement of existing fraud laws and greater adoption of voluntary industry-wide security standards.[193] Other commentators, Chakravorti states, have suggested the promulgation of authoritative standards by governments, voluntary or mandatory information sharing

187. *Id.* at 190.

188. There is robust debate in the literature, however, concerning whether specific industry policies, such as the charging of interchange fees, have anticompetitive effects. *See, e.g.*, Chakravorti, *supra* note 157, at 3 (stating that "[t]o date, there is still little consensus—either among policymakers or economic theorists—on what constitutes an efficient fee structure for card-based payments").

189. *Id.* at 5–20.

190. *Id.* at 18.

191. *Id.*

192. *Id.* at 18–19.

193. *Id.*

concerning breach incidents, and governmental response plans for wide-scale fraud.[194]

Stacey Schreft, an economist with the Federal Reserve Bank of Kansas City, has similarly noted that, although perfect security is unobtainable without destroying the social value of electronic payment systems, market forces alone cannot achieve an efficient amount of security.[195] Schreft argues that, "[b]ecause asymmetric information and externalities are associated with the transfer and use of PII in making payments, the full cost of an act of identity theft will not be borne by those best positioned to prevent the theft, giving them too little incentive to protect against the crime."[196] Schreft further states that, "payment system integrity and efficiency are public goods—goods that markets tend to underproduce even in the absence of identity theft."[197]

One of the market failures Schreft identifies in relation to identity theft results from asymmetric information.[198] Schreft suggests that, "[a]symmetric information prevents customers from differentiating between sellers based on security practices. This forces customers instead to make purchase decisions based on their expected degree of data security across sellers, discounting purchases from all sellers by the same expected cost from misuse of PII."[199]

Asymmetric information seems to be less of a problem in credit card payment networks because the industry has voluntarily adopted the PCI-DSS standard. Anyone who is interested can learn that PCI-DSS is the industry standard and can research what kind of security it provides. Nevertheless, as we have seen, some of the recent large-scale retail data breaches involve claims that one party or another in the network failed to follow all the requirements of PCI-DSS. It is difficult, if not impossible, for any one party in the network to know with any degree of certainty whether another party is *in fact* complying with the agreed-upon standard.

This problem is linked to network externalities, which Schreft also identifies as a market failure in connection with the provision of information security, particularly in credit card networks.[200] As Schreft notes,

194. *Id.*

195. Stacey L. Schreft, Fed. Reserve Bank of Kansas City, *Risks of Identity Theft: Can the Market Protect the Payment System?*, ECON. REV., 4Q/2007, at 5, 22, https://www.kansascityfed.org/~/media/files/publicat/econrev/econrevarchive/2007/4q07schreft.pdf.

196. *Id.*

197. *Id.*

198. *Id.* at 23.

199. *Id.* at 24.

200. *Id.* at 25.

> [n]etworks can adopt policies that impose minimum security practices or contractually assign liability for data breaches to improve within-network investment in security, but a network's security will still be too lax if the network's own breaches can impose losses on entities outside the network, including other networks, and the network does not bear the cost of those losses.[201]

This problem is particularly compounded because in terms of security, payment system networks are "weakest link" networks.[202] As Schreft argues, "[a] network's security is only as effective as the security of the weakest link—the participant most likely to experience a data breach."[203] These externalities, Schreft concludes, pose risks to the integrity and efficiency of the payment system.[204]

Schreft uses the TJX breach as an example of a case in which a retailer's failure to employ adequate security imposed externalities on banks, with estimated costs of more than $1 billion.[205] Although Schreft mentions that a class action lawsuit was filed by the banks, her paper was published before the case was resolved. In fact, the claims against TJX that were litigated were rejected by the district court under both negligence and contractual third-party beneficiary theories.[206] The Court of Appeals for the First Circuit affirmed all of these rulings, including the dismissal of the basic negligence claim under the economic loss doctrine, but reversed and remanded a negligent misrepresentation claim based on a recent case the district court may have overlooked.[207] The First Circuit noted that "the [negligent misrepresentation] claim thus survives but on life support."[208] The parties subsequently settled.[209]

Schreft acknowledges that the parties in credit card networks can contractually assign liability among themselves, but she thinks that this cannot provide a comprehensive solution because "many system participants have access to customer payment data between the point of sale and final settlement, and few of them can anticipate their ultimate ties to each other and enter into contractual agreements that allocate the risk of

201. *Id.* at 5, 25.

202. *See* Hal R. Varian, *System Reliability and Free Riding*, *in* ECONOMICS OF INFORMATION SECURITY 1–15 (L. Jean Camp & Stephen Lewis eds., 2004).

203. Schreft, *supra* note 195, at 25.

204. *Id.* at 26.

205. *Id.* at 25–26.

206. *See In re* TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83, 90–91 (D. Mass. 2007), *aff'd in part and vacated in part*, 564 F.3d 489 (1st Cir. 2009).

207. *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 501–02 (1st Cir. 2009).

208. *Id.* at 495.

209. *See In re TJX Cos. Retail Sec. Breach Litig.*, 584 F. Supp. 2d at 410 (approving class counsel fees).

harm from others' data security failures."[210] Schreft therefore concludes that public policy should require greater disclosure requirements, a public insurance scheme to secure the integrity of the system, and "the clear and comprehensive assignment of liability to address externalities."[211]

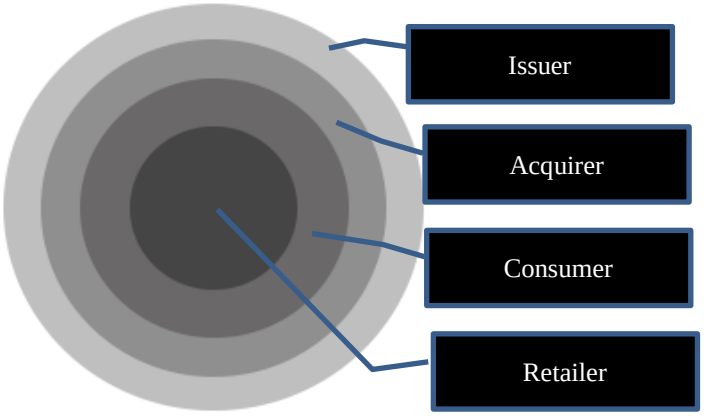
Schreft's examination of data security risks in the payment system is among the most comprehensive in the economic literature. Still, it is unclear whether she adequately accounts for the extensive web of contractual rights and duties that already encompass all parties in the major credit card networks. When she discusses the contractual allocation of liability, Schreft seems to have in mind some sort of individualized negotiations focused on the specific practices of individual players. The transaction costs entailed by such a requirement would grind the payment system to a halt. This is why the operating regulations of the major networks employ generally applicable standards with liability shifting and arbitration provisions. But by highlighting the weakest link and systemic externality problems inherent in payment system security, Schreft shows why contractual risk management provisions between the four immediate players in a consumer credit card transaction will not internalize all of the externalities inherent in the risk of a data breach.

3. Network Externalities and Distributed Networks

The problem of security-related network externalities is further compounded in the consumer credit card networks because the networks are widely scaled and distributed. The following diagram illustrates the externalities imposed on the other members of a credit card network by a retailer's failure to enact adequate data security, resulting in a consumer credit card information breach:

210. Schreft, *supra* note 195, at 28.

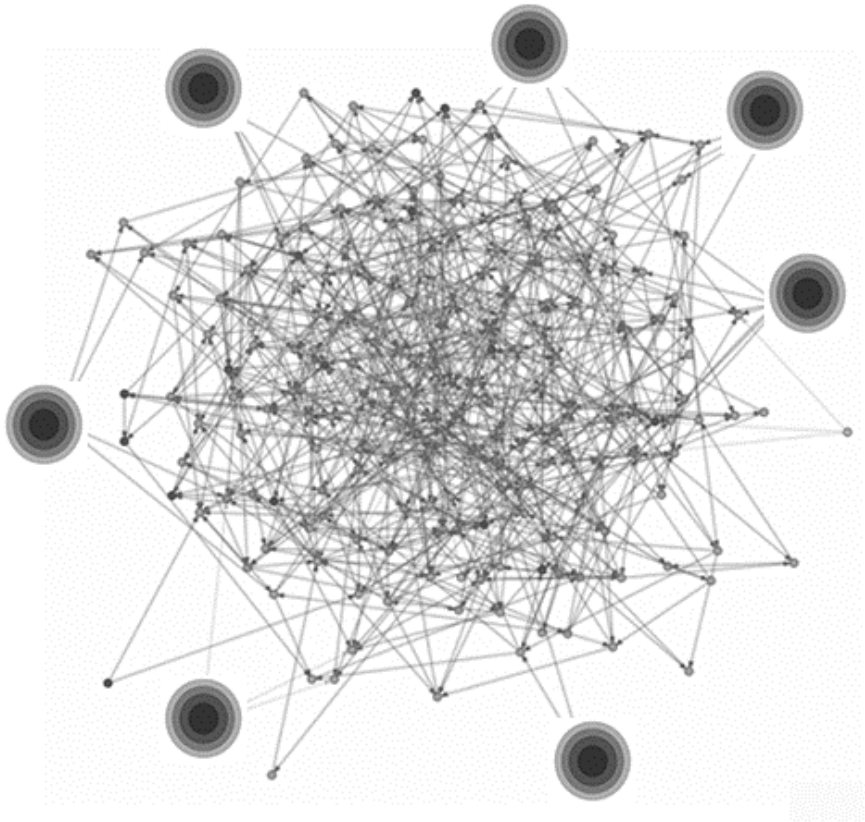
211. *Id.* at 30.



The retailer's failure to employ adequate security imposes costs on the consumer whose cardholder information is compromised. Costs are then imposed on the acquirer in the form of transaction costs and on the issuer in the form of transaction and cardholder reimbursement costs. If the retailer in fact failed to implement PCI-DSS as required by the card network agreement regulations, all these layers will collapse back onto the retailer. If the retailer complied with its requirements under the card network regulations, these layers will explode outward onto the issuer.

If this was the whole story, a robust contractual network might be the entire answer. We need to think of the credit card payment system, however, not only in terms of individual transactions, but as a distributed network. Imagine millions of these nested diagrams as nodes on an enormous distributed network:[212]

212. S. Kochemazov & A. Semenov, *Using Synchronous Boolean Networks to Model Several Phenomena of Collective Behavior*, WIKIMEDIA COMMONS (image modified), https://commons.wikimedia.org/wiki/File:Using-Synchronous-Boolean-Networks-to-Model-Several-Phenomena-of-Collective-Behavior-pone.0115156.s003.ogv (last visited Feb. 12, 2016); *see* Stepan Kochemazov & Alexander Semenov, *Using Synchronous Boolean Networks to Model Several Phenomena of Collective Behavior*, PLOS ONE 23–25 (Dec. 19, 2014), http://www.plosone.org/article/fetchObject.action?uri=info:doi/10.1371/journal.pone.0115156&representation=PDF. The intent of this graphic is illustrative and does not represent any actual network.



As individual nodes implode or explode, the potential exists for the entire system to become destabilized. Of course, one of the benefits of nodal networks is that they are to a great extent self-healing. If an individual node is destroyed, the system still maintains resiliency. But if large numbers of nodes are compromised in the same way at the same time, the effects could amplify across the entire network and the system could collapse. Think, for example, of a neural network such as the human brain. If we lose a few neurons, the system will likely find ways to compensate. If a small region of the brain is malfunctioning, other parts may be co-opted to compensate. There comes a point, however, at which damage is sufficiently large or extensive that a cascade of failures results and the entire organ is severely compromised or fails.[213]

These thought experiments illustrate why the metaphor of a "stream" of causality breaks down in a distributed nodal network. There is no "stream" of causality, but rather a non-linear "web" of causes and effects,

213. *See, e.g.*, *Types and Levels of Brain Injury*, BRAIN INJURY ALLIANCE UTAH, http://biau.org/types-and-levels-of-brain-injury/ (last visited Feb. 12, 2016).

running backward and forward, up and down, in and out, under and around.[214] In one sense, this should make the duty/proximate cause/economic loss analysis easier: outside the immediate "proximity" of the breach, determining the probability of loss with any reasonable certainty might prove impossible. In another sense, however, the difficulty of showing which affected parties are "upstream" and which are "downstream" of something like the Michigan Avenue Bridge could mean that tort law cannot perform its traditional functions of deterring excessively risky conduct, encouraging risk mitigation strategies, and adjusting the social costs of externalities.

4. Network Externalities and Weakest Link Networks

Economist Hal Varian explored these issues in a 2004 paper on "System Reliability and Free Riding."[215] Varian suggested a taxonomy that included three kinds of networks in connection with system reliability:

Total effort. Reliability depends on the sum of the efforts exerted by the individuals.

Weakest link. Reliability depends on the minimum effort.

Best shot. Reliability depends on the maximum effort.[216]

Varian illustrated this taxonomy with reference to a walled city: there may be one wall and the city's defense may depend on the sum of the efforts of its builders; there may be a wall of varying height, and the city's defense may depend on the wall's viability at its lowest point; or there may be multiple walls but only the highest wall is the final line of defense.[217]

Data security in computer networks can resemble any of these sorts of networks at various points in the system. At a larger scale, however, most computer data systems are "weakest link" networks. This is why so many reported data breaches involve "stupid" mistakes, such as individual employees losing or improperly discarding unencrypted storage media, lax password policies, unintentional software "backdoors," and the like.[218]

Varian examined each of the three types of networks in his taxonomy from a game-theoretic perspective. He concluded that systems will become

214. *See* Anderson & Moore, *supra* note 163, at 613 ("Computer networks from the Internet to decentralized peer-to-peer networks are complex but emerge from ad hoc interactions of many entities using simple ground rules. This emergent complexity, coupled with heterogeneity, is similar to social networks and even to the metabolic pathways in living organisms."); MacCarthy, *supra* note 19, at 8 (noting that, in a credit card data breach, "[d]amage is not contained at one node of the payment network but affects other nodes").

215. Varian, *supra* note 202, at 1–15.

216. *Id.* at 1.

217. *Id.*

218. *See, e.g.*, VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT (2015), http://www.verizonenterprise.com/DBIR/2015/.

"increasingly unreliable as the number of agents increases in the weakest link case."[219] This is not a surprising conclusion, as it is consistent with standard economic intuitions about agency costs and moral hazard.[220] Varian concludes that the optimal way to mitigate this risk, in asymmetric cases (where the parties' value and costs for security differ), is to impose a negligence rule.[221] The standard of care, Varian suggests, could be determined by the courts but might more efficiently be determined through insurance underwriters.[222]

This analysis might suggest that the economic loss doctrine should not bar negligence claims in consumer data breach cases. It is possible, however, to view the credit card networks as self-insuring systems. The network agreements already distribute liability based on a standard of care—the use of PCI-DSS and the presentment and authentication requirements for in-person transactions.

There are a number of problems with this analogy. First, the consumer is insured absolutely without regard to any standard of care. Second, the "underwriting" requirements may not be stringent enough, as evidenced by the prevalence of large scale breaches despite the network requirements. Moreover, as a related concern, the networks do not operate as objective insurers, but in fact possess market power and sometimes may act anti-competitively. Finally, there is a joker in the deck, which we have not yet closely examined—the widespread use of third-party payment processors that are not original parties to the payment network. We turn take a closer look at this joker in the next Part.

D. Third-Party Payment Processors

As described in Part II *supra*, in the case law, and the legal and economic literature, credit card payments typically involve three or four parties—the card network provider (such as Visa), the card customer, and one or two banks (the issuer and acquirer), all of which are part of a web of contractual relations. The "typical" scenario, however, might in fact more often be complicated by the presence of one or more non-bank entities, in addition to the card networks, in the payment processing chain. The *Heartland* breach discussed in Part II *supra* is an example of a case involving a third-party payment processor.[223] As noted in the summary of

219. Varian, *supra* note 202, at 7.

220. *See, e.g.*, Schreft, *supra* note 195.

221. Varian, *supra* note 202, at 10.

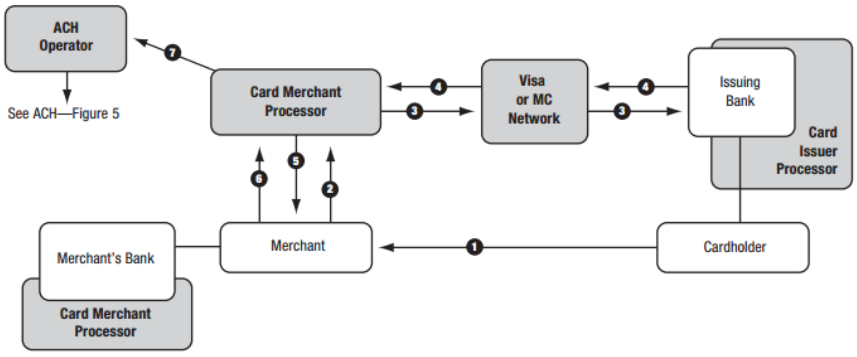
222. *Id.*

223. *See In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566 (S.D. Tex. 2011), *rev'd in part sub nom.*, Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013).

that case, on the record before it, the Fifth Circuit was unable to make any clear findings about Heartland Payment Systems' liability.

In a recent report, the Federal Reserve Bank of Kansas City noted that, "[n]onbanks are pervasive in the U.S. payment system."[224] In addition to the credit card networks themselves, the Report includes numerous other nonbank activities relating to the credit card payment chain, such as fraud system vendors, online transaction security systems, hardware providers, software providers, card-issuer processors, card merchant processors, internet banking platform providers, and P2P internet payment providers.[225] According to the Report, "[o]ne of the largest card-related activities is card-issuer processing," and "[t]wo nonbanks, First Data and TSYS, dominate this market."[226] The Report states that First Data has more than 300 million accounts and TSYS has more than 250 million accounts, and that together they provide processing services for nearly forty percent of all credit card accounts.[227]

Third-party payment processors such as First Data can provide services for the merchant and/or issuer in transactions that travel over the card brand network (for example, the VISA network). The following illustration from the 2003 Federal Reserve Report illustrates this type of transaction:[228]



224. Terri Bradford, Matt Davies & Stuart E. Weiner, NONBANKS IN THE PAYMENTS SYSTEM 1 (Federal Reserve Bank of Kansas City 2003), https://www.kansascityfed.org/~/media/files/publicat/psr/bksjournarticles/nonbankpaper.pdf.

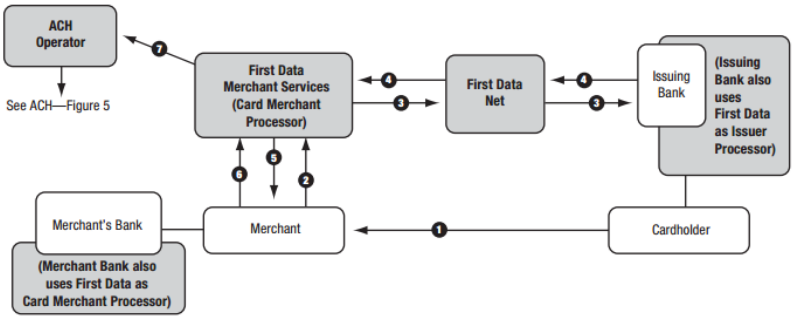
225. *Id.* at 5–6. Significant companies listed in the Report in these categories include Thomson Financial (http://thomsonreuters.com/en/products-services/financial.html), Bridger Systems (http://www.lexisnexis.com/risk/products/bridger-insight.aspx), Diebold (http://www.diebold.com/), Fiserv (https://www.fiserv.com/index.aspx), First Data (https://www.firstdata.com/en_us/home.html), TSYS (http://tsys.com/), Concord (http://www.concordmerchant.com/index.php/content/payment/), Paypal (https://www.paypal.com/home), and others.

226. *Id.* at 8.

227. *Id.*

228. *Id.* at 24.

Third-party processors can also provide network services in lieu of the card brand's network.[229] The following diagram from the 2003 Federal Reserve Report illustrates this type of transaction utilizing the First Data Network:[230]



In its most recent 10-K filing, First Data states that it provides services to merchants in approximately 3.9 million locations throughout the United States and that it "acquired $1.7 trillion of payment transaction dollar volume on behalf of U.S. merchants in 2014."[231] In its 2014 Annual Report, TSYS states that it processed 17.8 billion transactions in 2014, including thirty-five percent of the purchase volume within the top-50 U.S. Visa and MasterCard issuers.[232] In the "Risk Factors" portion of its 10-K, First Data notes that, "we process and store sensitive business information and personal consumer information in order to provide our services" and that "our position in the global payments industry may attract hackers to conduct attacks on our systems that could compromise the security of our data. In addition, the increasing sophistication level of cyber criminals may increase the risk of a security breach of our systems."[233]

The importance of third-party payment processors obviously increases the risk of failure in a "weakest link" network. As a joint report of the European Central Bank Oversight Division and Federal Reserve Bank of Kansas City report notes, the prevalence of nonbank payment processors,

229. *Id.* at 23.

230. *Id.* at 25.

231. FIRST DATA CORP., UNITED STATES SECURITIES AND EXCHANGE COMMISSION FORM 10-K, at 5 (2014), http://investor.firstdata.com/phoenix.zhtml?c=111215&p=irol-reportsannual.

232. TSYS, 2014 ANNUAL REPORT, at iii (2014), http://tsys.com/annual-report.html.

233. *Id.* at 16.

> involves a . . . complex mechanism with a multiplicity of contact points and the dissemination of sensitive data at various points along the processing chain, and the consequent vulnerability to risks in terms of data security and data (privacy) protection [at] any interaction point can be, in itself, a weak point in the chain suitable to being exploited by a criminal to intrude the payment network for illicit purposes.[234]

This increased level of complexity and risk necessarily leads to increased concern about externalities.

D. The Role of Commercial Cyber Risk Insurance

Like Varian, Anderson and Moore note that insurance is likely an effective way of identifying and managing software security risk in the face of network and other externalities.[235] Insurance underwriters would assign premiums based on the firm's overall IT infrastructure and management, including security.[236] The underwriting process, over the long run, would create a pool of data and best practices, which would enable cyber risks to be valued and managed more accurately.[237] However, when Anderson and Moore published their paper in 2006, there was not yet a mature cyber risk insurance market.[238] One of the reasons the insurance market had not matured was the uncertainty of legal standards for liability relating to defective, insecure software.[239]

Many of these uncertainties remain. A recent Department of Homeland Security ("DHS") insurance industry roundtable noted three impediments to the growth of cyber risk insurance:

- The lack of a secure method for pooling and sharing anonymized cyber incident information that could be made accessible to carriers and risk management professionals;
- The need for more robust cyber incident models and simulations that could inform underwriting risk factors for particular organizations; and

234. Stuart Weiner, et al., *Nonbanks and Risk in Retail Payments* 22 (Joint ECB-Bank of Eng. Conference on Payment Sys. and Fin. Stability, Working Paper No. 07-02, 2007), http://weis2008.econinfosec.org/papers/Sullivan.pdf.

235. Anderson & Moore, *supra* note 166, at 612.

236. *Id.*

237. *Id.*

238. *Id.*

239. *Id.*; *see also Examining the Evolving Cyber Insurance Marketplace*: *Hearing Before the S. Subcomm. on Consumer Prot., Prod. Safety, Ins. and Data Sec.*, 114th Cong. (2015) (testimony of Michael Menapace), http://www.commerce.senate.gov/public/_cache/files/90fa0bc7-8686-4b90-9a1b-3525cc62d4fe/8A982AD17B40EDD0101AD5974A36AD73.menapace-testimony-for-senate-hearing-on-cyber-insurance.pdf.

- The need for companies of all sizes to adopt enterprise risk management programs that incorporate cyber risk.[240]

Concerning this final point, the DHS report noted that cybersecurity is often not seen as a matter for enterprise risk management because of "a cultural divide that exists between CISOs on the one hand and chief financial officers, legal counsel, and risk managers on the other."[241] The industry participants in the DHS roundtable suggested that, until cyber risks are understood to present "potential harm to investment, market cap, and reputation, most companies will have difficulty elevating responsibility for cyber risk management beyond their IT departments."[242]

One of the classic economic functions of the tort system is to encourage risk spreading through insurance.[243] If principles such as the economic loss doctrine limit an actor's responsibility for the externalities it imposes through lax cybersecurity, this function could be frustrated. On the other hand, if a network already spreads risks through what amount to contractual forms of self-insurance, a tort remedy will prove redundant and will only increase other social costs. The next Part examines this question in the context of consumer credit card data breaches.

IV. APPLYING REGULATORY AND TORT THEORY TO THE ECONOMIC LOSS DOCTRINE IN CONSUMER CREDIT DATA BREACH CASES

The discussion of externalities above raises the question of whether the tort system can provide useful tools for mitigating systemic cybersecurity risk. This question lies at the heart of debates over the function of private litigation as a regulatory tool.[244] Even more broadly, it raises the fundamental question of whether a system such as the credit card payment

240. DEP'T OF HOMELAND SEC., INSURANCE INDUSTRY WORKING SESSION READOUT REPORT, INSURANCE FOR CYBER-RELATED CRITICAL INFRASTRUCTURE LOSS: KEY ISSUES 1–2 (2014), http://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf.

241. *Id.* at 2.

242. *Id.* at 3.

243. *See* SHAVELL, *supra* note 7, at 51–57 (generally explaining the importance of insurance in an accident and liability system).

244. *Cf., e.g.*, SEAN FARHANG, THE LITIGATION STATE: PUBLIC REGULATION AND PRIVATE LAWSUITS IN THE U.S. 60 (2010) ("These findings link long-run historical patterns of divided government and legislative-executive polarization, which increased in frequency and intensity starting in the late 1960s, with the coincident growth of the role of litigation and courts in the implementation and elaboration of federal statutory policy."); David Freeman Engstrom, *Agencies as Litigation Gatekeepers*, 123 YALE L.J. 616, 619 (2013) ("One of the most controversial developments in the American regulatory state in recent decades is a marked shift away from administrative regulation and enforcement and toward the use of private lawsuits as a regulatory tool.").

network requires external regulation *at all* in relation to systemic threats. After all, the network already contractually requires a presumably state-of-the-art security standard (PCI DSS), indemnifies innocent consumers who are victims of fraud, and spreads risk among the participating banks.

A. Investment, Not Regulation?

Some commentators, including Professor Derek Bambauer, addressing the question of "cybersecurity" broadly, suggest that a relatively hands-off approach is best. Bambauer argues that, "[t]he Internet is designed for exactly the challenge that cyber-attacks produce: disruption to segments of the network that force re-routing of data, with the concomitant risk of lost information."[245] Bambauer notes that the robust, redundant, self-healing nature of the Internet makes major, persistent service outages from cyber attacks unlikely.[246] For Bambauer, cybersecurity is an "information" problem, and he defines "information" as "something that users seek to access or engage with."[247] Cybersecurity is only a problem, Bambauer suggests, when users are unable to access "information." But cybersecurity regulation that decreases user access to "information" is counterproductive.[248] Bambauer, therefore, suggests a minimal suite of cybersecurity rules focused on data redundancy and recovery rather than breach prevention.[249]

There are both confusing and helpful elements to Bambauer's proposal. One of the most significantly confusing elements is Bambauer's definition of "information." In contrast to much of the literature in the philosophy of information, Bambauer focuses not on semantic content to define "information," but on a "user's" action in seeking to "access" or "engage" with something. There are plenty of elements of a communications system that a user may wish to "access" or "engage with," however, that should not be considered "information." Most significantly, this would include the physical "tubes" that Bamabauer previously defined

245. Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 613 (2011) (citing Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 64).

246. *Id.* at 617.

247. *Id.* at 622–25. Oddly, just before moving into his "information" policy paradigm, Bambauer cites Senator Ted Stevens' definition of "the Internet" as "a series of tubes." *Id.* at 621. In fact, it is best to think of the Internet as a multi-layered communications network, incorporating physical (tubes), communication, and code layers. *See, e.g.*, David W. Opderbeck, *Deconstructing Jefferson's Candle: Towards a Critical Realist Approach to Cultural Environmentalism and Information Policy*, 49 JURIMETRICS 203 (2009); David W. Opderbeck, *The Penguin's Genome, or Coase and Open Source Biotechnology*, 18 HARV. J. L. TECH. 167 (2004) [hereinafter Opderbeck, *The Penguin's Genome*].

248. *See* Bambauer, *supra* note 245, at 635–36.

249. *Id.* at 636–53.

as "the Internet." Whenever a user goes online, he or she seeks access to routers, cables, switches, and so on. This "physical layer" of the Internet is not itself "information" and may require its own appropriate level of "cybersecurity" that might differ from what is applicable to the "communications" and "code" layers.[250]

This problem is evident if we try to apply Bambauer's solution to the large-scale consumer credit card data breach problem confronted in this Article. A massive consumer data breach neither disrupts the physical layer of the network nor the communications layer. The consumer still retains her credit card data and can continue to make purchases. The code layer also remains intact. The network continues to function. But that functioning now entails significant additional costs because the thief is able to use the credit card data to obtain benefits from the network without providing corresponding benefits to the network.

A second confusing element of Bambauer's proposal is that his solutions are focused on maintaining *access* to "information" when he has already defined "information" in terms of "access." It seems, then, that Bambauer's proposal is circular, unless he is calling for the production of *more* information. In fact, the production of more information is indeed what Bambauer has in mind, since his proposal revolves around redundancy, and he suggests that governments should invest in the infrastructure required for large scale redundancy.[251] The cybersecurity problem, for Bambauer, is not about protecting existing bits and bytes of information, but rather about generating more and more copies of existing bits and bytes so that those bits and bytes are always available *somewhere*.

Again, the confusion is evident when this solution is applied to the retail data breach context. In that context, the problem is that *semantic content*, consumer credit card data, has been learned by a party who is not supposed to know that information and who can now use it to extract value from the system without providing a corresponding exchange of value. Redundancy will not solve this problem—in fact it would exacerbate it. Indeed, one of the core principles of PCI DSS is to minimize the attack surface by severely *limiting* the storage of credit card data to the data sufficient to communicate the semantic content required to complete a transaction.[252]

250. *See* David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 837–44 (2012); David W. Opderbeck, *Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch?*, 65 FED. COMM. L. J. 1, 44–46 (2013).

251. *See* Bambauer, *supra* note 245, at 656–58.

252. *See* PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 64 (2015) https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf. In a section titled "PCI-DSS Requirement 7: Restrict access to cardholder data by business need to know," the Council

Finally, even if redundancy could help mitigate a particular risk, building out redundancy entails significant costs. Bambauer acknowledges that, "the vast majority of network infrastructure in the U.S. is privately owned," and he does not argue that this infrastructure should be forcibly de-privatized.[253] Rather, he advocates a taxpayer-funded government subsidy of private backbone providers.[254] It is hard to see the economic efficiency or fairness in a plan that would spread the network externalities generated by private Internet backbone providers among the general tax base. Certainly such a plan would not encourage the network providers to internalize those externalities by adopting more efficient *preventative* cybersecurity, unless the subsidies also came with regulation that effectively transfers control over the networks, and thereby control over the Internet, to the U.S. government. Without a government takeover of the network and/or stronger preventative cybersecurity, Bambauer's plan would seem to result in a public subsidy of cyber crime that would scale exponentially along with network growth and that would quickly become unsustainable for the tax base.[255]

In short, without any direct reference to externality theory, Bambauer effectively suggests that the externalities of cybersecurity should be borne by everyone (at least everyone in the U.S., since his solution is U.S.-centric) through taxpayer-funded subsidization of the bandwidth required for data redundancy, without regard to whether redundancy will solve a particular problem such as consumer data breaches.[256] Although there is something romantic about the science fictional notion of the Internet as a self-healing organism that can be nurtured through public care and feeding without much concern about preventative medicine, the realities seem much harsher.[257]

---

states that, "The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice." *Id.*

253. *See* Bambauer, *supra* note 245, at 657–662.

254. *Id.* at 658–59.

255. Perhaps in some sense this would provide a desirable result. The network build-out required to increase redundancy as cybercrime escalates could have positive spillover benefits insofar as the increased capacity could be used for other purposes in addition to redundancy in response to cybercrime. It seems highly unlikely, however, that these positive spillovers would equal or exceed the costs of the subsidy. Moreover, generating positive spillovers from crime produces the significantly negative effect of reducing respect for the rule of law.

256. *See supra* note 245.

257. For an explicit connection between cybersecurity and the science fiction literature on cyberspace, see the abstract to Prof. Bambauer's article *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014). In that paper, Prof. Bambauer extends his argument that to promote cybersecurity, "[t]he federal government should use bribes to lure firms to implement disaggregation and heterogeneity – to divide and differ." *Id.* at 1062. (By "bribe" here he means a public grant.) He

B. Public Goods Infrastructure Regulation?

In his recent work on cybersecurity regulation, Nathan Sales has recognized that cybersecurity presents a classic regulatory problem.[258] In particular, Sales notes that, "cyber-security resembles environmental law in that both fields are primarily concerned with negative externalities."[259] Sales argues that "[j]ust as firms tend to underinvest in pollution controls because some costs of their emissions are borne by those who are downwind, they also tend to underinvest in cyber-defenses because some costs of intrusions are externalized onto others."[260] Sales further analogizes cybersecurity to public health regulation.[261] Just as infected individuals may impose negative externalities on others by spreading disease, computers compromised by malware may impose negative externalities on others by allowing the malware to spread.[262] This may suggest some sort of government-sponsored inoculation program.[263] Sales also thinks tort law can play a role by incentivizing actors in the network to take cyber precautions—that is, by forcing actors who create the risk of negative externalities to internalize those risks.[264]

But Sales recognizes that cybersecurity risk at best can be managed and not entirely avoided: "The optimal level of cyber-intrusions is not zero, and the optimal level of cyber-security expenditures is not infinity."[265] Sales presents a rubric for determining the range of possibilities for efficient levels of investment in cyber defense based on the "significance" of the target and the "sophistication" of the hacker.[266] Sales suggests that a combination of "significance" and "sophistication" that falls closer to the lower left area of his curve—that is, lower "significance" and lower "sophistication"—likely represents a level of investment in cybersecurity

---

also argues there that some key industries in critical sectors should be required to adopt data disaggregation and heterogeneity policies. *Id.* at 1065.

258. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U.L. REV. 1503 (2013).

259. *Id.* at 1508.

260. *Id.*

261. *Id.*

262. *Id.* at 1539–40.

263. *Id.* at 1440–41.

264. *Id.* at 1533–39.

265. *Id.* at 1511. Actually, the "optimal level of cyber-intrusions" would indeed be zero, and the optimal level of cyber-security expenditures likewise would be zero. That is, it would be best for society if nobody engaged in malicious cyber intrusions. What Sales likely means to say is that, given the reality that some people will engage in malicious cyber intrusions, the best response would have to take into account the costs of mitigation, the probability of harm, and the risk of loss. Given those factors, it is impossible with present technology to achieve zero risk of loss without imposing a grossly excessive burden in proportion to the probable loss.

266. *Id.* at 1516.

that is already socially optimal.[267] In other words, it is socially optimal for relatively insignificant targets that are subject to attacks by relatively unsophisticated hackers to invest only modestly in cybersecurity. A combination of "significance" and "sophistication" more towards the upper right of Sales' graph indicates that greater investment in cybersecurity is socially optimal.[268] In other words, it is socially optimal for relatively significant targets that are subject to attacks by relatively sophisticated hackers to invest more substantially in cybersecurity. Sales stops short, however, of suggesting that such investment should be required by government.[269] Instead, Sales argues in favor of private-public partnerships and some degree of governmental commitment of financial and other resources for higher level security at sensitive facilities, such as power plants.[270]

In effect, then, Sales conceives of cybersecurity as a public goods and externalities problem. This connection is made explicit by his analogy to the classic public goods case, the government's provision of military protection: "in World War II, factories were not expected to install anti-aircraft batteries to defend themselves against Luftwaffe bombers. Nor should we expect power plants to defend themselves against foreign governments' cyber-attacks."[271] The connection to public goods theory is made explicit in Sales' graph, in which the protection curve is labeled "Public Good."[272]

And yet, Sales also suggests that, "[p]rivate investment in cyber-security also resembles a tort problem—more precisely, a products liability problem."[273] He suggests that products liability law, if applied to items such as malware-prone software, could provide incentives to make the product more secure.[274] But Sales notes that "a venerable chestnut of tort law known as the economic loss doctrine," together with the licensing model of most software products, limits the possibility of tort liability for cybersecurity lapses.[275] Sales thinks this result is incorrect, although it is unclear when Sales might apply a negligence rule.[276]

267. *Id.* at 1512–16.

268. *Id.* at 1513, 1517.

269. *Id.* at 1509 ("These [cybersecurity] protocols should not be issued in the form of traditional agency commands. Instead, as is sometimes the case in environmental law and other fields, the private sector should actively participate in formulating the standards.").

270. *Id.* at 1517–18.

271. *Id.*

272. *Id.* at 1513.

273. *Id.* at 1533.

274. *Id.* at 1535.

275. *Id.*

276. *Id.* at 1535, 1557.

C. A Role for Negligence Law

As Sales suggests, the economic loss doctrine should *not* bar tort claims in data breach cases involving the consumer credit card system. Because the system is a highly distributed "weakest link" network, there are large numbers of failure points that could entail enormous negative externalities resulting from any one node's failure. Although the parties' relationships are governed by contracts, there is little opportunity for important players such as credit unions to negotiate different privacy, security, and indemnity terms because the major card brands possess market power. Moreover, the prevalence of third-party payment processors significantly skews the discipline that might be imposed through contract and might even explode the system.

Consider again the BJ's litigation. That court's stringent application of the economic loss doctrine might suggest that the court thought there were adequate remedies sounding in contract. This is partially correct. The court found there was enough evidence to survive summary judgment concerning the plaintiffs' claims that they were intended beneficiaries of the contractual relationship between Fifth Third and BJ's.[277] This was based on some documents suggesting that the security requirements in the Visa agreements between the acquirer bank and the merchant were designed to protect all the stakeholders in the Visa system, including card members and issuer banks.[278]

Third-party beneficiary theory, however, is a slender reed on which to rest the adjustment of risk in a massive consumer credit card breach case. The web of contractual relationships instantiated by a consumer credit card network such as the Visa network certainly is not intended to transform the acquirer banks, or the merchants, into the insurers of the issuer banks against their contractual duties to reimburse card holders in the event of fraud. There is a wide range of credit card fraud—not only arising from data breaches—that merchants and acquirer banks routinely take some measures to mitigate. But neither merchants nor acquirer banks can prevent all fraud.

The problem seems ripe for the application of classic cost-benefit negligence liability principles: there is always a rough calculation between the probability of some loss and the burden of measures required to prevent the loss.[279] If the economic loss doctrine prohibits the use of a cost-benefit

277. Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 168–173, 179 (3d Cir. 2008).

278. *See id.* at 169–71.

279. *See, e.g.*, United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (setting forth the "Hand balancing test"); GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970); SHAVELL, *supra* note 7; Keith N. Hylton, *Duty in Tort Law: An*

negligence formula in these circumstances, it must also prohibit the use of third party beneficiary theory as a proxy for a negligence claim. Either the credit card network agreements expressly provide for indemnification between the merchants, acquirer banks, and issuer banks, or they do not; and if the issuer banks desire such indemnification in light of data breach risks, they can bargain for it, or they can mitigate their risk through insurance. That, at least, is what a rigorous application of the economic loss doctrine in a consumer credit card data breach case should suggest. The fact that the court in *BJ's* allowed third-party beneficiary contract claims to proceed might imply that the court knew something was wrong with this result.

The industry security standard referenced in the credit card network standards, PCI DSS, may reflect a reasonable standard of care in some circumstances but not in others, a factual question that can and should be subject to the rigors and discipline of the judicial process. Indeed, some commentators note that the PCI DSS standard has proven inadequate and that the industry must move towards a higher level of protection.[280] Much of the economic literature suggests that the persistent incidence of large scale data breaches demonstrates that network externalities or other market failures have led to an underinvestment in security.[281]

In fact, the persistence of PCI-DSS as the default standard despite its apparent shortcomings indicates that an effort to negotiate a different standard would entail prohibitively high transaction costs. Where transaction costs are high, including in cyberspace, a negligence/liability rule usually is the best way to control externalities.[282] This could suggest a strict liability rule relating to cybersecurity, but the economic benefits of information infrastructure networks such as the global consumer credit card system are often also enormous. As Keith Hylton has suggested, in the

Economic Approach, 75 FORDHAM L. REV. 1501, 1503–04 (2006) ("[T]he traditional economic approach to tort law treats the Hand balancing test as the default rule, and strict liability as an option that should be adopted when it is desirable to reduce activity levels. The traditional approach has been applied largely to negligence law, and has been successful in explaining negligence doctrine." (citing WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW (1987)); Richard A. Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29 (1972).

280. *See, e.g.*, MacCarthy, *supra* note 19, at 3; Katherine Brocklehurst, *PCI DSS Compliance is No Security Guarantee*, TRIPWIRE (Feb. 13, 2014), http://www.tripwire.com/state-of-security/regulatory-compliance/pci-dss-compliance-security-guarantee/.

281. *See, e.g.*, MacCarthy, *supra* note 19, at 15 ("The fact that data breaches of enormous size continue suggests that the misaligned incentives in the U.S. payment industry have indeed resulted in underinvestment in security. Hackers discovered the vulnerabilities in payment systems. These vulnerabilities were fixable through sufficient expenditure of resources, but they were not fixed quickly.").

282. *See, e.g.*, Keith N. Hylton, *Property Rules, Liability Rules, and Immunity: An Application to Cyberspace*, 87 B.U. L. REV. 1, 14 (2007).

presence of high transaction costs, where the economic benefits of an activity outweigh the economic costs, the best way to control externalities is through a negligence liability rule.[283]

For Hylton, this would include certain kinds of negligence-based claims for cybersecurity vulnerabilities.[284] Hylton notes that:

> Cases of information theft would appear to be ideal for class actions. They involve small losses spread across large numbers of victims. . . . Where the information holder has been negligent, the penalty generated by class action litigants should be large enough to deter future negligence. Moreover, this is theoretically superior on deterrence grounds to a scheme involving statutory penalties, because the damage judgments awarded in class actions will have a closer fit to the actual harm suffered by victims than would statutorily set penalties.[285]

Similarly, Professor Vincent Johnson has argued that in circumstances where there is a business relationship between a database possessor and data subject, imposing a duty of care "will force the database possessor, who benefits from the use of computerized information, to internalize losses relating to improperly accessed data as a cost of doing business."[286]

The suggestion that data breach tort claims should not be barred by the economic loss doctrine does not affect the issue of the need to prove ascertainable losses in order to have Article III standing. This means that courts could continue to summarily dispose of speculative claims, such as consumer claims for future credit monitoring. Even as to these claims, some plaintiffs may be able to prove ascertainable losses relating to credit monitoring and other expenses, or the claims may be cognizable in state court.[287] Such claims should not founder on the economic loss doctrine.[288]

Allowing negligence claims for data breaches, where a business or individual has suffered an ascertainable pecuniary loss, would open the possibility of many kinds of claims that are not currently optimally socially adjusted for by contract, including claims involving third-party payment processors. In the process, it would facilitate more open and public scrutiny of industry security practices and would provide the impetus for more robust and predictable cyber insurance underwriting standards.

---

283. *Id.*

284. *Id.* at 29–36.

285. *Id.* at 38.

286. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 275 (2005) (citing VINCENT R. JOHNSON & ALAN GUNN, STUDIES IN AMERICAN TORT LAW 7–8 (3d ed. 2005)).

287. *See* Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113 (2011).

288. *See id.* at 122–23; Johnson, *supra* note 286, at 296–303.

V. CONCLUSION

Data breaches are pervasive and costly. Recent civil data breach cases have centered on the consumer credit card payment chain in the retail industry. An important issue in such cases is whether the economic loss doctrine should bar negligence claims for purely pecuniary losses suffered by a non-negligent party, such as an issuing bank or a federal credit union that must incur costs to reimburse cardholders for the fraudulent use of stolen card numbers.

The economic loss doctrine should not bar these claims. Large scale data networks, such as the consumer credit card networks, often entail significant network externalities. These include externalities relating to market concentration as well as to the "weakest link" nature of security in these networks. Although the primary players in these networks are tied together in a complex web of contractual relationships, there are significant transaction costs involved with any effort to change or monitor another party's security measures. Moreover, "outside" entities such as third-party payment processors, which are not in contractual privity with all other parties in the network, have become ubiquitous. Under these circumstances, a negligence rule should help improve cybersecurity hygiene and promote a more robust cyber risk insurance market.